

Regierungsrat, Rathausstrasse 2, 4410 Liestal

Eidgenössisches Justiz- und Polizeidepartement EJPD, Bern

ptss-aemterkonsultationen@isc-ejpd.admin.ch

Liestal, 1. April 2025

Vernehmlassung betreffend Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF; VD-ÜPF)

Sehr geehrter Herr Bundesrat

Wir bedanken uns für die Gelegenheit zur Meinungsäusserung und teilen Ihnen mit, dass wir die vorgeschlagenen Anpassungen begrüssen.

Zu den einzelnen Bestimmungen haben wir folgende Bemerkung:

Art. 35 Abs. 1 Bst. b sowie Art. 40 Abs. 1 Bst. b VÜPF

Bei den Auskunftstypen IR_4_NA und IR_10_TEL beantragen wir, dass auch ausgewiesen wird, ob es sich um eine physische SIM-Karte oder um eine eSIM handelt.

Hochachtungsvoll



Isaac Reber
Regierungspräsident



Elisabeth Heer Dietrich
Landschreiberin



ETAT DE FRIBOURG
STAAT FREIBURG

Conseil d'Etat
Route des Arsenaux 41, 1700 Fribourg

Conseil d'Etat CE
Staatsrat SR

Route des Arsenaux 41, 1700 Fribourg
T +41 26 305 10 40
www.fr.ch/ce

PAR COURRIEL

Département fédéral de justice et police DFJP
Palais fédéral ouest
3003 Berne

Courriel :

ptss-aemterkonsultationen@isc-ejpd.admin.ch

Fribourg, le 8 avril 2025

2025-521

Révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT) – Procédure de consultation

Monsieur le Conseiller fédéral,

Par courrier du 29 janvier 2025, vous nous avez consultés sur le projet cité en titre, et nous vous en remercions.

La révision envisagée n'appelle aucune remarque particulière de notre part, et nous pouvons ainsi pleinement la soutenir.

Nous vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de nos sentiments les meilleurs.

Au nom du Conseil d'Etat :

Jean-François Steiert, Président



Danielle Gagnaix-Morel, Chancelière d'Etat

L'original de ce document est établi en version électronique

Copie

—
à la Direction de la sécurité, de la justice et du sport, pour elle, la Police cantonale et le Ministère public ;
à la Chancellerie d'Etat.

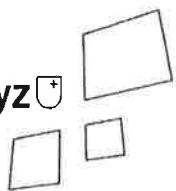
Volkswirtschaftsdepartement

Departementsvorsteherin

Bahnhofstrasse 15
Postfach 1180
6431 Schwyz
Telefon 041 819 16 52
E-Mail vd@sz.ch
www.sz.ch

kanton**schwyz**

6431 Schwyz, Postfach 1180



per E-Mail

Eidgenössisches Justiz- und Polizeidepartement
3003 Bern

ptss-aemterkonsultationen@isc-ejpd.admin.ch

E-Mail petra.steimen@sz.ch
Direktwahl 041 819 18 00
Datum 9. April 2025

Vernehmlassung Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF und VD-ÜPF) Vernehmlassung

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 29. Januar 2025 hat das Eidgenössische Departement für Justiz- und Polizei den Kantonsregierungen die Unterlagen zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF und VD-ÜPF) zur Vernehmlassung bis 6. Mai 2025 unterbreitet. Gerne äussern wir uns dazu wie folgt:

Im Dezember 2022 rief der damalige Ausschuss Fernmeldeüberwachung (FMÜ) die Begleitgruppe Rechtsetzung ins Leben, um insbesondere die Strafverfolgungsbehörden, aber auch die Mitwirkungspflichtigen in der Erarbeitung von Gesetzesvorlagen miteinzubeziehen. Das hat sich aus unserer Sicht bewährt. Der Dienst ÜPF hat mit dieser Begleitgruppe im Hinblick auf die Ausarbeitung der obgenannten Vorlagen mehrere Sitzungen durchgeführt, eingebrachte Vorbehalte und Fragen wurden berücksichtigt, beziehungsweise geklärt. Die nun präsentierten Entwürfe entsprechen nach unserem Dafürhalten dem in der Begleitgruppe Rechtsetzung Besprochenen. Das Ziel der Vorlage, die verschiedenen Kategorien von Mitwirkungspflichtigen näher zu definieren, deren Pflichten zu umschreiben und bekannte Lücken bei einzelnen Überwachungstypen zu schliessen, wird erreicht. Die Anliegen und Bedürfnisse der Strafverfolgungsbehörden im Rahmen des übergeordneten Rechts sind angemessen und zweckmässig berücksichtigt.

Nicht Thema der vorliegenden Teilrevision sind – naturgemäß – die Vereinfachung und Verbesserung der Beweiserhebung und Beweissicherung von Daten. Wir möchten bei dieser Gelegenheit jedoch darauf hinweisen, dass in Bezug auf die mittel- und längerfristige Anpassung an die technologische Entwicklung grundlegende Reformen in der Strafprozessordnung und im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2025 (BÜPF, SR 780.1) notwendig sind.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und versichern Sie, Herr Bundesrat, unserer vorzüglichen Hochachtung.

Freundliche Grüsse
Volkswirtschaftsdepartement
Departementsvorsteherin



Petra Steimen-Rickenbacher
Regierungsrätin



Elektronisch an ptss-aemterkonsultationen@isc-ejpd.admin.ch



**Kanton Zürich
Regierungsrat**

staatskanzlei@sk.zh.ch
Tel. +41 43 259 20 02
Neumühlequai 10
8090 Zürich
zh.ch

Eidgenössisches Justiz- und Polizeidepartement
3003 Bern

9. April 2025 (RRB Nr. 375/2025)

Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (Vernehmlassung)

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 29. Januar 2025 haben Sie uns eingeladen, zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs Stellung zu nehmen. Wir danken für diese Gelegenheit und äussern uns wie folgt:

Wir unterstützen die Teilrevision der VÜPF und VD-ÜPF und haben zu den einzelnen Bestimmungen folgende Anmerkungen:

Art. 48b Abs. 2 VÜPF

Wir beantragen, den Abs. 2 folgendermassen zu formulieren:

Bei Lokalisationseinsätzen mit besonderen technischen Geräten zur Überwachung des Fernmeldeverkehrs gem. Art. 269^{bis} StPO (IMSI-Catcher) soll auf Anfrage mit dem permanenten Identifikator (SUPI) eines gesuchten Mobilfunkgerätes der jeweilig aktuelle temporäre Identifikator (z. B. SUCI, 5G-GUTI) automatisiert geliefert werden.

Art. 48b Abs. 1 regelt den Fall, wie angefragte temporäre Identifikatoren zur Auskunft über die entsprechenden permanenten Identifikatoren führen. Der umgekehrte Fall ist jedoch nicht geregelt. Während einer Lokalisierung (z. B. einer Notsuche) wird jedoch der aktuell verwendete temporäre Identifikator benötigt, mit dem sich ein gesuchtes Gerät gerade ausweist. Da sich dieser immer wieder ändert, braucht es eine automatisierte Auskunft. Ferner ist die im Revisionsentwurf verlangte Präzisierung in Abs. 2, soweit sie über die einfache Nennung eines temporären Identifikators hinausgeht, in der Praxis oft nicht möglich, weil insbesondere bei Fällen zur Lokalisation mit IMSI-Catcher im Zeitpunkt der Anfrage noch nicht bekannt ist, in welchem Mobilfunkgebiet sich ein gesuchtes Gerät befindet. Werden z. B. SUCI-Nummern gleichzeitig mehrfach vergeben, bräuchte es jedoch die im Revisionsentwurf genannten standortgebundenen Angaben zur eindeutigen Identifikation. Die von uns beantragte Formulierung führt im Ergebnis dazu, dass die temporären Identifikatoren immer nur einmal gleichzeitig vergeben werden.

Art. 50 Abs. 9 VÜPF

Wir möchten darauf hinweisen, dass es mit dem heute eingesetzten Tool (WMC) technisch nicht möglich ist, einen Auftrag (im WMC = Anordnung) mit einer Nummer eines weiteren Endgerätes (Multi-Device) oder einer neuen SIM (Extra-SIM) zu ergänzen, wenn dieser Auftrag im WMC einmal erfasst wurde. Bislang muss im WMC dann eine zusätzliche Anordnung erfolgen.

Zudem ist auf Folgendes hinzuweisen:

Laut Auskunft des Schweizerischen Verbands der Telekommunikation, asut, betreffen rund 90% der Überwachungen des Post- und Fernmeldeverkehrs im Rahmen einer Strafverfolgung die drei grossen Anbieter Swisscom, Salt und Sunrise. Viele kleinere Unternehmen sind hingegen selten bis nie verpflichtet, Informationen zu liefern.

Die Einführung klarer Definitionen für Mitwirkungspflichten von Telekommunikationsanbietern ist grundsätzlich zu begrüssen, da sie zu mehr Rechtssicherheit führt. Es ist jedoch wichtig sicherzustellen, dass die Abstufungen und die damit verbundenen Pflichten für die jeweiligen Anbieter verhältnismässig und praxistauglich sind. Die von den Unternehmen zu tätigen Investitionen sollten in einem angemessenen Verhältnis zum Nutzen der Investitionen und zur Wirtschaftskraft der betroffenen Unternehmen stehen. Dabei ist zu berücksichtigen, dass zusätzliche Investitionen für kleinere Unternehmen verhältnismässig höhere Kosten bedeuten und ihre Wettbewerbsfähigkeit entsprechend beeinträchtigen können. Dies fällt umso mehr ins Gewicht, als das Entschädigungssystem nur für variable Kosten gilt, während die Investitionskosten (Fixkosten) von den Anbietern selbst getragen werden müssen.

Freundliche Grüsse

Im Namen des Regierungsrates

Die Präsidentin:

Natalie Rickli

Die Staatsschreiberin:

Dr. Kathrin Arioli





Conseil d'Etat
Staatsrat
CP 670, 1951 Sion

CANTON DU VALAIS
KANTON WALLIS



2025.01284

P.P. CH-1951
Sion

A-PRIORITY Poste CH SA



Monsieur
Beat Jans
Conseiller fédéral
Chef du Département fédéral de Justice
et police
Palais fédéral ouest
3003 Berne

Notre réf. C-62324
Votre réf. /

Date - 9 AVR. 2025

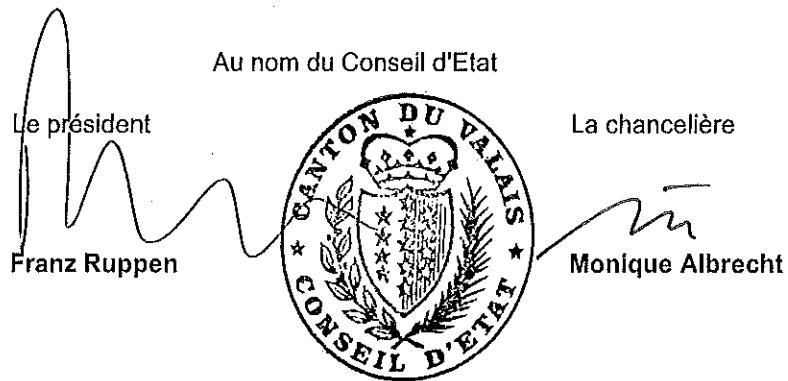
Révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT)

Monsieur le Conseiller fédéral,

Le Conseil d'Etat du canton du Valais vous remercie de l'avoir associé à la consultation citée en titre.

Nous saluons les modifications proposées, nécessaires à la mise à niveau des technologies de télécommunications, offrant ainsi de nouveaux types de renseignements utiles au domaine judiciaire.

Nous vous prions d'agréer, Monsieur le Conseiller fédéral, l'expression de notre considération distinguée.

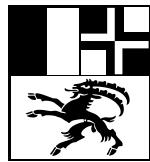


Copie à M. Christian Varone, Commandant de la Police cantonale
ptss-aemterkonsultationen@isc-ejp.admin.ch



Place de la Planta 3, CP 670, 1951 Sion
Tél. 027 606 21 00

Die Regierung
des Kantons Graubünden



La Regenza
dal chantun Grischun

Il Governo
del Cantone dei Grigioni

Sitzung vom

15. April 2025

Mitgeteilt den

15. April 2025

Protokoll Nr.

273/2025

Per E-Mail (PDF- und Word-Version) zustellen an:

ptss-aemterkonsultationen@isc-ejpd.admin.ch

Vernehmlassung EJPD - Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Stellungnahme

Sehr geehrter Herr Bundesrat

Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar 2025 erhalten die Kantone Gelegenheit, sich zu erwähntem Geschäft zu äussern. Dafür danken wir Ihnen bestens.

Die uns zugesandte Dokumentation haben wir geprüft. Die Regierung begrüsst grundsätzlich die Teilrevisionen der zwei Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF). Dass die Strafverfolgungsbehörden und die Mitwirkungspflichtigen im Rahmen der Begleitgruppe Rechtsetzung einbezogen worden sind, hat sich bewährt. Die Anliegen und Bedürfnisse der Strafverfolgungsbehörden im Rahmen des übergeordneten Rechts werden angemessen und zweckmässig berücksichtigt. Hingegen kommt die Vorlage, dem Anliegen der Strafverfolgungsbehörden, die Beweiserhebung und -sicherung von Daten im Strafverfahren zu vereinfachen und zu verbessern, nicht entgegen. Wir weisen darauf hin, dass in Bezug auf die mittel- und längerfristige Anpassung an die technologische Entwicklung grundlegende Reformen in der Schweizerischen Strafprozessordnung (StPO; SR 312.0) und im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR 780.1) notwendig sind.

Es ist positiv zu bewerten, dass neue Möglichkeiten in der Überwachung geschaffen werden. Dies stellt eine Verbesserung der aktuellen Situation dar. Es bleibt abzuwarten, wie sich die neuen Kategorien im Bereich von Mitwirkungspflichtigen sowie ihrer Pflichten auf die Dienstleistungsbereitschaft bzw. die Dienstleistungen selbst auswirkt.

Abschliessend danken wir für die Berücksichtigung unserer Anliegen und für die Möglichkeit zur Stellungnahme.



Namens der Regierung

Der Präsident:

A handwritten signature in black ink.

Marcus Caduff

Der Kanzleidirektor:

A handwritten signature in black ink.

i.V. C. Hartmann Lütscher



KANTON
NIDWALDEN

LANDAMMANN UND
REGIERUNGSRAT

Dorfplatz 2, Postfach 1246, 6371 Stans
Telefon 041 618 79 02, www.nw.ch

CH-6371 Stans, Dorfplatz 2, Postfach 1246, STK

PER E-MAIL

Eidgenössisches Justiz- und Polizeidepartement EJPD
Herr Bundesrat Beat Jans
Bundeshaus West
3003 Bern

Telefon 041 618 79 02
staatskanzlei@nw.ch
Stans, 15. April 2025

Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF). Stellungnahme

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 29. Januar 2025 eröffnete das Eidgenössische Justiz- und Polizeidepartement (EJPD) das Vernehmlassungsverfahren des titelerwähnten Geschäfts. Wir bedanken uns für die Möglichkeit zur Stellungnahme und verweisen auf unsere nachfolgende Begründung.

1 Allgemeine Beurteilung

Die vom Bundesrat vorgeschlagene Teilrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) sowie der Verordnung des EJPD über deren Durchführung (VD-ÜPF) erachten wir als notwendig und sachgerecht. Angesichts des raschen technologischen Fortschritts und der zunehmend vielfältigen Formen digitaler Kommunikation ist eine zeitgemässre rechtliche Grundlage für die Fernmeldeüberwachung unerlässlich.

Die überarbeitete Kategorisierung der Mitwirkungspflichtigen (MWP) trägt zu einer klareren Systematik bei und erhöht die Rechtssicherheit für die betroffenen Unternehmen. Gleichzeitig wird die Effizienz der Zusammenarbeit zwischen Strafverfolgungsbehörden und Dienstleistungsanbietern gestärkt.

2 Begrüssung der neuen Auskunfts- und Überwachungstypen

Besonders hervorheben möchten wir die auf Wunsch der Strafverfolgungsbehörden neu geschaffenen Auskunfts- und Überwachungstypen. Diese Erweiterungen erlauben differenziertere Ermittlungsansätze, insbesondere in komplexen Sachverhalten mit digitalen Spuren. Die Standardisierung bislang nur vereinzelt genutzter Anfragen fördert die Transparenz und verbessert die Umsetzbarkeit im Vollzug.

Wir begrüssen diesen Schritt ausdrücklich, da er sowohl dem Bedürfnis der Strafverfolgung nach zielgerichteten Auswertungen als auch den Erfordernissen eines verhältnismässigen und technisch abgestützten Zugriffs gerecht wird.

3 Weitere Anpassungen

Die übrigen Änderungen betreffen in erster Linie redaktionelle Präzisierungen, Anpassungen an bestehende Gegebenheiten sowie die Umsetzung der gesetzlichen Delegation aus Art. 2 Abs. 2 BÜPF. Diese Änderungen erscheinen weitgehend unbestritten. Wir nehmen sie zur Kenntnis und sehen in diesen Punkten keinen weiteren Handlungsbedarf.

4 Kostenfolgen für die Kantone

Ein zentrales Anliegen bleibt für uns die Kostenentwicklung im Bereich der Fernmeldeüberwachung. Seit dem Jahr 2024 werden den Kantonen die Überwachungskosten in Form von Pauschalen in Rechnung gestellt. Diese werden alle drei Jahre neu berechnet und können je nach technischer Entwicklung und Nutzung stark variieren.

Die in der Revision vorgesehenen zusätzlichen Auskunfts- und Überwachungstypen sowie die Differenzierung der Mitwirkungspflichten lassen einen weiteren Anstieg der Kosten erwarten. Dies wirft Fragen zur **Angemessenheit der verrechneten Pauschalen** auf, insbesondere hinsichtlich der tatsächlichen Aufwände der betroffenen Dienstleistungsunternehmen.

Aus Sicht der Kantone ist es essenziell, dass die Kosten in einem **angemessenen Verhältnis zum effektiven Nutzen für die Strafverfolgung** stehen. Wir regen daher an, dass die künftige Weiterentwicklung der technischen Standards und Kategorien regelmässig unter Berücksichtigung der **Kosten-Nutzen-Verhältnisse** evaluiert wird. Transparente Grundlagen für die Berechnung der Pauschalen sind ebenso notwendig wie eine Überprüfung, ob Synergieeffekte genutzt und Effizienzgewinne an die öffentliche Hand weitergegeben werden.

5 Fazit

Der Regierungsrat unterstützt die vorliegende Teilrevision grundsätzlich und erkennt ihren Mehrwert für die Effizienz und Modernisierung der Fernmeldeüberwachung an. Gleichzeitig erwarten wir, dass die finanziellen Auswirkungen für die Kantone auch künftig im Auge behalten und in einem ausgewogenen Verhältnis zur Wirksamkeit der Massnahmen gehalten werden.

Der Regierungsrat Nidwalden bedankt sich für die Möglichkeit zur Stellungnahme und deren Berücksichtigung.

Freundliche Grüsse
NAMENS DES REGIERUNGSRATES


Res Schmid
Landammann





lic. iur. Armin Eberli
Landschreiber

Geht an:
- ptss-aemterkonsultationen@isc-ejpd.admin.ch



Genève, le 16 avril 2025

Le Conseil d'Etat

1456-2025

Département fédéral de justice et police
(DFJP)
Monsieur Beat JANS
Conseiller fédéral
Palais fédéral ouest
3003 Berne

Concerne : consultation relative à la révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT)

Monsieur le Conseiller fédéral,

Nous avons pris connaissance avec attention de la révision partielle des deux ordonnances d'exécution de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (OSCPT et OME-SCPT).

Après consultation du pouvoir judiciaire qui n'a pas d'observation à formuler, nous vous informons soutenir le principe de cette révision, qui vise à adapter les outils de surveillance aux évolutions technologiques.

Cependant, nous rappelons que, par un vote clair en juin 2023, la population genevoise a inscrit dans sa Constitution le droit à l'intégrité numérique, notamment le droit à la sécurité numérique. Aussi, notre Conseil souligne que certaines dispositions de la LSCPT, dans leur mise en œuvre, pourraient entrer en tension avec ce droit fondamental.

A cet égard, il souhaite formuler des réserves au sujet des obligations imposées aux fournisseurs de services fondés sur le chiffrement de bout en bout. Ces obligations – telles que la fourniture automatisée de données – sont inapplicables en pratique sans remettre en cause l'architecture même de ces services, largement utilisés par des professions soumises à un devoir de confidentialité, telles que les avocats, les médecins, les journalistes ou les ONG travaillant dans des contextes sensibles, et qui reposent sur ces outils pour garantir l'effectivité concrète du droit à l'intégrité numérique.

Enfin, notre Conseil souhaite veiller à ne pas fragiliser un secteur stratégique pour l'économie numérique suisse. Il recommande ainsi de :

- prendre en compte les contraintes techniques propres aux prestataires concernés;
- garantir une mise en œuvre proportionnée et différenciée, respectueuse des principes fondamentaux de protection des données et des communications;

- en amont de toute modification des ordonnances, ouvrir un dialogue avec les acteurs économiques impactés, afin de nourrir le processus d'adaptation de leurs contributions concrètes.

Nous vous remercions de nous avoir consultés et vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de notre parfaite considération.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :



Michele Righetti-El Zayadi

La présidente :



Nathalie Fontanet

Copie à (format Word et pdf) : ptss-aemterkonsultationen@isc-ejpd.admin.ch

Justiz- und Sicherheitsdepartement
Bahnhofstrasse 15
Postfach 3768
6002 Luzern
Telefon 041 228 59 17
jsdds@lu.ch
www.lu.ch

Eidgenössisches Justiz- und Polizei-departement EJPD

per E-Mail
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Luzern, 15. April 2025

Protokoll-Nr.: 417

Fernmeldeüberwachung: Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF; VD-ÜPF): Stellungnahme Kanton Luzern

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Für die Gelegenheit, im Rahmen des oben genannten Vernehmlassungsverfahrens Stellung nehmen zu können, danken wir Ihnen. Im Namen und Auftrag des Regierungsrates stimmen wir der Vorlage zu und haben keine weiteren Bemerkungen.

Freundliche Grüsse



Ylfete Fanaj
Regierungsrätin



Landammann und Standeskommission

Sekretariat Ratskanzlei
Marktgasse 2
9050 Appenzell
Telefon +41 71 788 93 11
info@rk.ai.ch
www.ai.ch

Ratskanzlei, Marktgasse 2, 9050 Appenzell

Per E-Mail an
ptss-aemterkonsultationen@isc-
ejpd.admin.ch

Appenzell, 17. April 2025

Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) Stellungnahme Kanton Appenzell I.Rh.

Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar 2025 haben Sie uns die Vernehmlassungsunterlagen zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) zukommen lassen.

Die Standeskommission hat die Unterlagen geprüft. Sie begrüßt die Vorlage. Die Ziele der Teilrevision werden erreicht und die Bedürfnisse der Strafverfolgungsbehörden im Rahmen des übergeordneten Rechts angemessen berücksichtigt.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und grüssen Sie freundlich.

Im Auftrage von Landammann und Standeskommission
Der Ratschreiber:

Roman Dobler

Zur Kenntnis an:

- Justiz-, Polizei- und Militärdepartement Appenzell I.Rh., Marktgasse 10d, 9050 Appenzell
- Ständerat Daniel Fässler, Weissbadstrasse 3a, 9050 Appenzell
- Nationalrat Thomas Rechsteiner (thomas.rechsteiner@parl.ch)



Landammann und Regierungsrat des Kantons Uri

Eidgenössisches Justiz- und
Polizeidepartement (EJPD)
Bundeshaus West
3003 Bern

Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF); Vernehmlassung

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar 2025 laden Sie den Regierungsrat des Kantons Uri ein, zur Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) Stellung zu nehmen.

Der Regierungsrat begrüßt die geplante Revision - insbesondere das Schaffen von zeitgemässen Auskunfts- und Überwachungstypen - und verzichtet auf eine einlässliche Vernehmlassung.

Sehr geehrter Herr Bundesrat, sehr geehrte Damen und Herren, wir bedanken uns für die Möglichkeit zur Stellungnahme und grüßen Sie freundlich.

Altdorf, 22. April 2025



Im Namen des Regierungsrats

Der Landammann

Der Kanzleidirektor

Christian Arnold

Roman Balli

REGIERUNGSRAT

Regierungsgebäude, 5001 Aarau
Telefon 062 835 12 40
Fax 062 835 12 50
regierungsrat@ag.ch
www.ag.ch/regierungsrat

Per E-Mail
Informatik Service Center ISC-EJPD

ptss-aemterkonsultationen@isc-ejpd.admin.ch

23. April 2025

Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF); Vernehmlassung

Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar 2025 wurden die Kantonsregierungen zur Vernehmlassung zu Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) eingeladen. Der Regierungsrat des Kantons Aargau dankt Ihnen für die Gelegenheit, dazu Stellung nehmen zu können und äussert sich wie folgt.

Die Teilrevisionen werden ausdrücklich begrüsst. Wir weisen jedoch auf folgende Punkte hin:

Regelung der Mitwirkungspflichtigen

In den Art. 16d ff. der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) sollen unter anderem die Anbieterinnen von Diensten, die sich auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen (Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]) gemäss Art. 2 lit. c des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) geregelt werden. Diesen AAKD obliegt gemäss Art. 2 BÜPF eine Mitwirkungspflicht im Bereich der Überwachung des Post- und Fernmeldeverkehrs.

Die im Vernehmlassungsentwurf vorgeschlagene Regelung ist aus Sicht der Anbieterinnen zwar nachvollziehbar, jedoch aus polizeilicher Sicht unbefriedigend. Es ist zu beachten, dass durch die fehlende Erreichbarkeit von Anbieterinnen mit reduzierten oder minimalen Pflichten erhebliche Überwachungslücken entstehen können. In dringenden Fällen kann dies dazu führen, dass Teilnehmende nicht rechtzeitig identifiziert werden, was insbesondere in Situationen mit hoher Dringlichkeit oder akuter Gefahr gravierende Folgen haben kann. Muss etwa eine Anbieterin ohne Pikettpflicht kontaktiert werden, bleibt eine Anfrage unter Umständen für Tage unbeantwortet, was die Strafverfolgung erschwert oder gar verhindert. Auch wenn einzelne Anbieterinnen nur wenige Kunden haben, kann die Gesamtanzahl dieser Kunden bei allen kleineren Anbieterinnen zusammen erheblich sein. Dadurch steigt das Risiko, dass sich Kriminelle gezielt auf diese Anbieterinnen konzentrieren. Dies kann bei schweren Straftaten, beispielweise bei Entführungen oder terroristischen Bedrohungen, zu einem grossen Sicherheitsrisiko führen.

Regelung der Auskunftstypen

In den Art. 35 ff. VÜPF sind die verschiedenen Auskunftstypen für Netzzugangsdienste geregelt. Neu soll in Art. 38a VÜPF der Auskunftstyp "IR_58_IP_Intersect: Benutzeridentifikation durch Schnittmen genbildung" eingeführt werden. Dies wird ausdrücklich begrüßt. Es muss jedoch in Art. 11 VÜPF zwingend bestimmt werden, dass auch für diesen Auskunftstyp eine Pikettpflicht gilt. Es ist aus polizeilicher Sicht zwingend, dass diese Auskunft umgehend erteilt wird.

Für allfällige Rückfragen steht Ihnen Herr Rudolf Moos, Stabsmitarbeiter im Departement Volkswirtschaft und Inneres (rudolf.moos@ag.ch; 062 835 14 14), gerne zur Verfügung.

Wir danken Ihnen für die Berücksichtigung unserer Vernehmlassung.

Freundliche Grüsse

Im Namen des Regierungsrats



Dieter Egli
Landammann



Joana Filippi
Staatsschreiberin

Staatskanzlei, Regierungskanzlei, 8510 Frauenfeld

Eidgenössisches
Justiz- und Polizeidepartement EJPD
Herr Beat Jans
Bundesrat
Bundeshaus West
3003 Bern

Altnau, 29. April 2025

Nr. 236

Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Vernehmlassung

Sehr geehrter Herr Bundesrat

Wir danken Ihnen für die Möglichkeit der Stellungnahme zu den Entwürfen für eine Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF; SR 780.11) sowie der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF; SR 780.117) und teilen Ihnen mit, dass wir mit den Vorlagen einverstanden sind.

Im Übrigen weisen wir darauf hin, dass in Bezug auf die mittel- und längerfristige Anpassung an die technologische Entwicklung grundlegende Reformen in der Strafprozessordnung und im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) notwendig sein werden.

Mit freundlichen Grüßen

Der Präsident des Regierungsrates



Der Staatsschreiber





Sicherheitsdirektion, Postfach, 6301 Zug

Nur per E-Mail

Eidgenössisches Justiz- und Po-
lizeidepartement EJPD
Herr Bundesrat Beat Jans
Bundeshaus West
3003 Bern

T direkt +41 41 594 38 29
lukas.kunz@zg.ch
Zug, 30. April 2025 zgkulu
SD SDS 7.11 / 433

Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldever- kehrs (VÜPF, VD-ÜPF)

Stellungnahme des Kantons Zug

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar 2025 haben Sie die Kantonsregierungen eingeladen, sich bis am 06. Mai 2025 vernehmen zu lassen. Der Regierungsrat des Kantons Zug hat die Sicherheitsdirektion mit der direkten Erledigung der Vernehmlassung beauftragt. Nach Rücksprache mit dem Obergericht des Kantons Zug nehmen wir wie folgt zur Vorlage Stellung.

Der Kanton Zug begrüßt die vorgesehenen neuen Auskunfts- und Überwachungstypen. Die genaue Definition der Mitwirkungspflichtigen (MWP) gemäss VÜPF erachten wir als richtig und praxisrelevant. Aufgrund der technischen Komplexität der Vorlage sind die Anwender (u.a. Staatsanwaltschaft und Zwangsmassnahmengericht) weiterhin und regelmässig auf Unterstützung durch den Dienst ÜPF angewiesen. Dadurch kann die rechts- und prozesskonforme Umsetzung gewährleistet werden.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse
Sicherheitsdirektion

Laura Dittli
Regierungsrätin

Versand per E-Mail an:

- ptss-aemterkonsultationen@isc-ejpd.admin.ch; als PDF- und Word-Version
- Zuger Polizei (kommandooffice.polizei@zg.ch)
- Finanzdirektion (info.fd@zg.ch)
- Obergericht des Kantons Zug (marc.siegwart@zg.ch)
- Staatskanzlei (info.staatskanzlei@zg.ch; Abschluss der GEVER-Aufgabe)



CH-6060 Sarnen, Enetriederstrasse 1, SSD

Eidgenössisches Justiz- und Polizeidepartement EJPD

per Mail an:

ptss-aemterkonsultationen@isc-ejpd.admin.ch

Referenz/Aktenzeichen: OWSTK.5300
Unser Zeichen: ks

Sarnen, 1. Mai 2025

**Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF);
Stellungnahme.**

Sehr geehrter Herr Bundesrat,
geschätzter Herr

Für die Einladung zur Stellungnahme zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) danken wir Ihnen.

Durch die vorgesehene Kategorisierung der Mitwirkungspflichtigen wird mehr Klarheit generiert und es werden neue, zeitgemäss Auskunfts- und Überwachungstypen geschaffen. Der Kanton Obwalden befürwortet die vorgeschlagenen Anpassungen und hat keine Änderungsanträge.

Freundliche Grüsse

Christoph Amstad
Regierungsrat

Kopie an:

- Kantonale Mitglieder der Bundesversammlung
- Kantonspolizei
- Staatskanzlei

CONSEIL D'ETAT

Château cantonal
1014 Lausanne

Monsieur le Conseiller fédéral
Beat Jans
Chef du Département fédéral de justice et
police (DFJP)
Palais fédéral ouest
CH-3003 Berne

Par courriel :
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Réf. : 25_COU_1765

Lausanne, le 30 avril 2025

Consultation fédérale - Révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT)

Monsieur le Conseiller fédéral,

Nous faisons suite à la consultation citée en titre et vous remercions d'y avoir associé le Canton de Vaud.

La révision des deux ordonnances en question est saluée, car elle permettra de clarifier la différenciation des personnes obligées de collaborer. Au demeurant, le Conseil d'Etat vaudois n'a pas de remarques particulières à formuler.

Toutefois, le Conseil d'Etat constate que le nombre d'entreprises et de services concernés par les différentes obligations est extrêmement important et fait craindre la mise en œuvre d'un système s'apparentant à une surveillance généralisée en Suisse. Dans sa Stratégie numérique, le Conseil d'Etat souligne la nécessité d'empêcher les traitements abusifs de données personnelles. Finalement, le Conseil d'Etat s'est engagé fortement pour le développement d'un territoire de la confiance numérique et craint que cette révision ne vienne mettre en difficulté cet écosystème en pleine croissance. Dès lors, il demande une redéfinition des catégories de fournisseurs concernés par les différentes obligations et appelle à un dialogue avec les milieux concernés dans les meilleurs délais.

En conclusion, le Conseil d'Etat est d'avis que la Suisse devrait aligner ses pratiques de surveillance sur les standards européens, afin de concilier efficacement sécurité, innovation et respect des droits fondamentaux.

Nous vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de notre respectueuse considération.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE

Christelle Luisier Brodard

LE CHANCELIER

Michel Staffoni



Copies

- Office des affaires extérieures
- Police cantonale

Regierungsrat
Rathaus
8750 Glarus

Eidgenössisches Justiz- und
Polizeidepartement
3003 Bern

Glarus, 29. April 2025
Unsere Ref: 2025-17 / SKGEKO.4819

Vernehmlassung i. S. Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Hochgeachteter Herr Bundesrat
Sehr geehrte Damen und Herren

Das Eidgenössische Justiz- und Polizeidepartement gab uns in eingangs genannter Angelegenheit die Möglichkeit zur Stellungnahme. Dafür danken wir und lassen uns gerne wie folgt vernehmen:

Die Anliegen und Bedürfnisse der Strafverfolgungsbehörden werden vorliegend im Rahmen des übergeordneten Rechts angemessen und zweckmäßig berücksichtigt. Wir weisen jedoch darauf hin, dass mit dieser Revision unserem generellen Anliegen, nämlich die Beweiserhebung und -sicherung von Daten im Strafverfahren zu vereinfachen und zu verbessern, noch nicht Rechnung getragen werden kann. In Bezug auf die mittel- und längerfristige Anpassung an die technologische Entwicklung erachten wird demzufolge grundlegende Reformen in der Strafprozessordnung und im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) als notwendig.

Genehmigen Sie, hochgeachteter Herr Bundesrat, sehr geehrte Damen und Herren, den Ausdruck unserer vorzüglichen Hochachtung.

Freundliche Grüsse

Für den Regierungsrat

Kaspar Becker
Landammann

Arpad Baranyi
Ratsschreiber

E-Mail an (PDF- und Word-Version): ptss-aemterkonsultationen@isc-ejpd.admin.ch



Regierungsrat, 9102 Herisau

Eidg. Justiz- und Polizeidepartement
3003 Bern

Dr. iur. Roger Nobs
Ratschreiber
Tel. +41 71 353 63 51
roger.nobs@ar.ch

Herisau, 1. Mai 2025

Eidg. Vernehmlassung; Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF; VD-ÜPF); Stellungnahme des Regierungsrates von Appenzell Ausserrhoden

Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar 2025 wurden die Kantonsregierungen vom Eidg. Justiz- und Polizeidepartement eingeladen, zu den Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs Stellung zu nehmen. Die Vernehmlassungsfrist dauert bis zum 6. Mai 2025.

Der Regierungsrat von Appenzell Ausserrhoden nimmt dazu wie folgt Stellung:

Er stellt fest, dass das Ziel der Vorlage, die verschiedenen Kategorien von Mitwirkungspflichtigen näher zu definieren, deren Pflichten zu umschreiben und bekannte Lücken bei einzelnen Überwachungstypen zu schließen, erreicht wird. Die Anliegen und Bedürfnisse insbesondere der Strafverfolgungsbehörden im Rahmen des übergeordneten Rechts sind angemessen und zweckmäßig berücksichtigt.

Der Regierungsrat weist jedoch darauf hin, dass in Bezug auf die mittel- und längerfristige Anpassung an die technologische Entwicklung grundlegende Reformen in der Strafprozessordnung und im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) notwendig sind.

Der Regierungsrat begrüßt die vorliegenden Änderungen, verzichtet aber im Übrigen auf die Einreichung einer ausführlichen Stellungnahme.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse

Im Auftrag des Regierungsrates



Dr. iur. Roger Nobs, Ratschreiber



Rathaus, Marktplatz 9
CH-4001 Basel

Tel: +41 61 267 85 62
E-Mail: staatskanzlei@bs.ch
www.regierungsrat.bs.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD

Per Mail an:
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Basel, 29. April 2025

P250152

Regierungsratsbeschluss vom 29. April 2025

Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF); Stellungnahme des Kantons Basel-Stadt

Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar 2025 haben Sie uns die Vernehmlassungsunterlagen zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) zukommen lassen. Wir danken Ihnen für die Gelegenheit zur Stellungnahme und lassen Ihnen nachstehend unsere Anträge und Bemerkungen zukommen.

Der Kanton Basel-Stadt begrüßt die Vorlage grundsätzlich. Gleichzeitig bietet die Vorlagen aus Sicht der Strafverfolgungsbehörden Anlass zu folgenden Bemerkungen.

- **AAKD** (Anbieterinnen abgeleiteter Kommunikationsdienste) sind Anbieterinnen, deren Dienste sich auf Fernmeldedienste stützen und die ihren Benutzerinnen und Benutzern eine Einweg- oder Mehrwegkommunikation ermöglichen, wie etwa Online-Speicherdiensste, Dienste zum Hochladen und Teilen von Inhalten oder Cloud Computing. Die in der Vorlage vorgenommene Kategorisierung ist aus Sicht der Mitwirkungspflichtigen nachvollziehbar, für die Strafverfolgungsbehörden jedoch unbefriedigend. Wenn bei solchen Anbietern weder Kontaktstellen noch Pikettregelungen vorgesehen sind, entstehen Überwachungslücken. In dringenden Fällen könnten dadurch Teilnehmerinnen und Teilnehmer nicht rechtzeitig identifiziert werden – mit Folgen für die öffentliche Sicherheit und den Schutz von Menschenleben.

Hinzu kommt, dass viele dieser Anbieter ausserhalb des Geltungsbereichs des schweizerischen Rechts operieren. Es wird deshalb kaum durchsetzbar sein, dass Strafverfolgungsbehörden die notwendigen Informationen überhaupt oder zeitnah erhalten. Selbst wenn eine Verpflichtung zur Mitwirkung rechtlich möglich wäre, ist zu erwarten, dass die eingesetzte Ende-zu-Ende-Verschlüsselung eine Herausgabe relevanter Daten faktisch verunmöglich.

Für Anbieter mit reduzierten oder minimalen Pflichten (FDA bzw. AAKD) sollte zudem ebenfalls eine Mindestaufbewahrungspflicht für Randdaten von sechs Monaten vorgesehen werden.

- Betreffend **Überwachungs- resp. Auskunftstypen** sind aus Sicht einer Strafverfolgungsbehörde folgende Neuanschaffungen sinnvoll:

- IR_58_IP_INTERSECT
- IR_59_EMAIL_LAST
- IR_60_COM_LAST
- RT_61_NA_CC-TRUNC_IRI
- HD_62_IP

Unter dem Gesichtspunkt Gefahrenabwehr sollte der Auskunftstyp IR_58_IP_INTERSECT (Art. 38a VÜPF) jedoch ebenfalls pikettpflichtig sein. Zudem ist es angezeigt, für IR_58_IP_INTERSECT dieselben Bearbeitungsfristen von Auskünften vorzusehen wie für die in Art. 14 Abs. 2 Bst. c VD-ÜPF genannten Auskunftstypen.

Gemäss Art. 35 Abs. 1 Bst. b Ziff. 4 sowie Art. 40 Abs. 1 Bst. b Ziff. 4 umfassen die Angaben der Auskunftstypen IR_4_NA und IR_10_TEL bei einem Multi-Device-Angebot jeweils die Information, ob es sich um das Haupt- oder ein Nebengerät handelt. Dies sollte auch für die Auskunftstypen IR_6 und IR_12 standardmässig gelten und nicht bloss «gegebenenfalls» (vgl. Art. 36 Abs. 1 Bst. b Ziff. 6 und Art. 41 Abs. 1 Bst. b Ziff. 4).

Insgesamt ist vorgesehen, dass bestimmte MWP – abhängig von ihrer betrieblichen Grösse oder dem Umfang ihres Dienstleistungsangebots – nicht rund um die Uhr verfügbar sein müssen. Diese Einschränkung mag aus betriebswirtschaftlicher Sicht nachvollziehbar sein. Für die Strafverfolgungsbehörden hätte dies jedoch zur Folge, dass Auskunftsersuchen, die zwischen Freitagnachmittag und Montagmorgen oder an Feiertagen gestellt werden, unter Umständen unbeantwortet bleiben. Damit würden bewusst Sicherheitslücken in Kauf genommen. Dies wäre aus Sicht der Strafverfolgung problematisch, namentlich bei dringlichen Fällen, schwerwiegenden Rechtsverletzungen oder in Situationen, in denen es um die unmittelbare Gefahrenabwehr und den Schutz von Menschenleben geht.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen. Für Rückfragen steht Ihnen gerne die Staatsanwaltschaft Basel-Stadt, Herr Dr. phil. Martin Schütz, martin.schuetz@stawa.bs.ch, Tel. 061 267 19 90, zur Verfügung.

Freundliche Grüsse
Im Namen des Regierungsrates des Kantons Basel-Stadt



Dr. Conratin Cramer
Regierungspräsident



Barbara Schüpbach-Guggenbühl
Staatsschreiberin

Numero
1959

sl

0

Bellinzona
30 aprile 2025

Consiglio di Stato
Piazza Governo 6
Casella postale 2170
6501 Bellinzona
telefono +41 91 814 41 11
fax +41 91 814 44 35
e-mail can@ti.ch
web www.ti.ch

Repubblica e Cantone
Ticino

Il Consiglio di Stato

Dipartimento federale di giustizia e polizia
DFGP
Palazzo federale ovest
3003 Berna

Invio per posta elettronica (Word e pdf):
ptss-aemterkonsultationen@isc-
ejpd.admin.ch

Procedura di consultazione concernente la revisione parziale di due ordinanze esecutive in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT, OE-SCPT)

Gentili signore,
egregi signori,

abbiamo ricevuto la vostra lettera del 29 gennaio 2025 in merito alla summenzionata procedura di consultazione e ringraziamo per l'opportunità che ci viene offerta di esprimere il nostro giudizio.

Le ordinanze, unitamente al rapporto esplicativo, sono stati da noi esaminati in collaborazione con il Ministero pubblico e il servizio di polizia interessato. Preso atto delle modifiche proposte, non abbiamo particolari osservazioni, se non in relazione all'informazione opzionale per i due tipi di informazione (TEL e NA) prevista all'art. 36 cpv. 1 lett. b n. 6 e all'art. 41 cpv. 1 lett. b n. 4 OSCPT.

Siamo dell'avviso che tale possibilità dia origine a confusione agli inquirenti e crei richieste aggiuntive alle categorie di persone obbligate a collaborare (POC). Infatti, definire "opzionale" l'informazione in un prodotto, non permette all'inquirente di avere la certezza che l'abbonato abbia o meno tale offerta. Il richiedente è quindi obbligato a inviare un'ulteriore domanda tramite il relativo prodotto per ottenere questa informazione. Ritenuta l'importanza di essere a conoscenza di quali informazioni si ottengono con quali prodotti senza opzioni, proponiamo dunque di togliere l'espressione "eventualmente" dalle succitate disposizioni.

Vogliate gradire, gentili signore, egregi signori, i sensi della nostra massima stima.

RG n. 1959 del 30 aprile 2025

PER IL CONSIGLIO DI STATO

Il Presidente



Norman Gobbi

Il Cancelliere



Arnoldo Coduri

Copia a:

- Dipartimento delle istituzioni (di-dir@ti.ch)
- Segreteria generale del Dipartimento delle istituzioni (di-sg.ap@ti.ch)
- Polizia cantonale (polizia-segr@polca.ti.ch; servizio.giuridico@polca.ti.ch)
- Divisione della giustizia (di-dg@ti.ch)
- Deputazione ticinese alle Camere federali (can-relazioniesterne@ti.ch)
- Pubblicazione in Internet



Regierungsrat Christof Hartmann

Sicherheits- und Justizdepartement, Oberer Graben 32, 9001 St.Gallen

Eidgenössisches Justiz- und
Polizeidepartement
Bundeshaus West
3003 Bern

Regierungsrat Christof Hartmann
Sicherheits- und Justizdepartement
Oberer Graben 32
9001 St.Gallen
T +41 58 229 36 00
christof.hartmann@sg.ch

St.Gallen, 1. Mai 2025

Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF); Vernehmlassungsantwort

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 29. Januar 2025 laden Sie uns zur Vernehmlassung zu den Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) bis am 6. Mai 2025 ein. Wir danken für diese Gelegenheit und nehmen gern wie folgt Stellung:

Wir teilen Ihnen gerne mit, dass wir die Teilrevisionen unterstützen. Die Anpassungen sind notwendig und tragen zur verbesserten Verständlichkeit bei. Die Schaffung neuer Auskunfts- und Überwachungstypen begrüssen wir sehr. Die detaillierten Anmerkungen entnehmen Sie bitte dem Anhang.

Ausserhalb der unterbreiteten Teilrevisionen regen wir weitere Änderungen in der VÜPF an:

- Aus unserer Sicht sollte in Art. 20 Abs. 3 VÜPF der unbestimmte Begriff «geeigneter Weise» durch klare Vorgaben ersetzt werden, wie die Anbieterinnen von Fernmelddiensten die Überprüfung der ordnungsmässen Registrierung und Identifizierung durch den Wiederverkäufer vorzunehmen haben. Damit würden in der Praxis bestehende Probleme beseitigt.
- Zielführend wäre auch, Art. 48a Abs. 1 VÜPF anzupassen. Heute müssen bei einer Lokalisierung und insbesondere einer Notsuche alle temporären Identifikatoren abgefragt werden, was die Datenbandbreite über die Mobilfunkschnittstelle stark auslastet. Damit nicht mehr alle temporären Identifikatoren im Rahmen einer Lokalisierung, insbesondere einer Notsuche, angefragt werden müssen, soll automatisch ohne Anfrage und in Echtzeit der jeweilige temporäre Identifikator vom gesuchten Mobilfunkgerät geliefert werden. Damit wird einerseits die Datenbandbreite über die Mobilfunkluftschnittstelle zwischen technischem Gerät (IMSI-Catcher) und Mobilfunknetzbetreiberin erheblich reduziert. Andererseits finden Notsuchen häufig in Gebieten mit eingeschränkter



Mobilfunkversorgung statt, bei denen ohnehin eine geringe Datenbandbreite für die Übertragung zur Verfügung steht.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

A handwritten signature in blue ink, appearing to read "Ch Hartmann".

Regierungsrat Christof Hartmann

Beilage:
Anhang

Zustellung auch per E-Mail (pdf- und Word-Version) an:
ptss-aemterkonsultationen@isc-ejpf.admin.ch



Anhang zur Vernehmlassungsantwort «Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)»

Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF):

Artikel	Antrag	Begründung / Bemerkung
16b, 16e, 16f	Einfügung eines zusätzlichen Absatzes: Aufnahme einer Verpflichtung des Dienstes ÜPF zur Vornahme von Abklärungen (gestützt auf Meldungen oder eigene Informationen), wenn FDA oder AAKD höhergestuft (Upgrade) werden müssen und Einleitung entsprechender Massnahmen zur Höherstufung, wenn Voraussetzungen erfüllt sind.	Aus den genannten Bestimmungen sind keine Verpflichtungen an den Dienst ÜPF ersichtlich, die den Dienst zur Vornahme von Abklärungen sowie Einleitung entsprechender Massnahmen verpflichten würden. Erfüllt z.B. ein FDA oder AAKD mit reduzierten Pflichten die Voraussetzungen für eine Höherstufung (Upgrade) und meldet diese nicht an den Dienst ÜPF, findet offensichtlich keine zusätzliche Prüfung / Überprüfung statt. D.h. ein allfälliges Upgrade ist einzig und allein von der Meldung der FDA bzw. AAKD abhängig. Bei Erhalt oder Vorliegen entsprechender Hinweise sollte der Dienst ÜPF verpflichtet werden, entsprechende Abklärungen zur Beurteilung einzuleiten oder von sich aus tätig zu werden sowie notwendige Massnahmen (z.B. Upgrade) einzuleiten. Die Aufsicht gemäss Art. 41 BÜPF erscheint in dieser Hinsicht unzureichend.
Art. 19	Einfügen eines zusätzlichen Absatzes: Verpflichtung Dienst ÜPF zur Einleitung entsprechender Abklärungen und Ergreifung geeigneter Massnahmen, wenn Identifikationspflichten nicht oder nur ungenügend nachgekommen wird.	Der Dienst ÜPF ist zwingend zu verpflichten, entsprechende Abklärungen vorzunehmen und bei Bestätigung von ungenügenden oder nicht vorgenommenen Identifikationspflichten geeignete Massnahmen zu ergreifen, den Missstand zu beheben. In der Praxis ergeben sich zahlreiche Anzeichen sowie konkrete Missstände, dass den Registrierungspflichten durch zahlreiche Dienstleister mindestens ungenügend nachgekommen wird. Die Aufsicht gemäss Art. 41 BÜPF erscheint in dieser Hinsicht unzureichend. Das bisherige Untätigbleiben des Dienstes ÜPF sollte demnach in einen gesetzlichen Auftrag überführt werden.
Art. 20	Einfügen eines zusätzlichen Absatzes:	Der Dienst ÜPF ist zu verpflichten, entsprechende Abklärungen vorzunehmen und bei Bestätigung von ungenügenden



	<p>Verpflichtung Dienst ÜPF zur Einleitung entsprechender Abklärungen und Ergreifung geeigneter Massnahmen, wenn der Überprüfungspflicht nicht oder nur ungenügend nachgekommen wird.</p>	<p>oder nicht vorgenommenen Überprüfungspflichten geeignete Massnahmen zu ergreifen, den Missstand zu beheben. In der Praxis ergeben sich zahlreiche Anzeichen sowie konkrete Missstände, dass den Registrierungspflichten durch zahlreiche Dienstleister mindestens ungenügend nachgekommen wird. Die Aufsicht gemäss Art. 41 BÜPF erscheint in dieser Hinsicht unzureichend. Das bisherige Untätigbleiben des Dienstes UEPF sollte demnach in einen gesetzlichen Auftrag überführt werden.</p>
Art. 48b Abs. 2	<p>Streichung des neu aufgenommenen Einschubs («<i>und soweit für die eindeutige Bestimmung des jeweiligen permanenten Identifikator notwendig</i>») sowie auch die Verpflichtung zur Präzisierung im bestehenden Abs. 2. Stattdessen ist festzuhalten, dass das Auskunftsge- suech keine Präzisierung der standortbezogenen Angaben beinhalten muss.</p>	<p>Dieser Absatz hält fest, dass das Auskunftsgesuch die angefragten temporären Identifikatoren (z. B. SUCI, 5G-GUTI) und, soweit für die eindeutige Bestimmung des jeweiligen permanenten Identifikators notwendig, standortbezogene Angaben wie das zugehörige Mobilfunkgebiet, präzisiert. Gemäss dem erläuternden Bericht (S. 41) ist die Angabe des genannten Mobilfunkgebietes (Tracking Area) optional. Zwingend erforderlich ist diese Angabe hingegen im Fall einer Mehrfachverwendung einer angefragten SUCI. Die ersuchende Behörde weiss allerdings zum Zeitpunkt des Auskunftsgesuchs nicht, ob eine Mehrfachverwendung einer SUCI vorliegt. Deshalb soll die FDA sicherstellen, dass keine Mehrfachverwendung des temporären Identifikators (z. B. SUCI, 5G-GUTI) vorkommt. Zudem ist nicht definiert, was im Fall einer Mehrfachverwendung einer angefragten SUCI im Mobilfunknetz als Antwort geliefert wird, wenn das Mobilfunkgebiet (Tracking Area) nicht im Auskunftsersuchen vorhanden war.</p>
Art. 50 Abs. 9	Klärung bzw. Präzisierung vornehmen.	Es ist nicht klar verständlich, wie die Präzisierung in Abs. 9 in der Praxis umgesetzt werden soll. Bei einer aktiven Überwachung ist die Anordnung im WMC bereits abgeschlossen und beim Hinzukommen eines neuen Endgerätes (Multi-Device) oder einer neuen SIM (Extra-SIM) hat eine zusätzliche Anordnung zu erfolgen. Dies wird nun aber mit dem Zusatz «im Rahmen desselben Auftrages» ausgeschlossen.



Art. 60a	<p>Dieser neue Überwachungstyp ist zu streichen und die Auskunft im Rahmen von Art. 38a zu beantworten.</p>	<p>Aus Art. 60a Abs. 2 ergibt sich, dass die zu liefernden Angaben zu diesem Überwachungstyp gemäss Bst. a und b Bestandesdaten analog des Auskunftstyps IR_58_IP_INTERSECT (Art. 38a) sind. Es ist deshalb nicht nachvollziehbar, weshalb es sich um eine Überwachung handeln soll und demzufolge einer Genehmigung des Zwangsmassnahmengerichts bedarf.</p> <p>Allfällige gelieferte Mehrfachergebnisse sind durch die Strafbehörden ohnehin zu analysieren. Entgegen der Botschaft ist nach hier vertretener Auffassung die allfällige Ausleitung von mehreren Ergebnissen (unabhängig der Anzahl) nicht mit einem Antennensuchlauf vergleichbar, da beim Antennensuchlauf rückwirkende Randdaten ausgeleitet werden, vorliegend aber Bestandesdaten zur Verfügung gestellt werden. Die Eingriffstiefe ist ungleich, weshalb die Bestandesdaten im Rahmen der Auskunft erteilt werden kann und ein neuer Überwachungstyp nicht notwendig ist.</p>
----------	-------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Hôtel du Gouvernement – 2, rue de l'Hôpital, 2800 Delémont

Département fédéral de justice et police DFJP
Monsieur le Conseiller fédéral
Beat Jans
Palais fédéral ouest
3003 Berne

Hôtel du Gouvernement
2, rue de l'Hôpital
CH-2800 Delémont
t +41 32 420 51 11
f +41 32 420 72 01
chancellerie@jura.ch

Par email : ptss-aemterkonsultationen@isc-ejpd.admin.ch

Delémont, le 29 avril 2025

Révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication - consultation

Monsieur le Conseiller fédéral,

Le Gouvernement de la République et Canton du Jura accuse réception de votre courrier relatif à la procédure de consultation susmentionnée et il vous remercie de l'avoir consulté.

Il n'a dans ce cadre aucune remarque à formuler.

Tout en vous remerciant de prendre note de ce qui précède, le Gouvernement de la République et Canton du Jura vous prie de croire, Monsieur le Conseiller fédéral, à sa haute considération.

AU NOM DU GOUVERNEMENT DE LA
RÉPUBLIQUE ET CANTON DU JURA


Martial Courtet
Président




Jean-Baptiste Maître
Chancelier d'État



LE CONSEIL D'ÉTAT

DE LA RÉPUBLIQUE ET
CANTON DE NEUCHÂTEL

Département fédéral de justice et police
(DFJP)
Palais fédéral
3003 Berne

Révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT) : ouverture de la procédure de consultation

Monsieur le conseiller fédéral,

Nous vous remercions de nous avoir consultés sur la révision partielle de l'OSCPT. La présente prise de position se concentre principalement sur les incidences économiques du projet pour le tissu industriel et numérique cantonal.

Le Canton de Neuchâtel soutient les objectifs de sécurité publique poursuivis par la révision de l'OSCPT et encourage la Confédération à poursuivre ces efforts, tout en veillant à ajuster les mesures proposées — notamment envisager le relèvement du seuil d'assujettissement, étudier la limitation de l'obligation de déchiffrement et l'introduction d'un mécanisme d'indemnisation — afin de préserver un environnement favorable à l'émergence de nouveaux acteurs et au dynamisme entrepreneurial du secteur numérique et de la confidentialité des données en Suisse.

Pour y parvenir, le Conseil d'État recommande les actions suivantes :

1. Relèvement du seuil d'assujettissement : le seuil de 5000 usagers nous paraît bas, aucun élément tangible ne nous permet de proposer un seuil plus adapté, il pourrait être intéressant de le relever ou de le combiner avec un chiffre d'affaires minimum afin de protéger l'innovation émergente.
2. Précision à l'art. 50a : tenir compte des sociétés dont l'architecture ne permet pas de décrypter les données et par exemple limiter l'obligation de déchiffrement aux cas où l'opérateur détient effectivement la clé privée, garantissant la viabilité des services à chiffrement bout en bout.
3. Mécanisme d'indemnisation : instaurer une prise en charge proportionnée des coûts de mise en conformité pour les FSCD de moins de 250 EPT par exemple.
4. Analyse d'impact indépendante : réaliser avant l'entrée en vigueur une étude sectorielle quantifiant les charges pour les PME et l'effet sur l'attrait du site suisse.



Par ailleurs, le Canton de Neuchâtel félicite l'initiative visant à améliorer les définitions des catégories de POC, en particulier, celles des FST et des FSCD, afin de permettre aux fournisseurs de comprendre facilement de laquelle de ces catégories ils relèvent. L'introduction de nouvelles mesures de surveillance est également saluée, dès lors que celles-ci limitent la quantité de données nécessaires qui vont être traitées, analysées et sauvegardées, permettant ainsi aux autorités compétentes, notamment la police, de gagner en efficience, en supprimant directement ce qui n'est pas pertinent pour l'enquête.

Quant aux conséquences financières, il est relevé que, malgré le fait que ces nouveautés vont engendrer des dépenses supplémentaires (ex. nouvelles procédures, nouveaux serveurs, etc.), cela ne devrait pas engendrer des coûts supplémentaires pour les cantons, puisque la problématique du financement déjà relevée en 2023 lors de la procédure de consultation est toujours actuelle et n'a toujours pas trouvé de solution satisfaisante.

En vous remerciant encore de nous avoir consultés, nous vous prions de croire, Monsieur le conseiller fédéral, à l'assurance de notre très haute considération.

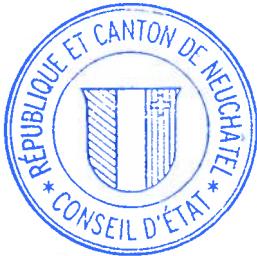
Neuchâtel, le 5 mai 2025

Au nom du Conseil d'État :

*La présidente,
F. MATER*



*La chancelière,
S. DESPLAND*



Regierungsrat

Rathaus
Barfüssergasse 24
4509 Solothurn
so.ch

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesrat Beat Jans
Bundeshaus West
3003 Bern

Per E-Mail an:
ptss-aemterkonsultationen@isc-ejpd.admin.ch

5. Mai 2025

Vernehmlassung zu den Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar 2025 haben Sie uns eingeladen, zu den Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) Stellung zu nehmen. Wir bedanken uns für die Gelegenheit, uns zur Angelegenheit äussern zu können.

Wir begrüssen die Vorlage grundsätzlich. Neben zahlreichen redaktionellen Anpassungen stehen zwei Aspekte im Zentrum der Vorlage. Einerseits die neue Organisation der Mitwirkungspflichtigen (MWP), wobei insbesondere betreffend Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD) neue Unterkategorien eingeführt werden und andererseits die Schaffung neuer Auskunfts- und Überwachungstypen.

Die nachfolgenden Hinweise und beantragten Anpassungen einzelner Bestimmungen stützen sich auf die Einschätzung erfahrener Fachspezialisten, welche die vorgeschlagenen Änderungen dieses hoch technischen und komplexen Regelungsgegenstands im Hinblick auf die Praxis beurteilt haben.

Zu den einzelnen Punkten:

1. Regelung der Mitwirkungspflichten – Definition AAKD

In den Art. 16d ff. der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) sollen unter anderem Anbieterinnen von Diensten geregelt werden, die sich auf Fernmelddienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen [Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD) gemäss Art. 2 lit. c des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)]. Diesen AAKD obliegt gemäss Art. 2 BÜPF Mitwirkungspflicht im Bereich der Überwachung des Post- und Fernmeldeverkehrs.

Die im Vernehmlassungsentwurf vorgeschlagene Regelung ist aus Sicht der Anbieterinnen zwar nachvollziehbar, jedoch aus Sicht der Strafverfolgungsbehörden und der Polizei (Gefahrenabwehr) unbefriedigend. Es ist zu beachten, dass durch die fehlende Erreichbarkeit bei reduzierten und minimalen Mitwirkungspflichten (MWP) erhebliche Überwachungslücken entstehen können. Dadurch kann es in dringenden Fällen dazu führen, dass Teilnehmende nicht rechtzeitig

identifiziert werden können. Dies kann insbesondere bei schweren Straftaten und akuten Gefahrenlagen – wie Entführungen, Erpressungen oder terroristischen Bedrohungen, aber auch bei Vermisstensuchen – gravierende Folgen haben.

Muss etwa eine Anbieterin ohne Pikettpflicht kontaktiert werden, bleibt eine Anfrage unter Umständen tagelang unbeantwortet – was die Strafverfolgung nicht nur behindert, sondern unter Umständen sogar verhindert. Unerheblich ist in diesem Zusammenhang das Argument, dass kleine Anbieterinnen nur wenige Kunden haben. Erstens summiert sich die Zahl der Kunden der einzelnen kleinen Anbieterinnen. Zweitens ist davon auszugehen, dass sich insbesondere Personen aus kriminellen Strukturen auf Anbieter mit reduzierten oder minimalen Pflichten konzentrieren werden. Drittens orientieren sich die Herausforderungen der Staatsanwaltschaft und der Polizei im Rahmen der Strafverfolgung und Gefahrenabwehr nicht am Grad der Mitwirkungspflichten der Anbieterinnen.

Wie effizient und effektiv Menschenleben geschützt werden können, sollte nicht von den Anbieterinnen abhängen.

Deshalb regen wir an, von reduzierten oder minimalen Mitwirkungspflichten für kleine Anbieterinnen abzusehen und beispielsweise eine Pikettpflicht für sämtliche MWP einzuführen.

2. Teilnehmer- und Benutzeridentifikation (Art. 19ff. VÜPF)

Schweizweit besteht ein Problem mit falschregistrierten Mobiltelefonnummern. Diese Nummern werden häufig als Tatmittel in der organisierten Kriminalität verwendet.

Die Identifikationspflicht ist vorliegend zu wenig konkret und birgt mit den heutigen technischen Möglichkeiten (Stichwort KI) ein erhebliches Missbrauchspotenzial.

Aus dem Grund regen wir an, die Identifikationsmöglichkeiten zu konkretisieren, eine abschliessende Definition der zu erhebenden Adressierungselemente vorzunehmen und eine Online-Registrierung erst dann zuzulassen, wenn verbesserte Sicherheitsstandards eingeführt wurden.

3. Regelung der Auskunftstypen

Neu soll in Art. 38 a VÜPF der Auskunftstyp k IR_58_IP_INTERSECT. Benutzeridentifikation durch Schnittmengenbildung eingeführt werden. Es ist zu begrüssen, dass mit der Einführung der neuen Auskunftstypen IR_58_IP_INTERSECT und HD_62_IP eine bisherige Überwachungslücke geschlossen wird. Insbesondere wurde die bisher problematische Situation behoben, bei der bei Anfragen zu NAT-Übersetzungen mehrere Kunden betroffen sein könnten, was zur Verweigerung der Auskunft führte. Diese Anpassung ist aus Sicht der Strafverfolgung ein bedeutender Fortschritt.

Allerdings entspricht es nicht den Anforderungen an eine effektive Gefahrenabwehr, dass der neue Auskunftstyp IR_58_IP_INTERSECT als nicht pikettpflichtig eingeführt wird. Damit bleibt eine Überwachungslücke bestehen, ohne den realen Bedarf zu berücksichtigen. Eine Pikettpflicht ist aufgrund derselben Ausführungen wie unter Ziffer 1 auch für diesen Auskunftstyp aus Sicht der Strafverfolgung unumgänglich. Zudem sollen die in Abs. 3 lit. b Ziff. 1-3 genannten Verbindungsparameter als fakultative Informationen deklariert werden. Dies ist insbesondere in Fällen wichtig, in denen einzelne Parameter lediglich bei einer bestimmten Verbindung vorliegen, während bei weiteren Verbindungen diese Parameter nicht bekannt sind, was eine Auskunft verhindern würde. Der Sinn und Zweck solch einer Abfrage gründet gerade darin, dass nicht sämtliche Daten vorliegen.

Weiteren Anpassungsbedarf erkennen wir bei Art. 48b Abs. 1 VÜPF, welcher gemäss Vorentwurf unverändert bleibt. Gemäss Abs. 1 müssen heute bei einer Lokalisierung und insbesondere bei Notsuchen jeweils alle temporären Identifikatoren abgefragt werden. Da diese Abfrage in der Praxis wiederkehrend erfolgen muss, würden solche Abfragen jedoch die Datenbandbreite über die Mobilfunkstelle jeweils stark auslasten.

Damit künftig nicht mehr wiederholt sämtliche temporären Identifikatoren im Rahmen einer Lokalisierung, insbesondere bei Notsuchen, angefragt werden müssen, sollte nach unserer Ansicht der jeweilige temporäre Identifikator des gesuchten Mobilfunkgeräts künftig automatisch und in Echtzeit geliefert werden, ohne dass eine erneute Anfrage erforderlich ist. Damit würde die Datenbandbreite über die Mobilfunk-Luftschnittstelle zwischen dem technischen Gerät (IMSI-Catcher) und der Mobilfunknetzbetreiberin erheblich reduziert. Dies ist insbesondere von Bedeutung, da Notsuchen häufig in Gebieten mit eingeschränkter Mobilfunkversorgung stattfinden, in denen nur eine geringe Datenbandbreite für die Übertragung zur Verfügung steht.

Deshalb regen wir an, Art. 48b Abs. 1 VÜPF wie folgt zu ändern:

Art. 48b Abs. 1

Bei der Lokalisierung, insbesondere der Notsuche, wird ohne Nachfrage der jeweilige aktuelle temporäre Identifikator des gesuchten Mobilfunkgerätes geliefert.

Art. 48b Abs. 2 VÜPF hält fest, dass das Auskunftsgesuch die angefragten temporären Identifikatoren (z.B. SUCI, 5G-GUTI) und, soweit für die eindeutige Bestimmung des jeweiligen permanenten Identifikators notwendig, standortbezogene Angaben, wie das zugehörige Mobilfunkgebiet, präzisieren muss. Gemäss dem erläuternden Bericht (S. 41) sei die Angabe des genannten Mobilfunkgebietes (Tracking Area) optional. Zwingend erforderlich sei die entsprechende Angabe hingegen im Fall einer Mehrfachverwendung einer angefragten SUCI. Hierzu gilt es festzuhalten, dass die ersuchende Behörde zum Zeitpunkt des Auskunftsgesuchs nicht weiß bzw. nicht wissen kann, ob eine Mehrfachverwendung einer SUCI vorliegt. Deshalb sollen die Anbieterinnen von Fernmeldediensten (FDA) sicherstellen, dass keine Mehrfachverwendung des temporären Identifikators (z.B. SUCI, 5G-GUTI) vorkommt. Darüber hinaus ist in der derzeitigen Vorlage nicht definiert, was im Fall einer Mehrfachverwendung einer angefragten SUCI im Mobilfunknetz als Antwort geliefert wird, wenn das Mobilfunkgebiet (Tracking Area) nicht im Auskunftsersuchen vorhanden war.

Entsprechend beantragen wir, sowohl den neu aufgenommenen Einschub (*«und soweit für die eindeutige Bestimmung des jeweiligen permanenten Identifikators notwendig»*) sowie auch die bereits bestehende Verpflichtung zur Präzisierung in Abs. 2 aufzuheben und stattdessen festzuhalten, dass das Auskunftsgesuch keine Präzisierung der standortbezogenen Angaben zu enthalten hat. Sollte dies aus technischer Sicht nicht möglich sein, müssen sämtliche Teilnehmer, die dieselben temporären Identifikatoren verwenden, zurückgemeldet werden.

4. Art. 50 Abs. 9 VÜPF

Zuletzt ist uns aufgrund der bestehenden Vorlage unklar, wie die Präzisierung in Art. 50 Abs. 9 VÜPF in der Praxis umgesetzt werden soll. Bei einer aktiven Überwachung ist die Anordnung bereits abgeschlossen, sodass beim Hinzukommen eines neuen Endgerätes (Multi-Device) oder einer neuen SIM (Extra-SIM) eine zusätzliche Anordnung erforderlich wird. In der Vorlage wird jedoch eine solche zusätzliche Anordnung mit dem Zusatz *«im Rahmen desselben Auftrages»* gemäss Wortlaut ausgeschlossen. Vor diesem Hintergrund ersuchen wir um Klärung, wie dieser Zusatz zu verstehen ist und welche Auswirkungen er auf das entsprechende Anordnungsverfahren hat.

Besten Dank für die Berücksichtigung unserer Anliegen.

IM NAMEN DES REGIERUNGSRATES

sig.
Sandra Kolly
Frau Landammann

sig.
Andreas Eng
Staatsschreiber

Kanton Schaffhausen

Finanzdepartement

J. J. Wepfer-Strasse 6

CH-8200 Schaffhausen

www.sh.ch

T +41 52 632 72 50

cornelia.stammhurter@sh.ch



Finanzdepartement

Eidgenössisches Justiz- und
Polizeidepartement EJPD

per E-Mail:

ptss-aemterkonsultationen@isc-
ejpd.admin.ch

Schaffhausen, 6. Mai 2025

**Vernehmlassung betreffend Teilrevisionen zweier Ausführungserlasse zur Überwachung
des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF); Stellungnahme**

Sehr geehrter Herr Bundesrat

Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar 2025 haben Sie uns eingeladen, in vorerwähnter Angelegenheit
Stellung zu nehmen. Wir danken Ihnen für diese Gelegenheit.

Der Kanton Schaffhausen stimmt unter Verweis auf die Vernehmlassung der KKPKS vom 2. Mai
2025, der er sich anschliesst, der Vorlage zu und hat keine weiteren Bemerkungen.

Wir danken Ihnen für die Kenntnisnahme und die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

Finanzdepartement

Dr. Cornelia Stamm Hurter
Regierungsrätin



Regierungsrat

Postgasse 68
Postfach
3000 Bern 8
info.regierungsrat@be.ch
www.be.ch/rr

Staatskanzlei, Postfach, 3000 Bern 8

Eidgenössisches Justiz- und Polizeidepartement EJPD

Per E-Mail (in Word & PDF) an:
ptss-aemterkonsultationen@isc-eipd.admin.ch

RRB Nr.: 407/2025 30. April 2025
Direktion: Sicherheitsdirektion
Klassifizierung: Nicht klassifiziert

Vernehmlassung des Bundes: EJPĐ: Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Der Regierungsrat dankt Ihnen für die Gelegenheit zur Stellungnahme. Die Anträge sowie die entsprechenden Begründungen des Kantons Bern bezüglich der zwei Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) finden Sie nachfolgend.¹

1. Anträge und Begründungen

1.1 VÜPF

1.1.1 Art. 20a Abs. 1 Bst. d (neu)

Antrag:

«Bei natürlichen Personen muss der Identitätsnachweis (...) durch Vorzeigen eines der folgenden, am Erfassungstag gültigen Dokumente erbracht werden»

Der Begriff «Vorzeigen» eines der aufgeführten und am Erfassungstag gültigen Dokuments muss näher definiert werden.

Begründung:

Der Identitätsnachweis kann heute auch online via dafür vorgesehene Apps durchgeführt werden.

Diesbezüglich stellen wir eine massive Zunahme von Falschregistrationen fest, welche mittels gefälschter Ausweise durchgeführt werden. Bei der Fälschung von Ausweisen gemäss Art. 252 StGB handelt es sich um ein Vergehen. Angesichts der Quantität und Qualität der Gesetzesverstösse bleibt die Verhältnismässigkeit der Massnahme insgesamt gewahrt. Die Vorschriften betreffend die Teilnehmer- und Benutzeridentifikation via App müssen daher zwingend und dringend angepasst werden.

Eine Anpassung könnte beispielsweise erfolgen durch:

- einen Überprüfungsmechanismus seitens Anbieterinnen von Fernmeldediensten (FDA), welcher Online-Registrationen unterschiedlicher Ausweisdokumente mit demselben Passfoto erkennt und entsprechend blockiert.
- die Speicherung der Verbindungsdaten zwischen dem Endgerät des Benutzers und den Servern der FDA während des Registrationsprozesses (IP-Adresse, Port, Protokoll, Zeitstempel).
- die Speicherung sämtlicher Fotos und Videos vom Endkunden, welche im Zuge der Registration mit einer App an die FDA übermittelt werden.

1.1.2 Art. 38 Abs. 3 (neu)

Antrag:

Angaben zur eindeutigen Benutzeridentifikation bei IP-Adressen mit sog. Netzwerkadressüberersetzung (NAT):

«Wenn die Angaben (...) geeignet sind, eine eindeutige Identifikation zu ermöglichen, ist die Lieferung von Mehrfachergebnissen zulässig. »

Im Zusammenhang mit der Benutzeridentifikation bei IP-Adressen muss der Begriff «Mehrfa-
chergebnisse» näher definiert werden.

Begründung:

Gemäss erläuterndem Bericht soll es nicht möglich sein, eine diesbezügliche Obergrenze an Ergebnissen festzulegen, was jedoch nicht nachvollziehbar ist.

Wird eine Obergrenze für die Anzahl Ergebnisse definiert, so muss der Provider die Daten bis hin zu dieser Grenze, sofern vorhanden, auch liefern. Ist jedoch *keine* Obergrenze festgelegt, so könnte ein Provider theoretisch alle Auskunftsfragen zurückweisen, welche mehr als ein Ergebnis liefern.

Dies würde dann dazu führen, dass die Behörden auf den neuen rückwirkenden Überwachungstyp HD_62_IP zurückgreifen müssen, was eine Anordnung durch die Staatsanwaltschaft und Genehmigung durch das Zwangsmassnahmengericht voraussetzt.

1.1.3 Art. 38a Abs. 3 Bst. b

Antrag:

«Das Auskunftsgesuch enthält die folgenden Angaben über jede der angefragten Internetverbindungen:

(...)

b. falls für die Identifikation notwendig:

1. die öffentliche Quell-Portnummer,
2. die öffentliche Ziel-IP-Adresse,
3. die Ziel-Portnummer, (...) »

Es werden zwei Optionen zur Anpassung vorgeschlagen:

Option A: Entfernen der oben dargelegten Ziffern 1 bis 3.

Option B: Ersetzen des Wortlautes «falls für die Identifikation notwendig» durch «falls bekannt».

Begründung:

Wenn aufgrund von fehlenden Parametern – dazu zählen insbesondere jene der Ziffern 1 bis 3 – der Auskunftstyp IR_8_IP (NAT) zum Zweck der Benutzeridentifikation bei IP-Adressen nicht beauftragt werden kann, so werden grundsätzlich sog. Schnittmengen-Analysen durchgeführt.

Bei Abs. 3 handelt es sich um eine sogenannte MUSS-Formulierung. Die FDA könnte folglich bei jeder Anfrage auf die Bekanntgabe der Parameter nach Bst. b bestehen, welche der anfragenden Behörde eben gerade nicht in jedem Fall bekannt sind. Vor diesem Hintergrund macht die Auflistung der Ziffern 1 bis 3 keinen Sinn.

1.1.4 Art. 38a Abs. 4

Antrag:

Der Auskunftstyp IR_58_IP_INTERSECT nach Art. 38a wird geschaffen, um die Identifikation der Benutzenden, der Urheberschaft oder der Herkunft von Internetverbindungen zu verbessern. In Abs. 4 wird präzisiert, dass die MWP Angaben zu Benutzenden, zur Urheberschaft oder zur Herkunft der Internetverbindungen nur dann liefert, wenn genau ein Ergebnis vorhanden ist. Falls mehr als ein Ergebnis vorhanden ist, wird nur mitgeteilt, dass mehr als ein Ergebnis vorhanden ist.

Entgegen der Vorlage sollen Mehrfachergebnisse analog zu Art. 38 Abs. 3 ebenfalls geliefert werden müssen.

Begründung:

Es ist nicht nachvollziehbar, weshalb hier nur genau ein Ergebnis geliefert wird, während Art. 38 Abs. 3 Mehrfachergebnisse zulässt. Der Inhalt beider Auskünfte ist identisch und beschränkt sich auf Bestandesdaten (keine Randdaten).

Die Verantwortung über das weitere Vorgehen obliegt danach der ermittelnden Strafbehörde, indem diese Mehrfachergebnisse mit den bereits getätigten Ermittlungen abgeglichen werden. Im Zweifelsfalle werden Mehrfachergebnisse verworfen.

1.1.5 Art. 60 Bst. g

Antrag:

Bei Mobilfunkdiensten sind die Standortangaben aus NAS-Signalisierungsnachrichten zu übermitteln. Es bedarf der Präzisierung im erläuternden Bericht, dass die Lieferung von Standortangaben aus NAS-Signalisierungsnachrichten *zwingend* ist, sofern diese Daten vorhanden sind.

Begründung:

In der Vernehmlassungsvorlage wird die Lieferung der Standortangaben aus NAS-Signalisierungsnachrichten als verpflichtend definiert. Im erläuternden Bericht wird jedoch erwähnt, dass die FDA solche Daten liefern „kann“.

1.1.6 Art. 64

Antrag:

Analyse der Netzabdeckung in Vorbereitung eines Antennensuchlaufs.

Art. 64 soll nicht aufgehoben werden.

Begründung:

Die Strafverfolgungsbehörden beziehen diese Dienstleistung aktuell über andere Kanäle.

Es ist jedoch nicht ausgeschlossen, dass der aktuelle Anbieter diese Dienstleistung dereinst nicht mehr zur Verfügung stellt. Und vor diesem Hintergrund soll Art. 64 bestehen bleiben.

1.1.7 Art. 65

Antrag:

In Vorbereitung eines Antennensuchlaufs: Referenzkommunikationen oder Referenznetzzügänge.

Art. 65 soll nicht aufgehoben werden

Begründung:

Siehe Begründung zu Art. 64. Vor diesem Hintergrund soll auch Art. 65 bestehen bleiben.

1.2 VD-ÜPF

1.2.1 Art. 14

Antrag:

Der Auskunftstyp IR_58_IP_INTERSECT nach Art. 38a VÜPF wird geschaffen, um die Identifikation der Benutzenden, der Urheberschaft oder der Herkunft von Internetverbindungen zu verbessern.

Der Auskunftstyp IR_58_IP_INTERSECT nach Art. 38a VÜPF soll zusätzlich im Rahmen einer Pikettpflicht auch an Feiertagen angeboten werden.

Begründung:

Eine mögliche Anwendung soll im Rahmen von Notsuchen oder schweren Delikten erfolgen.

2. Weitere Bemerkungen

Im Begleitschreiben zur Eröffnung der Vernehmlassung bitten Sie um Angabe einer Kontaktperson für Rückfragen. Für inhaltliche Rückfragen verweist der Regierungsrat auf die Kantonspolizei Bern: Herr Adrian Nyffeler, Chef Spezialfahndung 2 (031 638 55 27, pnff@police.be.ch).

Der Regierungsrat dankt Ihnen für die Berücksichtigung seiner Anliegen.

Freundliche Grüsse

Im Namen des Regierungsrates



Evi Allemann
Regierungspräsidentin



Christoph Auer
Staatsschreiber

Verteiler

- Datenschutzaufsichtsstelle des Kantons Bern
- Justizverwaltungsleitung
- Sicherheitsdirektion

FDP.Die Liberalen, Postfach, 3001 Bern

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Bern, 25. April 2025 / HG
VL VÜPF VD-ÜPF

Elektronischer Versand: ptss-aemterkonsultationen@isc-eipd.admin.ch

**Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)
Vernehmlassungsantwort der FDP.Die Liberalen**

Sehr geehrte Damen und Herren

Für Ihre Einladung zur Vernehmlassung oben genannter Vorlage danken wir Ihnen. Gerne geben wir Ihnen im Folgenden von unserer Position Kenntnis.

Die FDP.Die Liberalen lehnt die Teilrevisionen der zwei Ausführerlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) vollständig ab.

Die Anpassungen würden die Standortbedingungen für Schweizer Unternehmen mit Internetdiensten massiv verschlechtern. Die diesen durch die Revisionen neu auferlegten Mitwirkungspflichten haben mehrere, scharf einschneidende Konsequenzen. Die Pflichten widersprechen dabei den internationalen Standards, dem Geschäftsmodell diverser schweizerischer Unternehmen, den Grundsätzen der digitalen Welt und greifen in die Privatsphäre und Grundrechte der Nutzer ein.

Grundlegend gehen die Revisionen über die gesetzliche Grundlage hinaus. Das zugrundeliegende BÜPF regelt, wann eine Institution Mitwirkungspflichten erfüllen muss. Dabei bezieht sich dies auf einen geleisteten Dienst und nicht auf Unternehmen ab einem bestimmten Umsatz. Dass mit dem VÜPF Kategorisierungen mithilfe des Gesamtumsatzes vorgenommen werden, ist daher nicht gesetzeskonform.

In vergangenen Diskussionen über die Mitwirkungspflichten spielte die Verhältnismässigkeit eine wichtige Rolle. Durch die neuen Einteilungen von AAKD würden diese bei 5000 Nutzer beginnen. Die AAKD müssten beim Überschreiten dieser Schwelle dies selbstständig melden. Damit wären nahezu jegliche Cloud- und Filesharing-Anbieter, App-Entwickler und innovative Unternehmen in der Schweiz hiervon betroffen. Dies entspricht nicht der Verhältnismässigkeit. Da sich dies gleichzeitig nur auf Unternehmen mit schweizerischen Niederlassungen bezieht, wären vor allem schweizerische Anbieter hiervon betroffen.

Für die Umsetzung der Mitwirkungspflichten müssten die betroffenen AAKD ihre technische Infrastruktur für die Aufbewahrung von sogenannten Randdaten massiv ausbauen. Dies würde zu sehr umfangreichen jährlichen Zusatzkosten führen. Damit wären die Unternehmen im internationalen Umfeld, das keine so strengen Pflichten kennt, nicht mehr wettbewerbsfähig.

auf Privatsphäre und den Schutz personenbezogener Daten eingreifen. Die Schweiz geht mit den vorgeschlagenen Teilrevisionen einen eigenen, diesem Entscheid widersprüchlichen Weg.

Dieses Swiss Finish auf wirtschaftlicher und rechtlicher Ebene würde die betroffenen Unternehmen aus der Schweiz drängen und die hiesige Wirtschaft sowie den Standort für digital orientierte Unternehmen schwächen. Damit würde die Revision das Gegenteil ihres eigentlichen Ziels bezwecken: Der Zugriff auf sicherheitsrelevante Daten – der bereits im geltenden Rechtsrahmen möglich ist und durch die Kooperation der Unternehmen unterstützt wird – wäre durch das Abwandern der Unternehmen gebrochen. Damit schwächt die Schweiz sich als Unternehmensstandort, aber auch ihre Stellung bei anderen Staaten und Geheimdiensten im Kampf gegen internationale Kriminalität.

Die vorgeschlagenen Revisionen führen schlussendlich auch zu einem signifikanten Eingriff in die Privatsphäre und Grundrechte der Nutzer. Durch die mittelfristige Aufbewahrung von Primär- und Sekundärdaten über 6 Monate entstehen für die Millionen betroffenen Kundenkonten in der Schweiz immense Cyber-Risiken, die wiederum die Schweiz als digitalen Standort schwächen, anstatt stärken.

Die FDP.Die Liberalen lehnt aus diesen Gründen, die staats- und grundrechtlicher, wirtschaftliche und praktische Bedenken umfassen, die vorgeschlagenen Teilrevisionen der VÜPF und VD-ÜPF vollständig ab.

Wir danken Ihnen, sehr geehrte Damen und Herren, für die Gelegenheit zur Stellungnahme und für die Berücksichtigung unserer Überlegungen.

Freundliche Grüsse

FDP.Die Liberalen

Der Präsident

Thierry Burkart
Ständerat

Der Generalsekretär

Jonas Projer

Beilagen

Eidgenössisches Justiz- und Polizeidepartement EJPD
CH-3003 Bern

Elektronisch an:
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 5. Mai 2025

Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Antwort der Schweizerischen Volkspartei (SVP)

Sehr geehrte Damen und Herren

Mit der Änderung des Fernmeldegesetzes wurde auch das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) geändert. Der neue Absatz 2 ermächtigt den Bundesrat, die Kategorien von Mitwirkungspflichtigen näher zu umschreiben. Dies erfolgt im Rahmen der vorliegenden Teilrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF), mit dem Ziel, die Mitwirkungspflichten von Telekommunikationsanbieter klarer zu definieren und an die technologischen Entwicklungen anzupassen. Konkret heisst das neue Auskunfts- und Überwachungspflichten, neue operative Problemstellungen in der Umsetzung, neue technische Anpassungen sowie vereinzelt «*finanzielle und wirtschaftliche Konsequenzen*».

Die SVP lehnt die Vorlage ab, weil sie unverhältnismässig ist und vor allem ungerechtfertigt stark in die Wirtschaftsfreiheit eingreift. Die neuen Bestimmungen betreffen nämlich wortwörtlich KMU, die im Bereich der Telekommunikation tätig sind. «*Finanzielle und wirtschaftliche Konsequenzen*», auch wenn sie nur für «*Einzelne*» gelten, sind aus Sicht der SVP inakzeptabel und damit unverhältnismässig. Es steht für die SVP ausser Frage, dass den Strafverfolgungsbehörden alle notwendigen, dem technischen Fortschritt angepassten Überwachungsmöglichkeiten zur Verfügung stehen müssen - Der Entwurf begründet jedoch keinen Mehrwert und keine nachvollziehbare Güterabwägung.

Der Entwurf beansprucht, «*die Pflichten zwischen den verschiedenen Kategorien und Unterkategorien der MWP [Mitwirkungspflichtigen] besser und verhältnismässiger zu verteilen*», stellt aber selbst in Ziffer 4.3 des Berichts fest, dass der Entwurf offensichtlich das Potenzial hat, eine Reihe von KMU zu belasten, anstatt sie zu entlasten. Der Bericht versäumt es dann aber, auch nur annähernd nachvollziehbar zu begründen, warum diese negativen «*finanziellen und wirtschaftlichen Konsequenzen*» für «*Einzelne*» verhältnismässig und damit zumutbar sein sollen.

Unklar ist auch, welche Kostenfolgen die technischen Anforderungen für die Schweizer Technologieunternehmen haben werden und welche Bedeutung die neue Regelung im internationalen Wettbewerb haben wird. Auch die Bedeutung bzw. der Mehrwert für die Strafverfolgung wird nicht näher begründet.

Aus heutiger Sicht ist die Vorlage aus all diesen Gründen abzulehnen und der Bericht in den oben genannten Punkten generell zu ergänzen sowie eine Neuverteilung der Aufgaben vorzunehmen, welche auch die «*finanziellen und wirtschaftlichen Konsequenzen*» auf die einzelnen KMU berücksichtigt. Wettbewerbsnachteile für den Technologiestandort Schweiz sind nicht akzeptabel.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme und grüssen Sie freundlich.

SCHWEIZERISCHE VOLKSPARTEI

Der Parteipräsident

Der Generalsekretär



Marcel Dettling
Nationalrat



Henrique Schneider



Sozialdemokratische Partei der Schweiz / Parti Socialiste Suisse
Zentralsekretariat / Secrétariat central
Theaterplatz 4, 3011 Bern
Postfach / Case postale, 3001 Bern
Tel. 031 329 69 69 / cecile.heim@spschweiz.ch
www.spschweiz.ch / www.pssuisse.ch

Dienst Überwachung Post- und Fernmeldeverkehr
Informatik Service Center ISC-EJPD
3003 Ittigen
Per Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 30. April 2025

Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF): Stellungnahme der SP Schweiz

Sehr geehrter Herr Bundesrat,
Sehr geehrte Damen und Herren,

Besten Dank für die Einladung zur Teilnahme an der obenstehenden Vernehmlassung. Gerne unterbreiten wir Ihnen die folgende Stellungnahme.

Mit der vorliegenden Teilrevision der VÜPF werden die folgenden Kategorien von mitwirkungspflichtigen Unternehmen (MWP) näher umschrieben. Dafür werden zwei Kategorien von Anbieterinnen von Fernmeldediensten (FDA), drei Kategorien von Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD) und Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen (PZD) neu geschaffen und oder präzisiert. Zusammen mit den neuen Definitionen der FDA und AAKD, ihren jeweiligen Unterkategorien sowie der PZD in den Artikeln 16a-16h VÜPF werden auch die Bestimmungen der jeweiligen Hoch-(Upgrade) und Herunterstufung (Downgrade) der Anbieterinnen angepasst. Neu wird die Kategorie der AAKD in drei Unterkategorien unterteilt. Die FDA gliedern sich wie bisher in zwei Unterkategorien. Entsprechend werden die Pflichten und somit unter anderem die Verfügbarkeit

der Daten geändert und besser zwischen den verschiedenen Kategorien und Unterkategorien von MWP verteilt.

Die SP Schweiz anerkennt die wichtige Funktion des Dienstes Überwachung des Post- und Fernmeldeverkehrs (ÜPF) zugunsten der Strafverfolgung. Unter geltendem Recht greifen die Strafverfolgungsbehörden sowie der Nachrichtendienst bereits auf sicherheitsrelevante Daten zurück. Die geplante Verordnungsrevision geht aus Sicht der SP Schweiz jedoch zu weit. Als problematisch erachten wir folgende Punkte:

Erweiterter Geltungsbereich für FDA und AAKD

Die SP Schweiz räumt ein, dass eine Präzisierung der Definition von MWP nach dem [Bundesgerichtsentscheid im Fall Threema vs. EJPD](#) nötig ist. Jedoch scheint uns aufgrund unserer Interpretation des BÜPF diese Präzisierung nicht zwingend zu einer Ausweitung der bestehenden MWP führen zu müssen, wie es bei der vorliegenden Verordnungsrevision der Fall ist. Als besonders kritisch erachten wir, dass mit dieser Vorlage aufgrund der tiefen Schwellenwerte für die Hoch- und Herunterstufung ein deutlich erweiterter Kreis an Unternehmen als AAKD eingestuft wird, der einer deutlich umfassenderen Regulierung und erweiterten Pflichten unterworfen wird.

Die Verpflichtung zur Vorratsdatenspeicherung von sekundären Kommunikationsdaten für Anbieter von abgeleiteten Kommunikationsdiensten geht weit über entsprechende Regelungen in Europa oder anderen westlichen Ländern hinaus. Der Europäische Gerichtshof hat solche Bestrebungen immer wieder abgelehnt, es könnte auch hier zu einem Rechtsfall kommen. Das erhöht die Rechts- und Planungssicherheit der Betroffenen und führt zu einem Wettbewerbsnachteil gegenüber anderen Dienstleistern.

Schwächung des Datenschutzes und der Cybersicherheit

Besonders problematisch erachten wir den neuen Verordnungsartikel 50a, der die Anbieter dazu verpflichtet ihre Verschlüsselsysteme für Behörden jederzeit entschlüsselbar zu gestalten. Denn damit entstehen enorme Sicherheitsrisiken, die ein Schlupfloch für Hackerangriffe, Datenmissbrauch und Spionage darstellen. Zudem macht die Verpflichtung zur Sammlung von Randdaten Schweizer Unternehmen zu lukrativen Zielen krimineller Akteure. Denn die Speicherung sensibler Primär- und Sekundärdaten hunderter Millionen Kundenkonten in der Schweiz führt zu einer systemkritischen Datenmenge.

Gefährdung des Innovationsstandorts

Verschiedene Schweizer Firmen haben sich mit sicherer Kommunikation und sicherer Datenspeicherung einen internationalen Namen gemacht. Deren Geschäftsmodell ist durch diese Revision gefährdet, weil sowohl die Identifizierungspflicht wie auch die Speicherung der Randdaten dem Anspruch der Gewährleistung von Privatsphäre und sicherer Kommunikation nicht erfüllen kann. Die Ausweitung der Verpflichtungen führt zudem zu grossen

Mehrbelastungen und Kosten für KMU, was den vom Bundesrat geäusserten Zielen widerspricht.

Zusammenfassend lehnt die SP Schweiz diese Verordnungsrevision ab. Denn insbesondere in Anbetracht der geopolitischen Unsicherheiten erachtet es die SP Schweiz als zentral, die Schweiz als Kommunikations- und Technologiestandort sowie die Grundrechte der Nutzerinnen und Nutzer zu schützen.

Wir danken für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse,
SP Schweiz



Mattea Meyer
Co-Präsidentin



Cédric Wermuth
Co-Präsident



Cécile Heim
Politische Fachreferentin



GRÜNE Schweiz

Lucie Jakob

Waisenhausplatz 21

lucie.jakob@gruene.ch

031 511 93 21

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
CH-3003 Bern

Per Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 25.04.2025

Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrte Damen und Herren

Im Zusammenhang mit der im Titel genannten Vernehmlassung haben Sie die GRÜNEN zur Stellungnahme eingeladen. Wir danken Ihnen für die Einladung und äussern uns im Folgenden zu den für uns wichtigsten Punkten.

Die vorgeschlagene Teilrevision der VÜPF sowie der VD-ÜPF bewirkt das Gegenteil davon, was in der Botschaft des Bundesrates als Ziel der Vorlage definiert wurde: Weder bewirkt sie eine grössere Klarheit für Anbieterinnen im Bereich des Post- und Fernmeldeverkehrs, noch ist es ein pragmatischer Vorschlag mit wenig finanziellen Auswirkungen. Wird die Teilrevision wie vorliegend umgesetzt, bedeutet dies für viele KMU massive organisatorische, technische und finanzielle Konsequenzen. Dies, da gemäss dem Gesetzesentwurf nun beinahe alle Anbieterinnen von Kommunikationsdiensten in eine höhere Kategorie fallen würden, die ihnen strengere Pflichten auferlegt. Nicht wenige müssten ihre Dienste einstellen oder in ein anderes Land verlegen. Kleinere Open-Source und Non-Profit-Lösungen würden vom Markt verdrängt, während bestehende Monopole gestärkt werden. Die Schweiz verliert so auch ihren Ruf als IT- und Innovationsstandort.

Noch schwerer als diese formellen und finanziellen Aspekte wiegt jedoch die grossflächige Ausweitung der Überwachung, die mit der Teilrevision einhergeht. Neu wären bereits Unternehmen, die eine Dienstleistung für 5000 Nutzer*innen betreiben, einer strengerer Mitwirkungspflicht unterworfen: Sie müssten ihre Nutzer*innen mittels Speichern der IP-Adresse identifizieren können. Unternehmen, die Kommunikationsdienste mit mehr als einer

Million Nutzer*innen betreiben, wären zudem verpflichtet, während sechs Monaten die Randdaten (z.B. E-Mails, Aktivitäten, Geo-Lokalisierung) ihrer Nutzenden zu speichern. Diese enorm ausgeweitete Vorratsdatenspeicherung verunmöglicht das Betreiben von sicheren Messenger- oder Maildiensten sowie VPNs in der Schweiz, schwächt den Datenschutz und ist ein massiver Eingriff in die Privatsphäre der Nutzer*innen. Gerade für Menschenrechtsverteidiger*innen, Journalist*innen oder andere Berufsgruppen, die auf vertrauliche Kommunikationswege angewiesen sind, bedeutet die geplante Revision eine Gefährdung ihrer Arbeit. Der europäische Gerichtshof für Menschenrechte hat ähnliche Regelungen in der EU sowie davon abgeleitete Umsetzungen in Mitgliedstaaten für ungültig erklärt.¹

Gemäss erläuterndem Bericht sollen die geplanten Änderungen auch eine verbesserte Strafverfolgung sicherstellen. Allerdings wird auch dieses Ziel durch die Teilrevision der beiden Verordnungen verfehlt, da durch eine Abwanderung von Diensten wie Proton oder Threema, die bislang mit den Bundesbehörden kooperierten, ein wichtiger Zugriff auf Daten verloren gehen würde. Bereits jetzt können die Behörden die Herausgabe sicherheitsrelevanter Daten verlangen. Es ist auch fraglich, ob mehr Daten überhaupt zu mehr Ergebnissen führen würden – die Nadel im Heuhaufen ist mit noch mehr Heu nicht einfacher zu finden. Wenn überhaupt wäre der Zugriff auf wenige gezielte Daten wohl zielführender. Durch die massenhafte Speicherung von Nutzer*innendaten macht sich die Schweiz auch attraktiver für Cyberangriffe, was die öffentliche Sicherheit schwächt – und dies ausgerechnet in einer globalpolitisch sehr angespannten Zeit. Eine tatsächliche Investition in die Sicherheit wäre vielmehr der Ausbau von Verschlüsselungstechnologien.

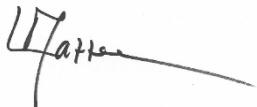
Auch nach dem Legalitätsprinzip sowie aus demokratiepolitischen Aspekten weist die Teilrevision problematische Punkte auf. Solch weitreichenden grundrechtlichen Konsequenzen müssten grundsätzlich auf Gesetzesebene geregelt werden und nicht wie vorliegend durch das Anpassen einer Verordnung. Zudem wird der gesetzliche Rahmen des BÜPF mit den vorgesehenen Änderungen überschritten, die so quasi durch die Hintertür eingeführt werden. Beispielsweise wurde in der parlamentarischen Diskussion um das BÜPF die Schranke des richterlichen Entscheids als zentrales Argument genutzt, die Teilrevision setzt diese Hürde jedoch nun praktisch ausser Kraft. Der vorliegende Entwurf ist also dahingehend auch rechtsstaatlich zweifelhaft.

Die GRÜNEN lehnen aus den oben genannten Gründen die Teilrevision der beiden Ausführungserlasse vollumfänglich ab. Diese verfehlt ihr Ziel und führt entgegen der in der Botschaft vorgebrachten Absicht weder zu mehr Klarheit noch zu einer finanziell tragbaren Lösung, sondern baut die Überwachung der Bevölkerung aus, erschwert die Arbeit von Journalist*innen, Menschenrechtsverteidiger*innen und Anwält*innen und schwächt den Datenschutz und die Sicherheit im digitalen Raum, aber auch in der Realität. Die Vorlage stellt einen massiven Eingriff in die Grundrechte der Schweizer Bevölkerung dar, insbesondere in die Privatsphäre.

¹ [Urteil](#) vom 8. April 2014, Rechtssachen C-293/12 und C-594/12 sowie [Urteil](#) vom 6. Oktober 2020, Rechtssachen C-623/17, C-511/18, C-512/18 und C-520/18.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen. Für Fragen stehen wir gerne zur Verfügung.

Freundliche Grüsse



Lisa Mazzone
Präsidentin



Lucie Jakob
Fachsekretärin

Grünlibérale Partei Schweiz
Monbijoustrasse 30, 3011 Bern

Eidgenössisches Justiz- und Polizeidepartement EJPD
3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

6. Mai 2025

Ihr Kontakt: Noëmi Emmenegger, Geschäftsführerin der Bundeshausfraktion, Tel. +41 31 311 33 03, E-Mail: schweiz@grunliberale.ch

Stellungnahme der Grünliberalen zur Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zur geplanten Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) Stellung zu beziehen. Nachfolgend finden Sie unsere Einschätzungen und Überlegungen zur Vernehmlassungsvorlage.

Kern der Revision ist eine erhebliche Verschärfung der Überwachungspflichten für KMU. Neu sollen bereits Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD) mit gerade einmal 5'000 Nutzenden strengen Überwachungspflichten unterworfen werden, indem eine neue mittlere Klasse von überwachungspflichtigen Unternehmen geschaffen wird. So sollen derartige Anbieterinnen künftig beispielsweise ihre Kunden zweifelsfrei identifizieren und Kommunikationsranddaten für sechs Monate speichern.

Die Revision widerspricht einer erst 2023 geäusserten Position des Bundesrats, gemäss der die in der noch geltenden Verordnung vorausgesetzte Kombination von mindestens 100 Millionen Umsatz *und* 5'000 Nutzern als Mittel zum Schutz der KMU dient (Bericht des Bundesrates in Erfüllung des Postulates 19.4031). Mit der Revision sollen diese Kriterien künftig getrennt betrachtet werden, sodass Unternehmen mit 5'000 Nutzenden *unabhängig von ihrem Umsatz* unter die neuen, erheblich strengereren Überwachungspflichten fallen.

Anbieterinnen abgeleiteter Kommunikationsdienste sind bereits nach geltendem Recht verpflichtet, bei Überwachungsmassnahmen des Bundes mitzuwirken, und zwar auch dann, wenn sie die beiden kumulativen Kriterien nicht erfüllen: Sie müssen insbesondere Auskünfte erteilen über Informationen, die bei ihnen vorliegen, und sie müssen dulden, dass die Überwachungsbehörden bei ihnen Überwachungsmassnahmen durchführen.

Die gesetzliche Grundlage der geplanten Unterstellung von AAKD unter strengere Überwachungspflichten, Art. 27 Abs. 3 des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs BÜPF, bleibt bei der vorliegenden Verordnungsrevision unangetastet. Das BÜPF setzt damit für eine strengere Massnahmen weiterhin eine «grosse Benutzerschaft» voraus. 5'000 Nutzende sind aber keinesfalls eine «grosse Benutzerschaft» in diesem Sinne: Es gibt im Gegenteil faktisch keine AAKD, die mit einer Nutzerbasis von nur gerade 5'000 Personen rentabel operieren können. Vielmehr ist der Markt für Internetdienstleistungen durch starke Skaleneffekte gekennzeichnet, sodass Unternehmen für einen rentablen Betrieb meist Hunderttausende, ja Millionen von Nutzenden benötigen.

Die Verordnungsrevision führt damit faktisch dazu, dass sich *sämtliche* AAKD der Schweiz plötzlich mit erheblich verschärften Überwachungspflichten konfrontiert sehen. Dies widerspricht Sinn und Geist der gesetzlichen Regelung des BÜPF, welche gerade das Ziel hat, KMU und deren Innovationskraft vor allzu schweren Eingriffen zu schützen (vgl. etwa die parlamentarische Debatte zu Art. 27 BÜPF, AB 2014 S 115 f., AB 2015 N 1155). Sie widerspricht zudem diametral der Praxis des Bundesgerichts, das AAKD vor der Einführung verschärfter Überwachungspflichten geschützt hat (Urteil vom 29. April 2021, EJPD gegen Threema GmbH).

Die Revision steht damit in klarem Widerspruch zum geltenden Recht (BÜPF), ja selbst zum revisionsauslösenden Postulat 19.4031, das explizit die Entlastung von KMU im Überwachungsbereich forderte und die nun vorgenommen Hochstufungen zu minimieren versuchte.

Die GLP lehnt die geplante Revision aus diesem Grund ab. Die geplante Verschärfung wäre rechtskonform nur durch eine (referendumspflichtige) Gesetzesrevision zu erreichen.

Abschliessend erlauben wir uns noch den Hinweis, dass wir die Gesetzgebungstechnik des Entwurfs für mangelhaft halten. Sowohl der Verordnungstext als auch der zugehörige erläuternde Bericht sind über weite Strecken verwirrend und kaum verständlich formuliert, unter anderem mit einer Vielzahl von Querverweisen, Abkürzungen, aber auch technischen Fehlern und unklaren Begrifflichkeiten. Die Texte sind in dieser Form selbst für Fachleute über weite Strecken kaum verständlich, geschweige denn als Ganzes zu überblicken. Gerade für KMU, die durch die Revision neu mit erheblich strenger Pflichten konfrontiert werden sollen, ist eine effiziente und rechtskonforme Umsetzung dieser Vorlage daher nicht zu erreichen. Das Legalitätsprinzip gemäss Art. 5 Bundesverfassung fordert vom Gesetzgeber, dass Gesetzestexte für die Adressaten verständlich formuliert sind. Die Texte der Verordnungsrevision genügen dieser Anforderung in keiner Weise. Auch aus diesem Grund lehnen wir die Revision ab.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und die Prüfung unserer Anmerkungen. Bei Fragen stehen Ihnen die Unterzeichnenden sowie unser zuständiges Fraktionsmitglied, Nationalrat Beat Flach, gerne zur Verfügung.

Mit freundlichen Grüßen



Jürg Grossen
Parteipräsident



Noëmi Emmenegger
Geschäftsführerin der Bundeshausfraktion

Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit zur eingangs erwähnten Vernehmlassung Stellung nehmen zu können.

Da diese Vorlage aufgrund der Dossieraufteilung zwischen economiesuisse und dem Schweizerischen Arbeitgeberverband von ersterem behandelt wird, verzichtet der Schweizerische Arbeitgeberverband auf eine Stellungnahme zu dieser Vernehmlassung.

Wir danken Ihnen bestens für Ihre Kenntnisnahme.

Freundliche Grüsse
Sabine Maeder

Assistentin
SCHWEIZERISCHER ARBEITGEBERVERBAND
Hegibachstrasse 47
Postfach
8032 Zürich
Tel. [REDACTED]
Direktwahl:
maeder@arbeitgeber.ch
<http://www.arbeitgeber.ch>



Von: Müggler Silvan

Gesendet: Freitag, 25. April 2025 10:35:13 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Vernehmlassung Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF): Keine Stellungnahme

Sehr geehrte Damen und Herren

Mit Ihrem Schreiben vom 29. Januar 2025 haben Sie dem Schweizerischen Gemeindeverband (SGV) das oben erwähnte Geschäft zur Vernehmlassung unterbreitet. Für die Gelegenheit, uns aus Sicht der rund 1500 dem SGV angeschlossenen Gemeinden äussern zu können, danken wir Ihnen.

Nach Studium der Unterlagen teilen wir Ihnen hiermit jedoch mit, dass der SGV zu dieser Vorlage keine Stellungnahme einreicht.

Vielen Dank für Ihre Kenntnisnahme.

Freundliche Grüsse

Silvan Müggler

Schweizerischer Gemeindeverband

Ökonom, Fachverantwortlicher Wirtschaft & Finanzen sowie Digitalisierung

Holzikofenweg 8

Postfach

3001 Bern

T: [REDACTED]

silvan.mueggler@chgemeinden.ch

<http://www.chgemeinden.ch>



SGV - Gemeinsam für starke Gemeinden

Der [**Schweizerische Gemeindeverband**](#) vertritt die Anliegen der Gemeinden auf nationaler Ebene. Er setzt sich dafür ein, dass der Gestaltungsspielraum der Gemeinden nicht weiter eingeschränkt wird. Er informiert in der «[**Schweizer Gemeinde**](#)» - [hier](#) geht es zur aktuellen Ausgabe - im Internet und an Fachtagungen über kommunalpolitisch relevante Themen und gute Praxisbeispiele. Unter den Gemeinden fördert er den Austausch, mit dem Ziel, ihre Leistungsfähigkeit zu steigern.

Von: Häusli Zoé
Gesendet: Dienstag, 6. Mai 2025 09:36:11 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: ISC-EJPD-Aemterkonsultationen ÜPF
Cc: [REDACTED]
Betreff: Réponse à la consultation: Révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT)

Madame, Monsieur,

Nous avons le plaisir de vous faire parvenir ci-joint la prise de position de l'Union suisse des arts et métiers usam concernant la consultation susmentionnée.

Meilleures salutations

Zoé Häusli

Zoé Häusli
Secrétaire / assistante politique
T: [REDACTED]
z.haeusli@sgv-usam.ch

Union suisse des arts et métiers
Schwarztorstrasse 26
Postfach
3001 Bern
www.sgv-usam.ch

Avez-vous une contribution intéressante ? Ou souhaitez-vous prendre contact avec nous via les médias sociaux ? Alors, utilisez notre hashtag et mentionnez-nous dans vos contributions sur les réseaux sociaux.

www.sgv-usam.ch/meso
<https://sgv-usam.ch/meso>





Monsieur le Conseiller fédéral Beat Jans
Département fédéral des finances
Bundesgasse 3
3003 Berne
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Berne, le 6 mai 2025 usam-MH/zh

Réponse à la procédure de consultation :

Révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT)

Monsieur le Conseiller fédéral Beat Jans,
Madame, Monsieur,

Plus grande organisation faîtière de l'économie suisse, l'Union suisse des arts et métiers usam représente plus de 230 associations et plus de 600 000 PME, soit 99,8% des entreprises de notre pays. La plus grande organisation faîtière de l'économie suisse s'engage sans répit pour l'aménagement d'un environnement économique et politique favorable au développement des petites et moyennes entreprises.

Le 29 janvier 2025, le Département fédéral de justice et police (DFJP) nous a convié à prendre position dans le cadre de la procédure de consultation sur la Révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT).

I. Contexte

L'Union suisse des arts et métiers usam a pris connaissance de la consultation relative aux révisions partielles de l'Ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT) et de l'Ordonnance sur les mesures d'exploration de la correspondance par poste et télécommunication (OME-SCPT).

La révision partielle vise à clarifier les catégories de personnes obligées de collaborer (POC), notamment les fournisseurs de services de télécommunication (FST) et les fournisseurs de services de communication dérivés (FSCD). Elle introduit trois sous-catégories pour les FSCD, au lieu de deux, afin de mieux répartir les obligations de manière proportionnée.

Des nouveaux types de renseignements et de surveillance sont créés pour répondre aux besoins des autorités de poursuite pénale, notamment pour l'identification des utilisateurs et la surveillance en temps réel ou rétroactive. Ces modifications devaient simplifier les procédures et améliorer l'efficacité de la surveillance tout en respectant les principes de proportionnalité et de protection des données.

Cette révision de deux ordonnances d'exécution, présentées comme visant à adapter les ordonnances pour les rendre plus favorables aux PME, soulèvent des préoccupations majeures quant à leur impact sur les entreprises suisses, en particulier les PME, ainsi que sur l'innovation et la compétitivité du secteur technologique en Suisse.

II. Appréciation de l'usam

L'usam rejette en bloc les révisions proposées. Bien que le Conseil fédéral ait annoncé que ces révisions visent à maintenir la charge financière des PME à un niveau bas, les modifications proposées outrepassent largement cet objectif. Elles imposent des obligations disproportionnées aux PME, remettent en question des modèles d'affaires établis et menacent la position de la Suisse en tant que lieu d'innovation technologique.

Les principales critiques de l'usam sont les suivantes :

- **Charge accrue pour les PME** : Les révisions élèvent une grande majorité des PME à un niveau d'obligations supérieur, les contraignant à participer activement et à grands frais dans des domaines où elles n'avaient jusqu'ici qu'une obligation de tolérance. Cela contredit l'objectif déclaré de maintenir la charge financière des PME à un niveau bas.
- **Menace pour les entreprises innovantes** : Les révisions remettent en question les modèles d'affaires d'entreprises suisses bien connues, comme Proton, en les obligeant à identifier leurs utilisateurs et à conserver des métadonnées pendant 6 mois. Cela pourrait contraindre ces entreprises à quitter la Suisse, portant atteinte à l'intérêt du pays pour les applications de haute sécurité exploitées localement.
- **Surveillance disproportionnée** : Les obligations de rétention de données secondaires de communication pour les fournisseurs de services de communication dérivés (FSCD) sont sans précédent en Europe et placent un fardeau excessif sur ces entreprises. Ces obligations, jugées illégales dans l'Union européenne, risquent de pénaliser gravement l'industrie technologique suisse.
- **Complexité et manque de clarté** : Le texte des révisions est structuré de manière confuse, avec de nombreuses références croisées, rendant son interprétation difficile même pour les experts. Cela crée une insécurité juridique pour les entreprises concernées, en particulier les PME.

Les révisions proposées comportent des risques considérables pour la Suisse en tant que lieu d'innovation et d'affaires. Elles ne répondent pas aux objectifs fondamentaux annoncés et menacent la réputation de la Suisse en tant que juridiction propice aux fournisseurs de technologies de l'information dignes de confiance.

Remarques spécifiques et points d'Attention

L'usam formule des propositions concrètes pour améliorer les révisions ou, le cas échéant, les rejeter. Voici une analyse détaillée des articles problématiques, reprenant l'ensemble des propositions du document initial, avec des explications développées :

OSCPT

Art. 16b, al. 1 :

Modifier l'al. 1 pour baser les critères sur le chiffre d'affaires de chaque service séparément, afin de ne pas pénaliser les entreprises innovantes qui dépassent déjà les seuils.

La formulation actuelle entrave l'innovation en obligeant les entreprises à remplir l'ensemble des obligations pour chaque nouveau service, même s'il est indépendant des autres activités. En basant les critères sur le chiffre d'affaires de l'ensemble de l'entreprise, les entreprises existantes qui dépassent

déjà les seuils ne peuvent plus lancer de nouveaux services sans devoir remplir l'ensemble des obligations, ce qui freine l'innovation et pénalise les entreprises souhaitant diversifier leurs activités.

Art. 16b, al. 1 :

Supprimer l'al. 1 let. b ch. 1.

Le seuil d'application basé sur les mandats de surveillance reçus au cours des douze derniers mois n'est pas pertinent, car il n'est pas corrélé à l'importance économique du fournisseur. De plus, il est courant que plusieurs mandats de surveillance soient émis pour une même affaire pénale, ce qui fausse la pertinence de ce critère. Il est donc préférable de se baser uniquement sur le chiffre d'affaires.

Art. 16c, al. 3 :

Supprimer l'al. 1 let. a.

La fourniture automatique d'informations élimine le contrôle humain et abaisse les obstacles à l'obtention de ces informations, ce qui augmente le risque d'utilisation abusive. De plus, la période de 12 mois pour la mise en œuvre d'un système aussi complexe est inadéquate et pourrait entraîner des déficiences techniques et juridiques. Cette obligation doit être supprimée pour éviter des abus et garantir la protection des droits fondamentaux.

Art. 16d :

Exclure les services de stockage en ligne et les VPN de cette interprétation.

L'inclusion de services de stockage en ligne comme iCloud, OneDrive ou Google Drive, souvent utilisés pour des usages privés, dépasse le cadre juridique. Ces services ne permettent pas une communication unidirectionnelle ou multidirectionnelle, comme le définit l'art. 2 lit. c LSCPT. De plus, les VPN, qui servent à rendre les utilisateurs anonymes, ne devraient pas être soumis à des obligations qui remettent en question leur fonction principale.

Art. 16g, al. 3, let. a, ch. 2 :

Supprimer l'obligation pour les FSCD de conserver les données secondaires de communication pour exécuter les surveillances rétroactives.

Cette obligation est disproportionnée, coûteuse et comporte des risques importants pour la sécurité et la vie privée des utilisateurs. Elle a également été jugée illégale dans l'Union européenne. La rétention de données pendant 6 mois demande des ressources et des investissements constants, ce qui pénalise les entreprises suisses par rapport à leurs concurrents internationaux.

Art. 16e, 16f, et 16g :

Supprimer les articles et adapter les critères existants pour que seul le chiffre d'affaires soit pertinent. Ajouter une exception pour les projets pilotes et les organisations sans but lucratif. Les critères actuels pénalisent les PME et les projets innovants, créant une insécurité juridique et entravant l'innovation. L'introduction de 5000 utilisateurs comme limite inférieure est inappropriée, car ce nombre ne constitue pas un « grand nombre d'utilisateurs » justifiant des mesures de surveillance plus strictes. De plus, l'introduction d'une unité de groupe pose des problèmes pour les entreprises ayant des sociétés associées, car tous les services et produits relèvent automatiquement du niveau le plus élevé, même s'ils sont à un stade précoce.

Art. 16h, al. 2 :

Supprimer la mention du rapport explicatif au profit du nombre d'utilisateurs simultanés.

La définition actuelle est trop large et crée des risques inacceptables pour les fournisseurs. Techniquement, il est facile de configurer un réseau pour permettre 1000 utilisateurs simultanés, ce qui pourrait classer des réseaux privés comme professionnels. Cela impose des obligations disproportionnées et crée une insécurité juridique permanente.

Art. 19, al. 1 :

Supprimer les mentions de « FSCD avec des obligations restreintes » et « FSCD avec des obligations complètes », ou les modifier en une obligation de fournir toute information collectée sans obligation d'identifier les utilisateurs.

L'obligation d'identification contredit les principes de minimisation des données et pénalise les entreprises respectueuses de la protection des données. Elle compromet également la compétitivité des PME et la position de la Suisse en tant que lieu d'innovation.

Art. 21, al. 6 :

Supprimer l'obligation pour les FSCD de conserver les données secondaires de communication pour exécuter les surveillances rétroactives.

Voir commentaire art. 16g, al. 3, let. a, ch. 2.

Art. 19, al. 2 :

Supprimer sans remplacement et maintenir les règles présentement applicables. La définition actuelle est trop vague et crée une insécurité juridique pour les fournisseurs.

Il n'est pas possible pour un fournisseur de s'assurer juridiquement de la définition utilisée, ce qui nécessite la suppression de cette disposition.

Art. 22 :

Supprimer sans remplacement.

Conserver la division en deux catégories existantes pour éviter une charge disproportionnée sur les PME. La suppression de cet article permet de maintenir une structure plus simple et plus claire.

Art. 11, al. 4 :

Supprimer sans remplacement.

Conserver la division en deux catégories existantes pour éviter une charge disproportionnée sur les PME. La suppression de cet article permet de maintenir une structure plus simple et plus claire.

Art. 16b :

Supprimer sans remplacement.

Conserver la division en deux catégories existantes pour éviter une charge disproportionnée sur les PME. La suppression de cet article permet de maintenir une structure plus simple et plus claire.

Art. 31, al. 1 :

Supprimer sans remplacement.

Conserver la division en deux catégories existantes pour éviter une charge disproportionnée sur les PME. La suppression de cet article permet de maintenir une structure plus simple et plus claire.

Art. 51 et 52 :

Abroger la suppression.

Conserver la division en deux catégories existantes pour éviter une charge disproportionnée sur les PME. La suppression de ces articles doit être abrogée pour maintenir une structure plus simple et plus claire.

Art. 60a :

Supprimer sans remplacement.

Les mesures rétroactives comportent des risques importants pour les droits fondamentaux des utilisateurs. Elles permettent à une autorité ordonnatrice d'exiger délibérément des résultats faux positifs, ce qui condamne objectivement des personnes innocentes et viole la présomption d'innocence.

Art. 42a et 43a :

Supprimer sans remplacement, ou alternativement supprimer les mentions des protocoles, adresses IP et port du client.

Les obligations actuelles sont disproportionnées et créent des risques pour la sécurité des utilisateurs. Elles permettent des requêtes automatiques sans contrôle juridique, ce qui augmente le risque d'abus et de surveillance en temps réel sans les garanties nécessaires.

Art. 50a :

Supprimer sans remplacement.

L'obligation de supprimer le cryptage à tout moment met en danger la sécurité des systèmes informatiques suisses et contredit les droits fondamentaux des utilisateurs. Elle rend les systèmes vulnérables aux attaques de pirates informatiques et à l'espionnage, ce qui est contraire à la Constitution suisse et aux lois sur la protection des données.

Art. 62, let. a et b :

Modifier les let. a et b pour préciser que les données doivent être conservées uniquement si elles existent.

La formulation actuelle impose des obligations disproportionnées et coûteuses pour les fournisseurs. Elle demande la conservation de données qui n'existent pas nécessairement, ce qui crée une charge excessive et inutile pour les entreprises.

OME-SCPT**Art. 14, al. 3 VD-ÜPF :**

Supprimer sans remplacement.

L'intervention active pour tous les FSCD est disproportionnée et économiquement non viable. Elle impose des obligations excessives aux PME et crée une insécurité juridique.

Art. 14, al. 4 VD-ÜPF :

Modifier le terme « FSCD avec des obligations minimales » en « FSCD sans obligations complètes ». La formulation actuelle élargit inutilement le champ d'application et augmente les obligations pour les entreprises concernées. Elle doit être modifiée pour éviter des charges disproportionnées sur les PME.

Art. 20, al. 1 VD-ÜPF :

Supprimer la phrase « et les fournisseurs avec des obligations réduites ».

L'intervention active pour tous les FSCD est disproportionnée et économiquement non viable. Elle impose des obligations excessives aux PME et crée une insécurité juridique.

III. Conclusion

L'usam appelle le Conseil fédéral à revoir sa copie et à élaborer des propositions qui respectent véritablement les intérêts des PME et de l'innovation en Suisse. Les modifications suggérées ne répondent pas aux objectifs annoncés et comportent des risques majeurs pour les PME, l'innovation et la

compétitivité de la Suisse. Les révisions doivent être entièrement repensées pour éviter de pénaliser les entreprises suisses et de compromettre la position du pays en tant que leader technologique.

Nous vous remercions de l'attention portée à notre prise de position et vous présentons, Madame, Monsieur, nos respectueuses salutations.

Union suisse des arts et métiers usam



Urs Furrer
Directeur



Mikael Huber
Responsable du dossier

Von: Paraskevi Meierhofer
Gesendet: Dienstag, 6. Mai 2025 11:39:10 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: ISC-EJPD-Aemterkonsultationen ÜPF
Cc: [REDACTED]
Betreff: Stellungnahme economiesuisse zur Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrte Damen und Herren

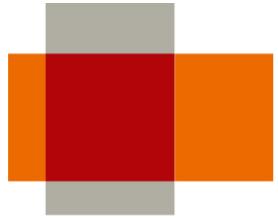
Gerne lassen wir Ihnen im Anhang unsere Stellungnahme zur Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) zukommen.

Wir danken für die Kenntnisnahme und bitten um eine Empfangsbestätigung.

Freundliche Grüsse

Paraskevi Meierhofer
Assistentin Wettbewerb & Regulatorisches
economiesuisse
Hegibachstrasse 47
CH-8032 Zürich

Telefon [REDACTED]
paraskevi.meierhofer@economiesuisse.ch
www.economiesuisse.ch



Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Ausschliesslich per E-Mail an:
ptss-aemterkonsultationen@isc-ejpd.admin.ch

6. Mai 2025

Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF): Stellungnahme economiesuisse

Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar haben Sie uns eingeladen, zu den im Betreff genannten Vorlagen Stellung zu nehmen. Wir danken Ihnen für diese Möglichkeit. Als Dachverband der Wirtschaft bündelt economiesuisse die Interessen von rund 100 Branchenverbänden, 20 Handelskammern und insgesamt etwa 100'000 Schweizer Unternehmen.

economiesuisse lehnt die vorgeschlagenen Anpassungen an VÜPF und VD-ÜPF mit Nachdruck ab. Die Vorlage lässt jegliche Verhältnismässigkeit vermissen und es ist im hohen Masse fragwürdig, ob die gesetzlichen Grundlagen für die vorgeschlagenen Anpassungen auf Verordnungsstufe überhaupt gegeben sind. Im Spannungsfeld zwischen Persönlichkeitsschutz, Wirtschaftsfreiheit und Sicherheit muss Fernmeldeüberwachung auf einer klaren gesetzlichen Grundlage basieren, die den Willen des Gesetzgebers und die Auslegung der Gerichte klar widerspiegelt. Solche Überwachungsmassnahmen müssen unterschiedliche Interessen abwägen und dabei Rücksicht auf die wirtschaftliche Machbarkeit, die Wettbewerbsfähigkeit, den Datenschutz und die Cybersicherheit nehmen. All diese Aspekte sind in den vorliegenden Ausführungserlassen zu Gunsten eines sehr weitgehenden Überwachungsanspruchs des Staates zurückgedrängt. Dies war aus unserer Sicht nicht die Absicht des Gesetzgebers. Wir fordern deshalb die Rückweisung und umfassende Überarbeitung der Vorlagen. Sie sind grundle- gend neu zu gestalten, mit Rücksicht auf die Grundrechte und den internationalen Kontext, einem ge- setzeskonformen Kategorisierungsmodell und ohne massive Mehrbelastung der Unternehmen. Diese grundlegende Korrektur ist zwingend notwendig, um eine zweckdienliche Fernmeldeüberwachung ohne massiven Kollateralschaden zu schaffen.

Weitere Ausführungen zu unserer Position finden sie nachfolgend.

1 Grundsatzkritik:

Auch bei der Sicherheit im digitalen Raum muss Verhältnismässigkeit der Massstab staatlicher Eingriffe sein. Sicherheitspolitisch motivierte Eingriffe in Grundrechte müssen verhältnismässig sein. Das bedeutet: Sie dürfen nur erfolgen, wenn sie einem legitimen öffentlichen Interesse dienen,

geeignet und erforderlich sind und die Interessenabwägung zugunsten des öffentlichen Wohls ausfällt. Gerade in sicherheitsrelevanten Bereichen ist Zurückhaltung geboten – Eingriffe dürfen nicht über das hinausgehen, was zum Schutz der Gesellschaft zwingend nötig ist. Eine freiheitlich-demokratische Ordnung lebt davon, dass der Staat auch unter Druck rechtsstaatlich handelt.

Der Staat trägt Verantwortung für die Sicherheit seiner Bevölkerung – auch im digitalen Raum. Er muss dazu in der Lage sein, schwere Straftaten im Internet wirksam zu verfolgen. Doch es gilt auch hier: Sicherheitsmaßnahmen dürfen die Freiheitsrechte nicht unverhältnismässig einschränken. Die digitale Strafverfolgung muss rechtsstaatlich eingebettet und zielgerichtet sein, nicht pauschal oder flächendeckend, wie dies in den Vernehmlassungsvorlagen leider der Fall ist. Nur so lässt sich ein verantwortungsvoller Ausgleich zwischen Freiheit und Sicherheit wahren – auch in einer zunehmend vernetzten Gesellschaft. Dies ist mit der vorliegenden Vorlage nicht gewährleistet. Letztlich fehlt auch ein Nachweis, dass die aktuellen Mittel und Kompetenzen der Strafuntersuchungsbehörden nicht mehr ausreichen, um eine effiziente Aufgabenerfüllung zu ermöglichen.

2 Standortvorteile nicht unnötig gefährden

Nebst diesen grundlegenden Kritikpunkten ist aus Sicht der Wirtschaft vor allem darauf hinzuweisen, dass die weitgehenden Forderungen der Vorlagen einen erheblichen Standortnachteil für unser Land zur Folge hätten. Die Schweiz ist ein hochkompetitiver Technologiestandort, der sich gerade auch im Startup-Bereich als Biotop der «Privacy Champions» international behauptet. Diese Dienste legen besonderen Wert auf Datensicherheit und besetzen damit ein wachstumsträchtiges Marktsegment. Auch etablierte Firmen finden hierzulande bisher günstige Rahmenbedingungen vor. International tätige Dienstleister versorgen nicht nur die Schweizer Firmen und Bevölkerung mit kostengünstigen, modernen und sicheren OTT-Diensten, sie stellen hierzulande auch mehrere Tausend Arbeitsplätze bereit, bilden Fachkräfte aus und liefern Steuersubstrat ab. Mit einer Ausweitung der fernmelderechtlichen Überwachungspflichten, wie sie die Vernehmlassungsvorlagen beinhalten, wären die günstigen Rahmenbedingungen für solche Dienstleister in der Schweiz akut gefährdet. Der technische, administrative und infrastrukturelle Mehraufwand wäre besonders für KMU enorm und liesse sich kaum mit entsprechenden Vorteilen für den Strafvollzug und die Sicherheit der Bevölkerung rechtfertigen. Wir sind dezidiert der Ansicht, dass eine schlankere Regulierung mit weniger erfassten Unternehmen und risikobasierten Pflichten mindestens vergleichbaren Nutzen für die Strafvollzugsbehörden bringt, wie die breite Vorratsdatenspeicherung, allerdings ohne, dass ein massiver wirtschaftlicher Kollateralschaden entsteht.

3 Geltungsbereich FDA und AAKD: Es braucht endlich gesetzeskonforme Ausführungsbestimmungen

Knackpunkt der Vorlagen sind vor allem die neu definierten Kategorien und Mitwirkungspflichten in der VÜPF. Dabei halten wir die umfassende Regulierung von AAKD für besonders problematisch. Sie ist einerseits so nicht vom Gesetzgeber vorgesehen, resp. sprengt den Rahmen der gesetzlichen Verweisungsnorm im BÜPF. Dieser Auffassung sind bekanntlich auch das Bundesgericht und das Bundesverwaltungsgericht, die sich in den letzten Jahren mehrfach mit der Thematik befasst haben¹. Andererseits folgen die Definitionen nicht den einschlägigen internationalen Standards², bspw. indem die Ausführungsbestimmungen auf Mehrwegkommunikation über die interpersonelle Kommunikation hinaus ausgeweitet werden.

Darüber hinaus wirken die Abgrenzungen und Schwellenwerte der Kategorien nach Umsatz und Anzahl Kunden beliebig gewählt, auch wenn dies bereits im geltenden Recht so geregelt ist. Der

¹ Siehe bspw. Bundesgerichtsurteil 2C_544/2020 und Urteil [A-5373/2020](#) des Bundesverwaltungsgerichts.

² Siehe bspw.

räumliche Geltungsbereich bleibt derweil unklar, also die Betroffenheit von Dienstanbietern ausserhalb der Schweiz und der Datenzugriff der Behörden, insb. wenn es sich um weitere Daten als «nur» Randdaten handelt. Insgesamt braucht es aus unserer Sicht ein pragmatischeres Konzept, das mit etablierten Standards und technischen Richtlinien im Einklang steht.

4 Datenschutz und Cybersicherheit nicht aufs Spiel setzen

Neben der Breite ist auch die Tiefe der angedachten Regulierung problematisch. Die rückwirkenden, pauschalen Überwachungspflichten, die auch vielen OTT-Anbietern auferlegt würden, hätten für die betroffenen Firmen empfindliche Kostenfolgen. In diesem Zusammenhang ist vor allem die Pflicht einer rund um die Uhr besetzten Pikett-Stelle zu nennen oder die generell notwendige, aufwändige Hardware-Infrastruktur. Besonders einschneidend wären jedoch die Folgen für die Bevölkerung, die man mit der vorgeschlagenen Stossrichtung faktisch einer Massenüberwachung mit Vorratsdatenspeicherung aussetzen würde, bspw. durch weitreichende Aufbewahrungs- und Identifikationspflichten. Dies ist mit dem politischen Willen, einen angemessenen und funktionalen Datenschutz in der Schweiz zu schaffen (bspw. Grundsatz der Datenminimierung im DSG), der gerade in der Privatwirtschaft mit erheblichem Aufwand umgesetzt wird, dies nicht zu vereinbaren. Hinzu kommt, dass eine umfassende Vorratsdatenspeicherung auf europäischer Ebene schon mehrfach durch die Gerichte als unverhältnismässig und damit unzulässig eingestuft wurde. Zu guter Letzt muss davon ausgegangen werden, dass die technische Umsetzung der Überwachung und Vorratsdatenspeicherung auch zu einer Schwächung der Cybersicherheit der Unternehmen führt. «Hintertüren» und andere Vorkehrungen wie Entschlüsselungspflichten, welche den Zugriff der Behörden gewährleisten sollen, stellen nämlich auch Angriffsvektoren für Dritte dar, seien sie kriminell, nachrichtendienstlich oder gar kriegerisch motiviert.

Insgesamt braucht es folglich auch hier klar mehr Augenmass. Die Bedürfnisse der Justizvollzugsbehörden müssen zwingend mit den Interessen der Unternehmen und der breiten Bevölkerung abgewogen werden.

Wir fordern damit eine grundlegende Überarbeitung der Vorlage unter Berücksichtigung unserer diversen und grundlegenden Kritikpunkte.

Bei Rückfragen stehen wir jederzeit gerne zur Verfügung.

Freundliche Grüsse

economiesuisse

Erich Herzog
Mitglied der Geschäftsleitung,
Bereichsleiter Wettbewerb & Regulatorisches

Lukas Federer
Stv. Bereichsleiter Energie,
Infrastruktur & Umwelt

Von: BA-Aemterkonsultationen
Gesendet: Dienstag, 29. April 2025 09:46:25 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: ISC-EJPD-Aemterkonsultationen ÜPF
Cc: [REDACTED]
Betreff: RE: Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF; VD-ÜPF); Eröffnung des Vernehmlassungsverfahrens

Madame, Monsieur,

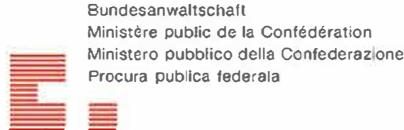
Par le présent, nous revenons à la consultation parlementaire citée en marge et vous remercions de nous donner l'opportunité de prendre position.

A cet égard, nous vous informons que le Ministère public de la Confédération n'a pas de remarques à formuler.

Nous vous adressons, Madame, Monsieur, nos sincères salutations.

Almedina Zrinic

Juriste Service juridique
Ministère public de la Confédération MPC
Guisanplatz 1, 3003 Berne
Tél.: +41 58 48 08805
almedina.zrinic@ba.admin.ch
www.bundesanwaltschaft.ch



Von: Roman Burkart

Gesendet: Dienstag, 11. März 2025 16:29:12 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: AW: [Extern] WG: Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF; VD-ÜPF); Eröffnung des Vernehmlassungsverfahrens

Sehr geehrte Damen und Herren,

Der Gegenstand der Vernehmlassung ist für unseren Verband nicht relevant und bedarf daher keiner Stellungnahme. Wir bedanken uns für die Möglichkeit zur Stellungnahme und verbleiben mit freundlichen Grüßen.

 **Roman Burkart**

Geschäftsführer

Interverband für Rettungswesen - IVR

Bahnhofstrasse 55, 5000 Aarau

Email: roman.burkart@ivr-ias.ch

Tel. Hauptnummer: +41 (0) 31 320 11 44

Tel. Direkt: +41 (0) 31 320 11 41

www.144.ch



SSK | CMP

Schweizerische Staatsanwaltschaftskonferenz SSK
Conférence suisse des Ministères publics CMP
Conferenza svizzera dei Ministeri pubblici CMP

Eidg. Justiz- und Polizeidepartement EJPD

Per Email:

ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 24. März 2025

Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar 2025 haben Sie unsere Konferenz eingeladen, an obgenannter Vernehmlassung teilzunehmen. Dafür danken wir Ihnen bestens.

Im Dezember 2022 rief der damalige Ausschuss FMÜ die Begleitgruppe Rechtsetzung ins Leben, um insbesondere die Strafverfolgungsbehörden, aber auch die MWP in der Erarbeitung von Gesetzesvorlagen miteinzubeziehen. Das hat sich aus Sicht der SSK bewährt: Der Dienst ÜPF hat mit dieser Begleitgruppe im Hinblick auf die Ausarbeitung der obgenannten Vorlagen mehrere Sitzungen durchgeführt, eingebrachte Vorbehalte und Fragen wurden aus unserer Sicht berücksichtigt, beziehungsweise geklärt. Die nun präsentierten Entwürfe entsprechen nach unserem Dafürhalten abgesehen von einigen redaktionellen Anpassungen dem in der Begleitgruppe Rechtsetzung Besprochenen.

Das Ziel der Vorlage, die verschiedenen Kategorien von Mitwirkungspflichtigen näher zu definieren, deren Pflichten zu umschreiben und bekannte Lücken bei einzelnen Überwachungstypen zu schliessen, wird erreicht. Die Anliegen und Bedürfnisse der Strafverfolgungsbehörden im Rahmen des übergeordneten Rechts sind angemessen und zweckmässig berücksichtigt.

Unserem generellen Anliegen, die Beweiserhebung und -sicherung von Daten im Strafverfahren zu vereinfachen und zu verbessern, kann diese Vorlage freilich nicht entgegenkommen. Wir möchten deshalb (wiederholt) darauf hinweisen, dass in Bezug auf die mittel- und längerfristige Anpassung an die technologische Entwicklung grundlegende Reformen in der Strafprozessordnung und im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) notwendig sind. Die SSK ist selbstverständlich sehr gerne bereit, hierbei das EJPD mit ausgewiesenen Expert:innen aus der Praxis zu unterstützen.

Mit freundlichen Grüßen

Christoph Ill, Präsident

Kopie:

- Mitglieder SSK-CMP
- Generalsekretariate KKJPD und KKPKS



Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
Conférence des directrices et directeurs des départements cantonaux de justice et police
Conferenza delle diretrici e dei direttori dei dipartimenti cantonali di giustizia e polizia

Per E-Mail an:

ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 31. März 2025

09.02.01/jäg

**Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs
(VÜPF; VD-ÜPF)**

Sehr geehrte Damen und Herren

Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) wurde eingeladen, zur oben erwähnten Vernehmlassung Stellung zu nehmen. Wir danken Ihnen dafür bestens.

Der Vorstand KKJPD hat in seiner Sitzung vom 24. März 2025 beschlossen, auf eine Stellungnahme im Namen der KKJPD zu verzichten und es den einzelnen Kantonen zu überlassen, sich zur Vorlage zu äussern.

Besten Dank für die Kenntnisnahme.

Freundliche Grüsse

Florian Düblin
Generalsekretär



LAW FIRM
ÉTUDE D'AVOCATS

Département fédéral de justice et police
DFJP
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Lausanne, le 9 avril 2025

Révision partielle de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT)

Monsieur le Conseiller fédéral,
Mesdames, Messieurs,

Dans le délai imparti au 6 mai 2025, le soussigné a le plaisir de participer spontanément et à titre personnel à la consultation mentionnée sous rubrique. Je me suis concentré sur les aspects principalement juridique et je renonce à aborder les aspects très techniques que sont les types de renseignement.

Besoin de clarifications et prise en compte des PME

La situation actuelle n'est guère satisfaisante et l'entrée en vigueur de l'art. 2 al. 2 LSCPT et la clarification des notions et des obligations des FST et FSCD sont nécessaires et bienvenues, même si on peut regretter que le Conseil fédéral ait choisi des notions différentes au regard de la LTC et de la LSCPT.

Il est fondamental de prendre en compte les besoins des PME suisses, et en particulier des FSCD qui fournissent des services en ligne car ils sont en concurrence directe avec des fournisseurs étrangers souvent soumis à des règles beaucoup moins contraignantes. Il est important également pour de nombreuses autres entreprises que la Suisse conserve son image de pays respectueux de la sphère privée.

Une obligation trop large de conservation de métadonnées, au surplus remise en cause à plusieurs reprises par les autorités judiciaires européennes, risque de contraindre des entreprises suisses à partir à l'étranger. Cela priverait notre pays de compétences

techniques et rendrait certainement aussi plus difficile l'accès des autorités de poursuite pénale aux données d'identification des abonnés. Il pourrait même être plus difficile pour certaines personnes d'utiliser des outils de communication sécurisés en Suisse.

Finalement, il faut garder en tête que le cybercriminel qui veut agir en ligne en ne laissant pas de traces trouvera toujours de nombreux fournisseurs opérant légalement depuis l'étranger (sans parler de l'offre illégale tout aussi facilement accessible). Ce n'est pas en adoptant des obligations restrictives pour quelques FSCD que la lutte contre la cybercriminalité sera fondamentalement facilitée. À l'inverse, permettre au plus grand nombre de personnes de protéger facilement leurs communications sans compétences techniques est essentiel à la sécurité de l'information et au bon fonctionnement de la démocratie, en Suisse comme à l'étranger.

Exploitants de réseaux de télécommunication internes

Le Conseil fédéral considère qu'il n'est pas nécessaire de préciser la notion d'exploitant de réseaux de télécommunication internes (art. 2 al. 1 let. d LSCPT). On peut imaginer que cela correspond (notamment) à la notion de l'art. 16a al. 2 OSCPT mais il serait mieux de le préciser.

FST ayant des obligations restreintes

La possibilité pour un FST de demander à être soumis seulement à des obligations restreintes doit être conservée. Les critères doivent en revanche être revus :

- cela doit toujours être accordé aux FST qui offrent principalement les services en question dans le domaine de la recherche et l'éducation (sinon une école serait par exemple soumise à des obligations complètes en raison d'un seul accès accordé pour des raisons administratives sans lien avec l'éducation) ;
- seul le chiffre d'affaires en lien avec les services concernés doit être pris en compte (sinon le critère de l'importance du service n'est pas respecté). Ce n'est pas la capacité financière du FST qui est déterminante (auquel cas ce serait plutôt son bénéfice que le chiffre d'affaires qui serait pertinent) ;
- l'art. 26 al. 6 LSCPT ne prévoit pas le nombre de cibles comme critère. Il est au surplus arbitraire car il suffit d'une grande procédure pénale pour que FST soit l'année suivante soumis à des obligations entières pour 12 mois seulement, ce qui aurait un impact significatif. Ce critère n'est d'ailleurs pas repris pour les FSCD.

En cas de d'assujettissement par le Service SCPT d'un FST à des obligations complètes (art. 16c OSCPT), les délais de six et douze mois doivent courir non pas depuis le moment de la déclaration du Service SCPT mais depuis le moment où la décision est entrée en force. Sinon, le risque est trop important que le FST doive faire des investissements importants pendant la procédure de recours, en particulier s'il n'a jamais eu d'obligations complètes.

FSCD

Une définition des FSCD est nécessaire et bienvenue.

Le rapport inclut les services de stockage en ligne tels que le stockage infonuagique, l'hébergement de fichiers, l'hébergement partagé, le stockage en ligne, le partage de fichiers. Cela ne semble pourtant pas ressortir de la lettre de l'art. 16d OSCPT. La principale fonction de ces services est généralement le stockage de données et pas la communication entre des tiers. Si c'est le cas, c'est un service connexe et cela ne doit pas suffire à le qualifier de FSCD. Ce point devra être clarifié.

La terminologie « restreinte » et « minimale » porte à confusion. Il serait préférable de parler d'obligations minimales, étendues et complètes.

Le nombre de 5000 usagers semble bas et risque d'être vite atteint, notamment pour des services gratuits et sans que les 5000 personnes qui se sont connectées une fois pour voir le service l'utilisent activement.

Comme pour les FST, c'est l'entrée en force de la décision du Service SCPT qui doit être déterminante pour le délai de mise en conformité.

Conservation des données secondaires par les FSCD

La surveillance rétroactive porte une atteinte importante à la sphère privée car elle concerne tous les utilisateurs sur qui elle fait porter un soupçon de commission d'infraction pénale pouvant justifier la mise en place d'une mesure de surveillance. La conservation pendant six mois de ces données par les FSCD ayant des obligations complètes constitue une atteinte importante à la sphère privée et un risque pour les personnes concernées. Elle ne devrait pas être imposée systématiquement au FSCD avec obligations complètes.

Ces dernières années, la CJUE a rappelé à plusieurs reprises que la conservation et l'accès aux données personnelles dans le domaine des communications électroniques cause une atteinte grave aux droits au respect de la vie privée, à la protection des données personnelles et à la liberté d'expression garantis par la Charte (et de manière similaire par la Constitution fédérale et la CEDH)¹.

¹ Voir, notamment, arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), du 2 octobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788), du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152), du 17 juin 2021, M.I.C.M. (C-597/19, EU:C:2021:492), et du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258).

Les FSCD ayant des obligations restreintes ne devraient pas non plus être soumis à l'obligation d'identifier les usagers. Cela mettrait à la charge des fournisseurs suisses des obligations qui dépassent largement celles de leurs concurrents étrangers.

Personnes qui mettent leur accès à un réseau public de télécommunication à la disposition de tiers

L'art. 16h OSCPT considère que la mise à disposition d'un accès (notamment WLAN) est faite à titre professionnel dès que l'accès public au réseau WLAN est considéré comme étant exploité à titre professionnel dès que de manière cumulée pour tous les accès au réseau WLAN d'une même personne, le nombre d'utilisateurs finals peut être supérieur 1000. Si l'on pense à une école, un hôpital ou une chaîne de cafés, ce nombre risque d'être rapidement atteint. Il s'agit en effet d'une nombre potentiel (y compris jamais atteints) cumulé pour tous les sites.

Le critère à retenir est bien plus de savoir si la personne met à disposition le réseau de manière professionnelle (contrat de prestations, rémunération, etc.) ou si c'est un service très annexe.

Quant au but d'éviter qu'un criminel n'utilise un réseau ouvert pour agir de manière anonyme, cette possibilité existera dans tous les cas.

Fournisseurs et usagers à l'étranger

La LSCPT et l'OSCPT s'appliquent naturellement aux fournisseurs étrangers qui fournissent des services de communication en Suisse. Ce sera particulièrement le cas des FSCD puisqu'ils n'ont pas besoin d'infrastructure, de ressources d'adressage ou de fréquences en Suisse. Il est pourtant essentiel qu'ils respectent leurs obligations légales, tant dans l'intérêt de la poursuite pénale que la LSCPT doit servir que dans l'égalité de traitement avec les FSCD suisses.

On peut donc regretter que rien ne soit prévu pour s'assurer du respect de leurs obligations par les FSCD étrangers ne serait-ce que par l'obligation de désigner un représentant en Suisse.

Ni l'OSCPT ni le rapport n'indiquent si le chiffre d'affaires et les usagers à l'étranger sont pris en compte dans les critères indiqués.

Suppression des chiffrements

Le rapport souligne avec raisons que le chiffrement de la communication numérique est un droit fondamental et que l'obligation de supprimer les chiffrements ne concerne pas les chiffrements de bout en bout entre les clients finaux, plus précisément entre leurs équipements terminaux ou les applications qu'ils utilisent pour communiquer.

Dans ce cas, ce n'est souvent pas le fournisseur qui appose le chiffrement et à moins de lui imposer de mettre en place une porte dérobée (ce qui serait inacceptable), il ne peut pas accéder au contenu. Cette distinction est toutefois arbitraire et souvent l'utilisateur ne saura pas s'il est seul ou non à disposer de la clé. En outre, cela reviendrait à mieux protéger ceux qui ont des compétences techniques (ou des moyens financiers pour les remplacer), que ceux qui ont besoin de l'assistance technique de leur fournisseur.

La disposition devrait donc respecter la même protection pour les chiffrements des données de bout en bout opérés avec une clé du fournisseur ou avec une clé du client. L'art. 50a OSCPT doit donc se limiter à la suppression des chiffrements de transport entre l'opérateur et ses clients finaux, mais pas les chiffrements de bout en bout entre clients finaux, qu'ils soient mis en place par le client ou par le fournisseur pour le client.

Analyse d'impact relative à la protection des données personnelles (AIPD)

Le Rapport explicatif relatif à l'ouverture de la procédure de consultation indique de manière lapidaire que « l'AIPD réalisée a montré qu'il n'y avait pas de risque élevé pour ce projet ». L'art. 22 LPD prévoit en effet qu'une analyse d'impact relative à la protection des données personnelles (AIPD) doit être effectuée au préalable lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. C'est certainement le cas en l'espèce et l'absence d'information sur les conclusions de l'AIPD ne sont pas très rassurants, d'autant que tous les FST et FSCD seront déliés de procéder à une AIPD vu qu'ils traiteront les données sur la base d'une obligation légale (22 al. 4 LPD). Encore une fois le risque est particulièrement élevé avec les obligations de conservation des données.

Veuillez croire, Monsieur le Conseiller fédéral, Mesdames, Messieurs, à l'expression de ma parfaite considération.



Sylvain Métille
Dr jur, avocat
Professeur à l'Université
metille@hdclegal.ch



per E-Mail an:
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Prof. Dr. Michael Schaeppman
Rektor

Zürich, 15. April 2025

Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF): Stellungnahme

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zur obgenannten Vorlage Stellung zu nehmen.

Wie im erläuternden Bericht erwähnt wird, steht die Vorlage mit dem Postulat Albert Vitali «Für ein verhältnismässiges Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs» in Zusammenhang. Im erwähnten Postulat wurde beanstandet, dass der im BÜPF vorgesehene Mechanismus, kleine Anbieterinnen von Überwachungspflichten zu befreien und ihnen lediglich eine Duldungspflicht aufzuerlegen ("Down-grade"), nicht ausreichend zur Anwendung komme.

Der Bundesrat wies in seinem Bericht darauf hin, er beabsichtige «mit der laufenden Revision der VÜPF (Revision des Geltungsbereichs) die rechtlichen Grundlagen so zu optimieren, dass es anhand der Definitionen einfach ersichtlich sein wird, welcher Kategorie eine Anbieterin zugewiesen ist». Dies werde dazu führen, so der Bundesrat, «dass von den beim Dienst ÜPF elektronisch erfassten Anbieterinnen nur wenige in der Kategorie FDA verbleiben, wovon die grosse Mehrheit in den Genuss von reduzierten Pflichten kommen dürfte» (Bericht des Bundesrats vom 18. Oktober 2023, S. 7).

Vor diesem Hintergrund überrascht es, dass die Vorlage hinsichtlich der «Downgrades» für Anbieterinnen von Fernmeldediensten (FDA) eine massive Verschärfung vorsieht:

Aktuell erfolgt ein Downgrade, wenn eine FDA mit weniger als 10 Überwachungsaufträgen pro Jahr betraut wird und mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten einen Jahresumsatz von weniger als 100 Millionen Franken erzielt (Art. 51 Abs. 1 Bst. b VÜPF). Neu soll die Limite von 100 Millionen Franken auf den *Jahresumsatz des gesamten Unternehmens* bezogen werden anstatt allein auf den mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten erzielten Umsatz (Art. 16b Abs. 1 lit. b Ziff. 2 E-VÜPF).

Die Universität Zürich (UZH) versorgt wenige andere Institutionen – namentlich vereinzelte Assoziierte Institute der Universität, die Zentralbibliothek Zürich (eine öffentlich-rechtliche Stiftung) und bestimmte Bereiche der Universitätsspitäler – mit Netzwerkdienstleistungen und gilt daher als FDA. Gestützt auf den erwähnten Art. 51 Abs. 1 Bst. b VÜPF profitiert sie aktuell von einem Downgrade, da sie die dort genannten Schwellen nicht erreicht. Der mit den Fernmeldedienstleistungen erzielte Umsatz ist marginal. Hingegen überschreitet der Jahresumsatz «des gesamten Unternehmens» (d.h. der gesamten Universität) den Betrag von 100 Millionen Franken.

Es ist nicht ersichtlich, inwiefern der Umsatz der gesamten Universität in Bezug auf ein «Downgrade» als FDA eine Rolle spielen sollte. Entscheidend muss weiterhin sein, dass die UZH nur in sehr geringem Masse als FDA tätig ist. Sollte in ihrem Fall kein Downgrade mehr möglich sein, widerspräche dies klar der Stossrichtung, welche der Bundesrat für die vorliegende Vorlage in Aussicht gestellt hat.

Wir beantragen daher, dass in Art. 16b Abs. 1 lit. b Ziff. 2 E-VÜPF weiterhin auf den mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten erzielten Umsatz abgestellt wird und nicht auf den Umsatz des gesamten Unternehmens.

Zwar besteht weiterhin die Möglichkeit eines Downgrade für FDA, die ihre Fernmeldedienste nur im Bereich Bildung und Forschung anbieten (Art. 51 Abs. 1 Bst. a VÜPF bzw. Art. 16b Abs. 1 lit. a E-VÜPF). Dies ist zu begrüssen. Die Fernmeldedienste der UZH finden denn auch grösstenteils im Bereich von Bildung und Forschung statt. Doch handelt es sich dabei um keine klar abgegrenzte Vorgabe. Es ist daher mit Unsicherheiten zu rechnen, ob tatsächlich sämtliche erbrachten Fernmeldedienstleistungen unter «Bildung und Forschung» fallen.

Neu sollen ausserdem Anbieterinnen von Netzwerkdienstleistungen zwischen öffentlich-rechtlichen Körperschaften nicht mehr als FDA gelten (Art. 16a Abs. 2 Bst. d E-VÜPF). Auch das ist zu begrüssen. Allerdings ist anzumerken, dass anstelle des (je nach Verständnis einschränkenden) Begriffs «Körperschaft» der Begriff «Organisation» verwendet werden sollte. Bei der Mehrheit der Institutionen, gegenüber denen die UZH Netzwerkdienstleistungen erbringt, handelt es sich um öffentlich-rechtliche Organisationen, allerdings nicht bei allen. Die UZH ist daher weiterhin auf die Möglichkeit eines Downgrade angewiesen.

Für Rückfragen stehen Ihnen Markus Golder, markus.golder@rud.uzh.ch, und Andreas Meier, andreas.meier@rud.uzh.ch, gerne zur Verfügung.

Freundliche Grüsse



Prof. Dr. Michael Schaepman
Rektor

Eidgenössisches Justiz- und Polizeidepartement
Bundeshaus West
3003 Bern

Ausschliesslich per E-Mail an:
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Neuenhof, 28. April 2025

Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat Jans,
Sehr geehrte Damen und Herren

Gerne nehmen wir die Möglichkeit wahr, innerhalb der gesetzten Frist Stellung zur Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) zu nehmen.

Die SEPPmail AG ist ein Anbieter von Lösungen zur Verschlüsselung von E-Mail und ist seit 25 Jahren im Schweizer Markt aktiv. Zu unseren Kunden zählen Grosskunden aus den Bereichen Banken, Versicherungen, Gesundheitswesen, Gemeinden, Kantone und notabene auch die Bundesverwaltung. Der Kundenstamm besteht aus ca 12'000 Firmenkunden, hauptsächlich aus dem DACH-Raum. Die Lösungen werden sowohl für die Installation beim Kunden wie als Cloud-Lösung angeboten. Zudem bieten Partner eigene Cloud-Lösungen basierend auf der SEPPmail-Technologie an («Managed Services Provider», MSPs).

SEPPmail schliesst sich der Vernehmlassungsantwort von Swico, dem Wirtschaftsverband der Digitalindustrie, vollumfänglich an (wir verzichten an dieser Stelle darauf, die Antwort der Swico hier zu wiederholen). Die vorliegende Vernehmlassung tangiert SEPPmail als potentiellen AAKD und Anbieter von Verschlüsselungslösungen besonders. Wir haben daher im Folgenden zusätzliche Anmerkungen und Anpassungen notiert.

Zusammenfassung: Schweizerische Anbieter von Lösungen zur vertraulichen Kommunikation gegenüber ausländischen Mitbewerbern benachteiligt was zur Folge haben könnte, dass gewisse Leistungen nicht mehr in der Schweiz erbracht werden können. Bei der Cloud-Lösung könnte das zur Folge haben, dass besonders im wichtigen deutschen Markt das Vertrauen in den Standort Schweiz uns insbesondere in unsere Cloud-Lösung abnimmt. Um die massiven Nachteile und prohibitiv hohen Kosten auszugleichen müsste SEPPmail eine Verlagerung relevanter Dienste aus der Schweiz heraus ernsthaft in Betracht ziehen.

BEMERKUNG ZU EINZELNEN ARTIKELN VÜPF

AAKD (Art. 16d bis g)

Um als Anbieter von Cloud-Lösungen erfolgreich zu sein, braucht es in der Regel (zehn- oder hundert-) tausende von Benutzern. Das bedeutet, dass selbst ein Startup oder ein KMU die Pflichten einer AAKD mit reduzierten Pflichten erfüllen müsste – etwas, das in der Praxis eine erhebliche und mitunter prohibitiv hohe finanzielle und personelle Belastung für eine solche Organisation darstellt.

Selbst die Schwelle von 1 Million Teilnehmenden ist für ein Startup nicht aussergewöhnlich. Faktisch wären faktisch alle Anbieter von Cloud-Lösungen, die aus der Schweiz heraus operieren, als AAKD einzustufen, was unverhältnismässig ist. Das Innovationspotential der gesamten Branche würde massiv beeinträchtigt.

Anpassung: Verzicht auf die Kategorie “AAKD mit minimalen Pflichten”; Verzicht auf “Anzahl Teilnehmende” als Kriterium für AAKD; deutliche Erhöhung der Schwellwerte (Faktor 10 bis 100).

Teilnehmer und Benutzeridentifikation (Art. 19)

Cloud-Lösungen müssen einfach und unkompliziert aufgesetzt werden können – der Vorgang der Aufschaltung ist mitunter der entscheidende kritische Faktor für den Erfolg einer Lösung. Durch eine Identifikationspflicht entstehen zusätzliche Hürden, welche Angebote aus der Schweiz heraus im internationalen Markt unattraktiver machen.

Anpassung: Streichung der Identifikationspflicht für AAKD (Art. 19 Abs. 2)

Nachweis der Auskunfts- und Ueberwachungsbereitschaft für AAKD mit reduzierten Pflichten (Art. 31 Abs. 1)

Die Anforderungen an die Bereitschaft ist für eine typische KMU oder ein typisches Startup untragbar. Eine solche Anforderung würde die Schweiz als Standort für solche Dienstleistungen faktisch untragbar machen – der Standort Schweiz würde deutlich unattraktiver werden.

Anpassung: Streichung von Art. 31 Abs. 1

Auskunftstype IR_59_EMAIL_LAST (Art. 42a)

Die Pflicht, Metadaten aus dem E-Mail-Verkehr aufzubewahren widerspricht direkt dem datenschutzrechtlichen Gebot der Datensparsamkeit. Zudem sind im E-Mail-Verkehr zwischen Servern (Relaying, Transport) etwa Benutzererkennungen wenn überhaupt dann nur mit zusätzlichem grossem Aufwand eruierbar – die Umsetzung ist also an fragwürdige Voraussetzungen gebunden.

Anpassung: Streichung von Art. 42a

Entfernung von Verschlüsselungen (Art. 50a)

Die Anforderung zur Entfernung von Verschlüsselungen würde alle AAKD mit mehr als 5'000 Benutzer betreffen. Somit wäre faktisch die gesamte Schweizerische AAKD-Branche betroffen.

Bei der asymmetrischen Verschlüsselung von E-Mail-Nachrichten (S/MIME oder PGP) kann eine von einem absendenden System verschlüsselte Nachricht nur noch mit dem privaten Schlüssel des Empfängers gelesen werden.

Die Pflicht zur Entfernung von Verschlüsselungen bei E-Mail würde demnach bedeuten, dass die gesamte Schweizerische AAKD-Branche alle gesendeten Nachrichten im Klartext speichern müsste – eine technische und rechtliche Herausforderung.

Das würde zum Beispiel zur Folge haben, dass bei der Verschlüsselung von E-Mails im Schweizer Gesundheitswesen (HIN.ch) oder von Banken eine unverschlüsselte Kopie der Daten für die Dauer der Vorratsdatenhaltung abgelegt werden müsste. Das widerspricht fundamentalen Grundsätzen des Datenschutzes, und notabene auch dem Bankkundengeheimnis (Art. 47 BankG, SR 952.0).

Die Entfernung von Verschlüsselung im Bereich von HTTPS wäre technisch nur über einen “SSL Man in the Middle Proxy” möglich. Dies würde den gesamten Web-Verkehr in der Schweiz massiv verteuern und wäre unverhältnismässig.

Es ist zudem rechtsstaatlich bedenklich, einen massiven Eingriff in die Grundrechte auf dem Verordnungsweg einführen zu wollen.

Anpassung: Streichung des Art. 50a.

BEMERKUNGEN ZU EINZELNEN ARTIKELN DER VD-ÜPF

Art 14 Abs 3 VD-ÜPF

Die Fristen sind für Startups und KMUs nur mit grossem Einsatz von Ressourcen zu leisten. Diese Anforderungen sind unverhältnismässig und wirtschaftlich nicht tragbar.

Anpassung: Streichung (respektive Anpassung auf massiv höhere/andere Schwellwerte gemäss Anpassung Art. 16d-g VÜPF)

Wir bedanken uns für die Berücksichtigung unserer Anliegen und stehen für Rückfragen gerne zur Verfügung (E-Mail: leisi@seppmail.ch).

Freundliche Grüsse,

Stefan Klein, CEO
SEPPmail AG

Matthias Leisi, CTO
SEPPmail AG

Libertäre Partei
Zugerstrasse 76b
CH-6340 Baar
info@libertaere-partei.ch



Per E-Mail als Word und PDF an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Baar, 29. April 2025

Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Vernehmlassungsantwort

Sehr geehrte Damen und Herren

Im Rahmen der Vernehmlassung zur obenerwähnten Angelegenheit erlauben wir uns, Stellung zu nehmen. Die libertäre Partei lehnt die Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) deutlich ab.

Im Folgenden möchten wir zunächst auf einige grundsätzliche Überlegungen hinweisen, bevor wir uns konkret der zur Diskussion stehenden Teilrevision widmen.

Postkonto

Kontonummer: 60-181123-3, Lautend auf: Libertäre Partei, 6340 Baar, IBAN: CH70 0900 0000 6018 1123 3,
SWIFT/BIC: POFICHBEXXX, Bank: PostFinance AG, Mingerstrasse 20, 3030 Bern

Grundsätzliches

Privatsphäre als unveräußerliches individuelles Recht

Aus einer konsequent freiheitlichen Sichtweise kann die fundamentale Bedeutung des Rechts auf Privatsphäre kaum überschätzt werden. Die Privatsphäre ist kein Privileg, das vom Staat gnädigerweise gewährt wird, sondern ein unveräußerliches Recht jedes Individuums. Sie bildet die Grundlage für die persönliche Freiheit, Selbstbestimmung und den Schutz vor willkürlicher Einmischung durch staatliche Akteure. Diesem Umstand wird in der Schweizer Rechtsordnung durch Art. 13 BV Rechnung getragen.

Präventiver Generalverdacht des Staates

Jede staatliche Überwachung, insbesondere wenn sie unter dem hehren Deckmantel irgendeiner «Verbrechensprävention» geschieht, ist letztlich nur ein Ausfluss der staatlichen Begierde, den Einfluss auf das Leben der Bürger auszudehnen.

Die Annahme, dass alle Kommunizierenden potenziell schuldig sind und daher präventiv überwacht werden müssen, entspricht einem unzulässigen Generalverdacht und hat in einem Rechtsstaat nichts verloren.

Fortschreitende Ausweitung der staatlichen Überwachung

Als Libertäre betrachten wir den Staat grundsätzlich kritisch. Für uns ist er nicht einfach ein wohlwollendes Schutzorgan. Vielmehr sind staatliche Behörden Zentren der Macht mit einem inhärenten Drang zur Ausweitung ihrer Kompetenzen. Die Entwicklungen der letzten Jahre und Jahrzehnte, namentlich der Wildwuchs an Regulierungen in jedem erdenklichen Bereich, das ausufernde Staatswachstum und die stetige Zunahme von Staatsangestellten zeigen dies eindrücklich.

Geschichte und Gegenwart belegen klar, dass einmal etablierte staatliche Massnahmen – insbesondere auch Überwachungsinstrumente – nie zurückgebaut, sondern stetig ausgeweitet werden. Die zuständigen Organe sind dabei äusserst kritisch im Erfinden neuer Bedrohungsszenarien. Während vor allem am Anfang des Jahrhunderts oft mit Terrorismus argumentiert wurde, geht es mittlerweile vermehrt um Pseudodelikte wie «hate speech», also um das Verhindern legitimer Meinungsäusserungen mittels staatlicher Repression.

Sicherheit durch Freiheit – nicht umgekehrt

Wer, wie manche «Law&Order»-Politiker, behauptet, dass Freiheit nur durch Sicherheit entstehen könne, verkennt, dass echte Sicherheit nicht durch allgegenwärtige Kontrolle sondern nur durch die Stärkung individueller Rechte und Verantwortlichkeiten entstehen kann. Die Menschheit hat in ihrer Geschichte verschiedene Szenarien durchlaufen, die klar belegen, wohin ein einseitiges Sicherheitsdenken führt.

Eine freie Gesellschaft, wie sie zur Schweiz passt, darf sich nicht durch hypothetische Bedrohungen in ein System von Kontrolle und Überwachung drängen lassen. Die Freiheit birgt immer Risiken, aber der Verlust der Freiheit ist das grösste Risiko von allen.

Verschlüsselung als legitimes Werkzeug zur Verteidigung der Freiheit

Die technischen Eigenschaften einer vernetzten Welt, bei der Datenpakete eine Vielzahl von Stationen durchlaufen und potenziell abgefangen werden können, machen eine Verschlüsselung von Inhalten unumgänglich, um das Recht auf Privatsphäre in der digitalen Welt zu wahren. Verschlüsselung ist nicht mehr als das digitale Pendant zu einem zugeklebten Couvert oder einer verschlossenen Haustüre und schützt Individuen vor unbefugtem Zugriff.

Ein Angriff auf die Verschlüsselung – in welcher Form auch immer, sei es durch Hintertüren, gesetzliche Bestimmungen oder Überwachungspflichten – ist aus unserer Sicht ein direkter Angriff auf das Recht des Einzelnen, sich vor Übergriffen zu schützen. Aus freiheitlicher Sicht ist es völlig unhaltbar, den Bürger dazu zu zwingen, seine Schutzmechanismen zu schwächen, nur damit der Überwachungsstaat seine Kontrollmöglichkeiten ausbauen kann.

Zur Teilrevision im Besonderen

Das BÜPF als eigentlicher Sündenfall

Die Libertäre Partei ist sich bewusst, dass es vorliegend um die Änderung von Verordnungen geht, die sich auf das Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) stützen. Dabei ist letztlich klar, dass nicht die ausführenden Verordnungen das Hauptproblem sind sondern das BÜPF an und für sich den eigentlichen Sündenfall darstellt.

Auch wenn dies nicht das Thema der Vernehmlassungsantwort ist, sei angemerkt, dass dieses eigentliche Überwachungsgesetz aus unserer Sicht nie hätte in Kraft treten dürfen, da es den oben erwähnten Grundsätzen diametral entgegensteht. Als besonders bittere Pille enthält es zudem zahlreiche Ausführungsbestimmungen, die dem Bundesrat einen grossen Spielraum zukommen lassen, beispielsweise wenn es um die Festlegung der Überwachungstypen geht.

Überwachungsausbau unter dem Deckmantel der Vereinfachung

Die Teilrevision wird in erster Linie damit begründet, dass Handlungsbedarf bei der Definition der Kategorien von Mitwirkungspflichtigen (MWP) bestehe. Gemäss der bundesrätlichen Mitteilung sei es das Ziel der Änderung, eine Angleichung zwischen Fernmeldedienstanbietern (FDA) und Anbieter abgeleiteter Kommunikationsdienste (AAKD) zu erreichen.

Konkret wird die Kategorie der AAKD in drei statt zwei Unterkategorien unterteilt, womit eine bessere Differenzierung der Hochstufungskriterien ermöglicht werde. Aus unserer Sicht

ist dies eine zurückhaltende Formulierung für die Tatsache, dass nun eine grössere Zahl von AAKD, die sich bisher mit weniger Pflichten konfrontiert sahen, hochgestuft werden können. Es geht also mehr um eine Ausweitung als um eine wirkliche Differenzierung.

Im Lichte der bundesgerichtlichen Rechtsprechung im Fall Threema ist es nicht unplausibel anzunehmen, dass nun auf dem Verordnungsweg versucht wird, Anbietern zusätzliche Pflichten aufzuerlegen.[1]

Neue Auskunftstypen: Ausbau der digitalen Überwachungsarchitektur

Die Revision soll ausserdem drei neue Auskunfts- und zwei neue Überwachungstypen schaffen[2]:

Im Rahmen dieser Revision werden auf Wunsch der Strafverfolgungsbehörden drei Auskunfts- und zwei Überwachungstypen neu geschaffen, dies um einerseits bestimmte Auskünfte und rückwirkende Überwachungen für die Benutzeridentifikation zu standardisieren, die bisher als Spezialfälle ausgeführt wurden, und andererseits bei Echtzeitüberwachungen die Möglichkeit zu schaffen, nur einen Teil der Inhaltsdaten zu überwachen:

- der Auskunftstyp IR_58_IP_INTERSECT: Benutzeridentifikation durch Schnittmengenbildung (Art. 38a VÜPF);
- der Auskunftstyp IR_59_EMAIL_LAST: Auskunft über den letzten Zugriff auf einen E-Mail-Dienst (Art. 42a VÜPF);
- der Auskunftstyp IR_60_COM_LAST: Auskunft über den letzten Zugriff auf einen anderen Fernmelde- oder abgeleiteten Kommunikationsdienst (Art. 43a VÜPF);
- der Überwachungstyp RT_61_NA_CC-TRUNC_IRI: Echtzeitüberwachung von Randdaten und gekürzten Inhalten bei Netzzugangsdiensten (Art. 55a VÜPF);
- der Überwachungstyp HD_62_IP: rückwirkende Überwachung zum Zweck der Teilnehmeridentifikation bei Internetverbindungen (Art. 60a VÜPF).

Diese Passage aus dem erläuternden Bericht belegt eindrücklich, was wir oben bereits bei den grundsätzlichen Überlegungen erwähnt haben. Die euphemistisch als «Wunsch» bezeichnete Gier der Behörden nach mehr Überwachung ist unstillbar. In vollständiger Eigendynamik fordern sie stets mehr und mehr und die Erosion von Grund- und Freiheitsrechten schreitet voran. Bezeichnend ist in diesem Zusammenhang, dass die Schaffung neuer Auskunftstypen auch damit begründet wird, dass bisher als Spezialfälle abgewickelte Formen der Auskunft so häufig geworden sind, dass nun eine Standardisierung als neuer Auskunftstyp angezeigt sei.[3]

Dies offenbart eine Praxis, bei der die Daten von Bürgern nicht nur im Rahmen konkreter Ermittlungen sondern zunehmend routinemässig «präventiv» abgefragt werden können. Die Kombination dieser Überwachungs- und Auskunftstypen erlaubt es, umfassende Bewegungs-, Kommunikations- und Verhaltensprofile von Individuen zu erstellen und ist damit rechtsstaatlich unhaltbar. Eine Vereinfachung und Standardisierung solcher Abfragen erhöht zudem das Risiko, dass sie immer häufiger und für immer weiter gefasste Zwecke eingesetzt werden.

Entfernung der Verschlüsselungen

Die Revision umfasst weiter Umschreibungen zur gesetzlichen Pflicht der Entfernung von anbieterseitigen Verschlüsselungen. Die Medienmitteilung des Bundesrats versucht hier, allfällige Sorgen zu zerstreuen, indem darauf hingewiesen wird, dass sogenannte Ende-zu-Ende-Verschlüsselungen nicht betroffen seien. Auch mit dieser Einschränkung bleibt die Entschlüsselungspflicht jedoch ein massiver Eingriff, da potenziell jede Form serverseitiger Verschlüsselung oder Transportverschlüsselung zwangsweise aufgehoben werden könnte.

Selbst wenn aktuell E2E-Verschlüsselungen noch nicht betroffen sind, bleibt abzuwarten, wie lange dies noch der Fall sein wird. Wie bereits beschrieben, werden staatliche Überwachungsansprüche ständig ausgeweitet. Es dürfte also eine Frage der Zeit sein, bis entsprechende Änderungen diskutiert werden.

Aus libertärer Optik ist Verschlüsselung nicht einfach eine technische Spielerei, sondern ein elementares Werkzeug der individuellen Freiheit. Das Recht, seine Kommunikation und Daten vor jedem Zugriff – insbesondere durch den Staat – zu schützen, sollte selbstverständlich und unverhandelbar sein.

Schwächung des Wirtschaftsstandorts

Bei der Begründung der Revision wird angeführt, dass durch die neuen Kategorien eine Vereinfachung für die Meldepflichtigen stattfinde. Dies ist selbstverständlich eine höchst ironische Aussage, denn am einfachsten wäre es für alle Unternehmen, wenn sie sich überhaupt nicht mit staatlichen Überwachungsmassnahmen auseinandersetzen müssten.

Realistisch ist hingegen, dass diese «Vereinfachung» dazu führt, dass bestimmte Anbieter von Kommunikationsdienstleistungen den Standort Schweiz als unattraktiv erachten und verlassen, wie Andy Yen, CEO der Proton AG gegenüber den Medien klar zum Ausdruck gebracht hat.[4]

Durch die zunehmende Drangsalierung von innovativen Unternehmen wie Proton oder Threema wird der Standort Schweiz somit deutlich geschädigt.

Fazit

Die geplante Revision ist kein harmloser technischer Anpassungsschritt sondern ein weiterer massiver Angriff auf die individuelle Freiheit und Privatsphäre der Bürger. Unter dem Vorwand von Schlagworten wie «Klarheit», «Verhältnismässigkeit», «notwendige Anpassungen» etc. wird ein immer feinmaschigeres Netz geschaffen, das mehr Anbieter, mehr Daten und mehr Kommunikationsformen unter staatliche Kontrolle bringt.

Neue Auskunftstypen, ausgeweitete Mitwirkungspflichten und verpflichtende Entschlüsselung führen zu einer Normalisierung der Überwachung und berauben den Rechtsstaat seiner grundsätzlich freiheitlichen Natur. Die Revision ist sinnbildlich für das

Postkonto

Kontonummer: 60-181123-3, Lautend auf: Libertäre Partei, 6340 Baar, IBAN: CH70 0900 0000 6018 1123 3, SWIFT/BIC: POFICHBEXXX, Bank: PostFinance AG, Mingerstrasse 20, 3030 Bern

Misstrauen des Staats gegenüber den eigenen Bürgern und ist ein weiterer Mosaikstein in einem immer weiter wachsenden Überwachungsapparat. Sie ist deshalb in ihrer Gesamtheit abzulehnen.

Wer die Sicherheit (oder die Illusion davon) über die Freiheit stellt, bekommt am Ende weder das eine noch das andere.

Einen freien Staat erkennt man daran, dass er nicht alles weiss – und es auch nicht wissen darf.

Freundliche Grüsse,

Libertäre Partei

Martin Hartmann
Präsident

Andreas Puccio
Ressort Politik

[1] Vgl. hierzu auch
<https://www.luzernerzeitung.ch/wirtschaft/ueberwachung-exklusiv-bei-diesen-diensten-will-der-bund-kuenftig-mitschnueffeln-ld.2744140>

[2] Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens, S. 6

[3] Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens, S. 36

[4] <https://www.netzwoche.ch/news/2025-04-15/genfer-firma-proton-ueberlegt-die-schweiz-zu-verlassen>

Postkonto

Kontonummer: 60-181123-3, Lautend auf: Libertäre Partei, 6340 Baar, IBAN: CH70 0900 0000 6018 1123 3,
SWIFT/BIC: POFICHBEXXX, Bank: PostFinance AG, Mingerstrasse 20, 3030 Bern

Vernehmlassung zu den Teilrevisionen der VÜPF und der VD-ÜPF

Datum	29.4.2025
Eingereicht von	Monzoon Networks AG
Kontaktperson bei Fragen (Name/Tel./E-Mail)	Beat Aeschlimann (+41 43 5000 472, beat.aeschlimann@monzoon.net)

Allgemeine Bemerkungen / Remarques générales / Osservazioni generali:

Wir begrüssen grundsätzlich die Teilrevisionen der VÜPF und der VD-ÜPF

JA NEIN

Vorbemerkung:

Bemerkungen zu einzelnen Artikeln der VÜPF

Nr.	Artikel	Antrag	Begründung / Bemerkung
VÜPF / OSCPT / OSCPT			
1	Art 16e i.V.m. Erläuterungsbericht Hinweis «Mikroblogging»	AAKD mit minimalen Pflichten sind von allen Regelungen VÜPF auszunehmen	<p>Im Erläuterungsbericht wird im Zusammenhang mit AAKD mit minimalen Pflichten auf «Microblogging-Dienste eingegangen und erläutert, deren Hauptfunktion « ... besteht in der Regel im öffentlichen Publizieren von Inhalten». «Bei direkten oder persönlichen Nachrichten ... » seien diese Dienste als AAKD einzustufen.</p> <p>Diese Einschätzung geht an der Realität vorbei.</p> <p>Insbesondere bei föderierten Diensten wie «Mastodon», «Pixelfed» o.ä. werden zehntausende von Klein-Instanzen durch Privatpersonen betrieben. Die genutzten Protokolle wie z.B. ActivityPub erlauben auch direkte und persönliche Nachrichten, auch wenn die Instanz nur als Single-User Instanz betrieben wird.</p> <p>Mit der geplanten Einstufung gem. Art. 16e sind allein in der Schweiz Hunderte von AAKDs mit minimalen Pflichten zu erwarten - die geplante Handhabung überschreitet damit jede Verhältnismässigkeit.</p>
2	Art 16h	<p>Der Begriff «Endbenutzer:in» ist durch den Begriff «Teilnehmende» zu ersetzen</p> <p>Die Abkürzung «PZD» ist einzuführen</p>	<p>Der Begriff «Endbenutzer:in» ist in VÜPF nicht definiert.</p> <p>VÜPF definiert in Anhang/Begriffe und Abkürzungen: «Teilnehmende: Personen, die mit einer FDA oder einer AAKD einen Vertrag über die Inanspruchnahme von deren Diensten geschlossen oder sich für deren Dienste registriert oder von dieser ein Zugangsmittel zu deren Diensten erhalten haben;»</p> <p>Konsequenterweise sollte – wie die Abkürzungen «FDA» und «AAKD» – auch die Abkürzung «PZD» in der VÜPF eingeführt werden.</p> <p>Folgerichtig müsste die Begriffsdefinition lauten: «Teilnehmende: Personen, die mit einer FDA, einer AAKD oder einer PZD einen Vertrag über die Inanspruchnahme von deren Diensten geschlossen oder sich für deren Dienste registriert oder von dieser ein Zugangsmittel zu deren Diensten erhalten haben;»</p> <p>Am Rande sei bemerkt, dass auch Teilnehmende in WLAN-Hotspots einen Zugangsvertrag schliessen, sei es konkludent bei Registrierung oder tatsächlich durch käuflichen Erwerb eines Zugangscodes.</p> <p>Zudem müsste Art 1, Abs.2, lit. (I) dann lauten: «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetzen Dritten zur Verfügung stellen (PZD);»</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
3	Art 16h, Abs. 2	Die Definition der maximal möglichen Endbenutzer ist zu streichen – die bisherige Definition der Grenze für «professionelle Nutzung» gemäss EJPD-Merkblatt ist beizubehalten	<p>Der geänderte Artikel hebt auf «Endbenutzer» ab. Ein «Endbenutzer» ist für den PZD jedoch keine technisch greifbare Definition, da technisch nur Endgeräte innerhalb der Systeme bekannt sind und «Endbenutzer» (i.S. von Personen) in aller Regel mehrere Endgeräte gleichzeitig «benutzen».</p> <p>Somit fehlt der beschriebenen Eigenschaft « ... kumuliert maximal mehr als 1000 Endbenutzerinnen und – benutzer ... » jegliche technische Parametrierungsmöglichkeit.</p> <p>Denkbare technische Parametrierungen wären:</p> <ol style="list-style-type: none"> 1. maximal assoziierte WLAN-MAC-Adressen 2. Grösse von IP-Subnetzen <p>(1) wird typischerweise von Hardwareherstellern nicht bekanntgegeben und ist deshalb ungeeignet (2) kann in jedem einfachen, privaten WLAN-Router nahezu beliebig gross ausfallen, ohne dass der - technisch nicht versierte – Eigentümer dies beurteilen kann. Dieser wird damit schnell zum PZD ohne sich dessen bewusst zu sein.</p> <p>Weiterhin ist diese «1000er»-Regelung nicht durch ÜPF nachprüfbar und kann somit beliebig leicht unterlaufen werden.</p> <p>Am Rande sei bemerkt: An WLAN-Hotspots können (auch durch «Endbenutzer») WLAN-zu-WLAN Router eingesetzt werden, welche eine beliebige – für den PZD nicht erkennbare – Menge weitere Endgeräte versorgen.</p> <p>Fazit: diese Regelung ist weder technisch umsetzbar noch seitens des Gesetzgebers nachprüfbar</p>
4	Art 19, Abs. 2	Die Regelung ist auf durch den FDA selbst professionell betriebene WLAN-Zugänge zu beschränken	Sofern der FDA den professionell betriebenen WLAN-Zugang nicht selbst betreibt, ist er technisch nicht in der Lage zu erkennen, ob der von ihm erbrachte Internetzugang für einen professionell betriebenen öffentlichen WLAN-Zugang genutzt wird. Es ist dem FDA weiterhin nicht zuzumuten, jeden von ihm erbrachten Internetzugang einmalig/wiederholt auf diesen Sachverhalt zu prüfen.

Der Präsident

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrat Beat Jans
Bundeshaus West
3003 Bern

Per E-Mail an:
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 29. April 2025

Stellungnahme der KKPKS zu den Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar 2025 haben Sie uns zur Stellungnahme in titelerwähnter Angelegenheit eingeladen. Wir bedanken uns dafür und nehmen wie folgt Stellung:

Die KKPKS befürwortet die Vorlage grundsätzlich und begrüßt zudem ausdrücklich den erfolgten Einbezug im Rahmen der Begleitgruppe Rechtsetzung. Die folgend beantragten Anpassungen einzelner Bestimmungen sowie Anregungen stützen sich auf die Einschätzung erfahrener Fachspezialisten, welche die vorgeschlagenen Änderungen dieses hoch technischen und komplexen Regelungsgegenstandes im Hinblick auf die Umsetzung in der Praxis beurteilt haben. Aufgrund der Komplexität der Materie würde es die KKPKS zudem, über die folgend beantragten Anpassungen hinaus, als wünschenswert erachten, wenn der Dienst ÜPF eine vereinfachte Übersicht zu den im Rahmen dieser Vorlage neu geschaffenen Möglichkeiten betreffend Auskunft sowie Überwachung ausarbeiten und diese in der Folge den kantonalen Strafverfolgungsbehörden zur Verfügung stellen würde. Nach Gesagtem gilt es nun konkret auf die einzelnen Bestimmungen der Vorlage einzugehen.

Konkrete Bestimmungen der aktuellen Vernehmlassungsvorlage

Art. 48b Abs. 2 VÜPF

Art. 48b Abs. 2 VÜPF hält fest, dass das Auskunftsgesuch die angefragten temporären Identifikatoren (z. B. SUCI, 5G-GUTI) und, soweit für die eindeutige Bestimmung des jeweiligen permanenten Identifikators notwendig, standortbezogene Angaben wie das zugehörige Mobilfunkgebiet, zu präzisieren hat. Gemäss dem erläuternden Bericht (S. 41) sei die Angabe des genannten Mobilfunkgebietes (Tracking Area) optional. Zwingend erforderlich sei die entsprechende Angabe hingegen im Fall einer Mehrfachverwendung einer angefragten SUCI. Hierzu gilt es festzuhalten, dass die ersuchende Behörde zum Zeitpunkt des Auskunftsgesuchs nicht weiß bzw. nicht wissen kann, ob eine Mehrfachverwendung einer SUCI vorliegt. Deshalb sollten die Anbieterinnen von Fernmeldediensten (FDA) sicherstellen, dass keine Mehrfachverwendung des temporären Identifikators (z. B. SUCI, 5G-GUTI) vorkommt. Darüber hinaus ist in der derzeitigen Vorlage nicht definiert, was im Fall einer Mehrfachverwendung einer angefragten SUCI im Mobilfunknetz als Antwort geliefert wird, wenn das Mobilfunkgebiet (Tracking Area) nicht im Auskunftsersuchen vorhanden war.

Der Präsident

Entsprechend beantragt die KKPKS, sowohl den neu aufgenommenen Einschub (*«und, soweit für die eindeutige Bestimmung des jeweiligen permanenten Identifikators notwendig»*) sowie auch die bereits bestehende Verpflichtung zur Präzisierung in Art. 48b Abs. 2 VÜPF aufzuheben und stattdessen festzuhalten, dass das Auskunftsgesuch keine Präzisierung der standortbezogenen Angaben zu enthalten hat.

Art. 48b Abs. 1 VÜPF

Weiteren Anpassungsbedarf sieht die KKPKS auch betreffend Art. 48b Abs. 1 VÜPF, welcher gemäss Vorentwurf unverändert bleibt. Gemäss Abs. 1 müssen heute bei einer Lokalisierung und insbesondere einer Notsuche jeweils alle temporären Identifikatoren abgefragt werden. Eine solche Abfrage würde jedoch die Datenbandbreite über die Mobilfunkstelle jeweils stark auslasten.

Damit künftig nicht mehr sämtliche temporären Identifikatoren im Rahmen einer Lokalisierung insbesondere einer Notsuche angefragt werden müssen, soll nach Ansicht der KKPKS neu automatisch ohne Anfrage und in Echtzeit der jeweilige temporäre Identifikator des gesuchten Mobilfunkgeräts geliefert werden. Damit würde die Datenbandbreite über die Mobilfunkluftschicht zwischen technischem Gerät (IMSI-Catcher) und Mobilfunknetzbetreiberin erheblich reduziert. Dies ist insbesondere deshalb von Relevanz, weil Notsuchen häufig in Gebieten mit eingeschränkter Mobilfunkversorgung stattfinden, in welchen nur eine geringe Datenbandbreite für die Übertragung zur Verfügung steht.

Deshalb beantragt die KKPKS, Art. 48b Abs. 1 VÜPF wie folgt zu ändern:

Art. 48b Abs. 1

Bei der Lokalisierung, insbesondere der Notsuche, wird ohne Anfrage der jeweilige aktuelle temporäre Identifikator des gesuchten Mobilfunkgerätes geliefert.

Art. 50 Abs. 9 VÜPF

Zuletzt ist der KKPKS aufgrund der bestehenden Vorlage unklar, wie die Präzisierung in Art. 50 Abs. 9 VÜPF in der Praxis umgesetzt werden soll. Bei einer aktiven Überwachung ist die Anordnung bereits abgeschlossen, weshalb beim Hinzukommen eines neuen Endgerätes (Multi-Device) oder einer neuen SIM (Extra-SIM) derzeit eine zusätzliche Anordnung zu erfolgen hat. Eine solche zusätzliche Anordnung wird in der Vorlage nun aber mit dem Zusatz *«im Rahmen desselben Auftrages»* gemäss Wortlaut ausgeschlossen. Vor diesem Hintergrund ersucht die KKPKS um Klärung, wie dieser Zusatz zu verstehen ist bzw. wie sich dieser auf das entsprechende Anordnungsverfahren auswirkt.

Anregungen in Bezug auf die bestehenden gesetzlichen Grundlagen

Die KKPKS möchte die vorliegende Vernehmlassung zudem zum Anlass nehmen, einige zentrale Punkte im Zusammenhang mit den bestehenden Identifikations- und Registrierungspflichten aufzugehen. Dies gerade auch mit Blick auf die Wirksamkeit der gesetzlichen Grundlagen in der Strafverfolgungspraxis.

Die Anregungen betreffen insbesondere die nach Ansicht der KKPKS fehlende Aufsichtspflicht des Dienstes ÜPF sowie die unpräzise Ausgestaltung der Anforderungen an die Identifikationsmittel und Überprüfungspflichten gemäss Art. 19 und 20 VÜPF. Die vorgeschlagenen Ergänzungen zielen auf eine verbesserte Datenqualität und eine stärkere Rechtsdurchsetzung in diesem sensiblen Bereich ab.

Der Präsident

Art. 19 VÜPF

Während in Art. 19 Abs. 1 und Abs. 2 VÜPF die FDA, die AAKD und auch die Wiederverkäuferinnen zur Einhaltung der Identifikationspflichten gesetzlich verpflichtet werden, fehlt eine analoge Verpflichtung gegenüber dem Dienst ÜPF. Zwar verpflichtet Art. 41 BÜPF den Dienst ÜPF zur Wahrung der Einhaltung der Gesetzgebung betreffend die Überwachung des Post- und Fernmeldeverkehrs und ermöglicht bei Rechtsverletzung entsprechende (auch vorsorgliche) Massnahmen anzurufen, jedoch zeigt sich in der Strafverfolgungspraxis, dass insbesondere bei den Registrierungsprozessen von Teilnehmenden (siehe folgend) der Dienst ÜPF diesen Aufsichtspflichten nur ungenügend nachkommt.

Deshalb beantragt die KKPKS, in Art. 19 VÜPF einen zusätzlichen Absatz aufzunehmen, der den Dienst ÜPF in vergleichbarer Weise wie die FDA, die AAKD und die Wiederverkäuferinnen verpflichtet, die noch zu definierenden, konkreteren Vorgaben (siehe folgend) zu kontrollieren und bei entsprechenden Verstößen zu intervenieren.

Art. 19 Abs. 1 und 2 VÜPF

Art. 19 Abs. 1 VÜPF hält fest, dass die FDA, die AAKD mit weitergehenden Auskunftspflichten, die AAKD mit weitergehenden Überwachungspflichten und die Wiederverkäuferinnen sicherzustellen haben, dass die Teilnehmenden mit geeigneten Mitteln identifiziert werden. Auch Art. 19 Abs. 2 VÜPF bedient sich der Ausdrucksweise «*geeignete Mittel*». Was unter «*geeigneten Mitteln*» zu verstehen ist, wird in der Verordnung nicht ausgeführt und ist soweit ersichtlich auch nicht näher definiert. Einzig dem erläuternden Bericht (S. 30 f.) lässt sich eine beispielhafte Aufzählung entnehmen. Hierzu ist festzuhalten, dass in der Strafverfolgungspraxis bereits seit längerer Zeit erhebliche Schwierigkeiten bei der Einhaltung der Registrierungspflichten sowie bei der durch die Registrierung angefallenen mangelhaften Datenqualität auftreten. Da nur ungenügende Vorgaben hinsichtlich dieser «*geeigneten Mittel*», aber auch dahingehend wer solche Registrierungen vornehmen kann, bestehen, ergeben sich diesbezüglich zwischen den FDA, AAKD und den Wiederverkäuferinnen grosse Unterschiede. Diese Umstände führen zu zahlreichen – auch erwiesenen – Falschregistrierungen, was wiederum negative Auswirkungen auf die Ermittlungsergebnisse der Strafverfolgungsbehörden hat.

Entsprechend beantragt die KKPKS, in Art. 19 Abs. 1 und 2 VÜPF den unbestimmten Begriff von «*geeigneten Mitteln*» weiter zu präzisieren, indem in der Verordnung oder zumindest in einem Anhang zur Verordnung konkrete Vorgaben zu den verwendeten Mitteln, zur Qualitätsprüfung wie auch zum Bezug Dritter (Identifikationsanbieter) festgehalten werden.

Art. 20 Abs. 3 VÜPF

Art. 20 Abs. 3 VÜPF hält fest, dass die FDA die ordnungsgemäße Registrierung und Identifizierung der oder des Teilnehmenden durch die Wiederverkäuferin sowie die Weiterleitung dieser Informationen an die FDA «*in geeigneter Weise*» überprüft. Anknüpfend an die vorstehend geschilderte Problematik betreffend Falschregistrierungen zu Art. 19 Abs. 1 und Abs. 2 VÜPF ergibt sich eine ähnliche Unbestimmtheit, die weiter zu konkretisieren ist.

Vor diesem Hintergrund beantragt die KKPKS, den in Art. 20 Abs. 3 VÜPF enthaltenen, unbestimmten Begriff «*in geeigneter Weise*» zu präzisieren, indem in der Verordnung oder zumindest in einem Anhang zur Verordnung konkrete Vorgaben zur Art und Weise der vorzunehmenden Überprüfungs pflicht sowie zur Qualitätssicherung der FDA festgehalten werden.

Diese Anpassungen würden die Wirksamkeit der bestehenden Identifikations- und Registrierungspflichten in der Strafverfolgungspraxis erhöhen.

Der Präsident

Besten Dank für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Der Präsident

Matteo Cocchi, Kdt Kantonspolizei Tessin

Kopie: Mitglieder der KKPKS, GS KKJPD, GS SSK

Von: Cédric Honegger <ch@macrogram.ch>

Gesendet: Donnerstag, 1. Mai 2025 16:27

An: Biberstein Jean-Louis ISC-EJPD <jean-louis.biberstein@isc-ejpd.admin.ch>

Betreff: Surveillance des télécommunications

Monsieur,

Permettez-moi de réagir en lien avec cette publication :

<https://www.news.admin.ch/fr/nsb?id=103968>

Je suis interloqué qu'aujourd'hui encore, des technocrates zélés en mal de pouvoir tentent discrètement en coulisse, d'espionner la population suisse.

Au niveau de l'ampleur, ce projet dépasse largement un autre exemple du passé : le scandale des fiches.

<https://www.rts.ch/info/suisse/10886146-le-scandale-des-fiches-eclatait-en-suisse-il-y-a-tout-juste-trente-ans.html>

Selon moi, ce projet est un non-sens car :

1.

Les organisations criminelles visées trouveront ou ont déjà trouvé d'autres moyens de communiquer. Ce sera donc inefficace.

2.

Les entreprises légitimes du pays sauront que le secret des affaires est compromis. Une partie fera le choix bien triste de déménager au moins une partie de leur infrastructure.

3.

La population saura également qu'elle est surveillée à très large échelle et en temps réel. Cela induira une défiance totalement compréhensible envers les autorités.

Pour un sujet de cette importance, il s'agit que le peuple soit consulté via une votation. La mise en place de tels outils via une simple loi ou ordonnance est inacceptable.

Meilleures salutations,

MACROGRAM SA

Cédric Honegger

Tel: +41 -21 657 1434

www.macrogram.ch

Digitale Gesellschaft, CH-4000 Basel

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
CH-3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Basel, 2. Mai 2025

Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat Beat Jans
Sehr geehrte Empfänger:innen

Am 29. Januar 2025 eröffnete der Bundesrat die Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF). Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Vorentwurf wie folgt Stellung:

Vorbemerkung

Die geplante Revision der VÜPF ist ein Frontalangriff auf unsere Grundrechte, die Rechtsstaatlichkeit sowie den IT- und Innovationsstandort Schweiz.

Mit ihrer Umsetzung würde geltendes Recht in einem Ausmass verletzt, das alarmieren muss: Die Revision ist in vielerlei Hinsicht unvereinbar mit dem Bundesgesetz betreffend die Überwachung des

Post- und Fernmeldeverkehrs (BÜPF), verstösst gegen das Datenschutzgesetz (DSG), steht in klarem Widerspruch zu den verfassungsmässigen Grundrechten und verstösst gegen Völkerrecht. Die vorgesehenen Änderungen führen zu einer massiv ausgeweiteten Überwachung – ganz grundsätzlich und flächendeckend. Dies ist mit der Ausrichtung des BÜPF, das eine fein austarierte Interessenabwägung zwischen Freiheit und Privatsphäre einerseits und Sicherheit durch Überwachungsmassnahmen andererseits verfolgt, absolut nicht vereinbar.

Die Auswirkungen auf den Wirtschafts- und Innovationsstandort Schweiz wären verheerend: Die Ausweitung der Überwachung und die damit verbundenen, übermässigen Mitwirkungspflichten machen die Schweiz für IT-Anbieter äusserst unattraktiv. Renommierte Unternehmen wie Proton oder Threema, deren Geschäftsmodelle durch die Vorlage direkt ins Visier geraten, würden in ihrer Existenz bedroht. Die ersten Konsequenzen sind bereits sichtbar: Proton hat angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen (siehe [Tages-Anzeiger vom 1. April 2025](#)). Der Chef des Unternehmens erklärte in einem Interview: «Diese Entscheidung ist wirtschaftlicher Selbstmord für die Schweiz» ([watson.ch vom 9. April 2025](#)). Ähnlich äussert sich Threema-Chef Robin Simon: «Der Wirtschaftsstandort würde durch die Revision geschwächt und für Tech-Start-ups unattraktiv.» Aktuell lasse sich Threema alle Optionen offen ([Tages-Anzeiger vom 8. April 2025](#)). Diese Warnzeichen sind ernst zu nehmen und zeigen das verheerende Ausmass der geplanten Revision.

Neben den verheerenden wirtschaftlichen Auswirkungen wird gleichzeitig der grundrechtlich garantierte Anspruch auf sichere und vertrauliche Kommunikation ausgehöhlt. Wenn Anbieterinnen abwandern, bleibt jedoch – als wäre dies nicht genug – nicht nur privaten Nutzer:innen der Zugang zu geschützten Kommunikationsmitteln verwehrt.

Ebenso betroffen sind auch Personen, die einem Berufsgeheimnis unterstehen, wie Journalistinnen oder Anwälte. Die Änderungen treffen zudem schutzbedürftige Personengruppen besonders hart: Whistleblower:innen, Menschen mit ungeklärtem Aufenthaltsstatus oder ohne Papiere aber auch Aktivist:innen verlieren ebenso den Zugang zu vertraulichen Kommunikationsmitteln. Die Revision ignoriert diese Schutzbedürfnisse und erweitert stattdessen die Eingriffsbefugnisse des Staates in einer Weise, die hochgefährlich ist.

Besonders widersprüchlich erscheint das Vorgehen des Bundes angesichts der Tatsache, dass ausgerechnet der Bundesrat selbst Threema als Messenger nutzt – ein Dienst, den er nun faktisch aus dem Markt drängt. Damit sägt die Regierung ausgerechnet an jenem Ast, auf dem sie in Sachen sicherer Kommunikation bislang selbst sitzt.

Hinzu kommt: Die geplanten Regelungen sind technisch unausgereift, unnötig komplex und in Teilen schlüssig nicht umsetzbar. Vielmehr wird ein kaum noch durchschaubares Normengeflecht geschaffen, das weder den Mitwirkungspflichtigen noch den Betroffenen ein Mindestmass an Rechtsklarheit bietet. Die Revision wird ausserdem präsentiert, als handle es sich dabei um Änderungen zur besseren Überblickbarkeit der Rechtslage und zur Schaffung von mehr Rechtssicherheit - tatsächlich aber wird der persönliche Anwendungsbereich der Mitwirkungspflichtigen enorm erweitert und eine Vielzahl neuer Anbieterinnen in den Kreis der Mitwirkungspflichtigen einbezogen. Von Transparenz kann nicht die Rede sein.

Es ist im Übrigen nicht haltbar, dass eine dermassen breit angelegte Ausweitung von Pflichten auf Verordnungsstufe angelegt wird. Solch einschneidende Veränderungen mit weitreichenden Konsequenzen sind in Gesetzesform zu erlassen. Der Bundesrat überschreitet seine Kompetenzen hier um ein Weites.

Diese Vorlage schwächt nicht nur den Innovations- und Wirtschaftsstandort Schweiz – sie untergräbt gleichzeitig im grossen Stil verfassungsmässig geschützte Rechte. Aus grundrechtlicher, datenschutzrechtlicher und gesellschaftspolitischer Sicht ist sie schlicht inakzeptabel. Die geplanten Änderungen stehen dem erklärten Ziel von mehr Freundlichkeit sowie allgemeinen rechtsstaatlichen Grundsätzen sowie Schutzbedürfnissen Einzelner diametral entgegen.

Deshalb lehnen wir die Revision vollumfänglich und in aller Deutlichkeit ab.

Bemerkungen zu einzelnen Artikeln der VÜPF

Alle Artikel

Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung (Art. 6 Abs. 3 DSG) gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kund:innen auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.

Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.ä. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.

Antrag: Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.

Art. 16b Abs. 1

Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile (Art. 16b Abs. 1 lit. b Ziff. 2 VE-VÜPF) wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Mitwirkungspflichten in Kauf nehmen.

Dazu kommt, dass das Kriterium bezüglich der Überwachungsaufträge nicht vom BÜPF gestützt wird, denn: Die Anzahl von Überwachungsaufträgen ist von der wirtschaftlichen Bedeutung einer FDA völlig losgelöst. Die wirtschaftliche Bedeutung ist aber gemäss Art. 26 Abs. 6 BÜPF ausschlaggebend dafür, ob eine FDA von den vollen Pflichten (teilweise) befreit werden kann. Im Umkehrschluss ist die wirtschaftliche Bedeutsamkeit somit Erfordernis für die Auferlegung von vollen Pflichten. Wenn eine FDA nun aber rein aufgrund einer bestimmten Anzahl von Überwachungsaufträgen nach Art. 16b Abs. 1 lit. b Ziff. 1 VE-VÜPF als vollpflichtige FDA qualifiziert wird, steht dies im Widerspruch zum BÜPF und entbehrt damit einer Rechtsgrundlage.

Dieses bereits in der aktuellen Version der VÜPF vorhandene Problem sollte im Zuge einer Revision nicht bestehen bleiben, sondern muss behoben werden.

Antrag: Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter

Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.» Es ist auf die Regelung in Art. 26 Abs. 6 BÜPF abzustellen und eine Einzelfallbetrachtung zur Einstufung vorzunehmen.

Art. 16c Abs. 3

Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als «natürliche» Schutzmechanismen gegen eine übermässige oder missbräuchliche Nutzung solcher Massnahmen durch die Untersuchungsbehörden. Die automatisierte Erteilung von Auskünften ist unverhältnismässig und widerspricht dem Prinzip der Datenminimierung. Die pauschale und undifferenzierte Regel beeinträchtigt zwangsläufig den Grundrechtsschutz.

Der vorgesehene Umsetzungszeitraum von 12 Monaten zur Umsetzung eines dermassen komplexen Systems ist ausserdem völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.

Antrag: Streichung von lit. a «automatisierte Erteilung der Auskünfte» (ebenso in Art. 18 Abs. 2).

Art. 16d

Gemäss erläuterndem Bericht stellen Kommunikationsdienste, die nicht zu den in Art. 16a Abs. 1 aufgezählten Fernmeldediensten gehören und auf die die Ausnahmen nach Art. 16a Abs. 2 nicht zutreffen, abgeleitete Kommunikationsdienste dar. Diese klarere Definition des Begriffs AAKD ist begrüssenswert, doch ist die Konkretisierung der abgeleiteten Kommunikationsdienste im erläuternden Bericht einerseits rechtsstaatlich problematisch und andererseits geht die neue Auslegung nach den Ausführungen im erläuterndem Bericht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdielen wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter etc.) genutzt werden.

Art. 2 lit. c BÜPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft jedoch auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug in die Auslegung unrechtmässig ist – auch hier setzt sich die Revision inakzeptabel über die gesetzlichen Vorgaben des BÜPF hinweg. Onlinespeicherdielen sind deshalb aus Art. 16d zu streichen.

Zudem anerkennt der erläuternde Bericht zwar, dass VPNs zur Anonymisierung der Nutzer:innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil angebrachte Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Das Bedürfnis, auch künftig VPN-Dienste in Anspruch nehmen zu können, ist zu schützen und darf nicht vereitelt werden. Anbieter von VPNs sind daher ebenfalls aus Art. 16d auszunehmen.

Es ist irritierend, dass die bewusst separat ausgestalteten Kategorien AAKD und FDA einander zunehmend angeglichen werden, und zwar zuungunsten der AAKD, die als Kategorie mit grundsätzlich weniger weitreichenden Pflichten als die FDA konzipiert wurde. Dies missachtet den Willen des Gesetzgebers, den es zu wahren gilt.

Antrag: Streichung von Onlinespeicherdiensten und VPN-Anbieterinnen aus der Aufzählung der möglichen abgeleiteten Kommunikationsdienste in den Ausführungen zu Art. 16d im erläuternden Bericht und in der Auslegung.

Art. 16e, Art. 16f und Art. 16g

Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch komplett entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung mit deutlich erweiterten Pflichten. Entscheidend ist, dass neuerdings das Kriterium von 5'000 Nutzer:innen allein zum Auferlegen massiver Überwachungspflichten ausreicht: Erreicht eine AAKD diese Grösse, fällt sie neu in die Kategorie der AAKD mit reduzierten Pflichten und untersteht somit bereits sehr weitgehenden Mitwirkungspflichten, insbesondere der Identifikationspflicht.

Die Einführung von 5'000 Nutzer:innen als gesondert zu beurteilende Untergrenze verletzt Art. 27 Abs. 3 BÜPF, denn 5'000 Personen sind keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strengereren Überwachungsmassnahmen, gerechtfertigt wären. 5'000 Nutzer:innen werden in der digitalen Welt vielmehr sehr rasch erreicht – die Revision verkennt technische Realitäten.

Zusätzlich führt das Einführen eines Konzernatbestandes in Art. 16f Abs. 3 zu massiven Problemen: Produkte und Dienste müssen nicht mehr für sich allein bestimmte Schwellenwerte erreichen – es genügt, wenn das Mutterunternehmen oder verbundene Gesellschaften diese überschreiten. Insbesondere bei Unternehmen mit Beteiligungsstrukturen führt dies dazu, dass sämtliche Angebote pauschal der höchsten Überwachungsstufe unterstellt werden – unabhängig davon, ob sich einzelne Dienste noch im frühen Entwicklungsstadium befinden oder faktisch kaum genutzt werden. Somit müsste jedes neue Projekt von Beginn an mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden, was Innovation behindert. Zudem missachtet der Konzernatbestand das Verhältnismässigkeitsgebot: Unterschiedliche organisatorische Einheiten mit eigenständigen Angeboten werden unrechtmässig zusammengefasst, obwohl sie individuell zu prüfen wären. Die Anwendung starrer Schwellen auf ganze Konzerne statt auf einzelne Dienste umgeht eine notwendige Einzelfallprüfung.

Eine solche Regelung stünde sodann *im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali*, das die zu seltene Anwendung von Downgrades kritisierte:

«Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»

Statt KMU zu entlasten, führt die Revision neu zu einem «automatischen» *Upgrade per Verordnung ohne Verfügung* (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.

Eine Analyse der offiziellen VÜPF-Statistik unterstreicht diese offensichtliche Unverhältnismässigkeit. Im Jahr 2023 betrafen 98,97% der total 9'430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,03% für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,74% wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100% des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.

Die neue Vorlage schliesst nun ebenfalls sowohl die Registrierung via normaler E-Mail als auch die komplett anonyme Registrierung (z. B. Signal oder Telegram) aus, da AAKD bereits mit reduzierten Pflichten neu automatisch zwingend die Endnutzer:innen identifizieren müssen. Hiervon betroffen sind nicht nur alle AAKD mit reduzierten Pflichten, sondern auch all deren Wiederverkäufer. Faktisch resultiert das Gesetz somit darin, dass man sich bei keinem Dienst mehr anmelden können soll, ohne den Pass, Führerschein oder die ID entweder direkt oder indirekt zu hinterlegen. Dass Nutzer:innen künftig hierzu gezwungen wären, stellt einen massiven Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 BV) dar und ist unzumutbar.

Ein weiteres Kernproblem, das die automatische Hochstufung mit sich bringt, ist die Rechtsunsicherheit. Die Vorlage will mit klarer definierten Kategorien und Pflichten ein übersichtlichere Situation schaffen, verfehlt dieses Ziel jedoch gänzlich. Bislang fand die Hochstufung per Verfügung statt, wodurch es für die Mitwirkungspflichtigen klar erkennbar war, wann sie unter welche Pflichten fallen. Ausserdem bewirkt diese Praxis eine sinnvolle Einzelfallbetrachtung anstelle pauschaler und unzweckmässiger automatischer Hochstufungen. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den massgebenden Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes kann aber im Zweifelsfall nur schwer zu beantworten sein. Gerade deshalb besteht ein schutzwürdiges Interesse der Anbieter an Klarheit über ihre Pflichten, da sie fortan eventuell die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Diese Umstrukturierung lässt ich nicht mit der Funktionsweise von Verwaltungsverfahren vereinbaren. Die Pflicht zur Abklärung, wann eine Hochstufung vorliegt und was diese für das Unternehmen bedeutet, darf nicht in die Verantwortung der Unternehmen fallen. Der Staat zieht sich hier aus der Verantwortung und schiebt diese den Unternehmen zu, wodurch diesen zwangsläufig zeitlicher und finanzieller Mehraufwand entsteht. Von einer automatischen Hochstufung von AAKD ist daher abzusehen.

Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.

Gegenüber der geltenden VÜPF *erweitert die Revision die Pflichten zur Automatisierung noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragetypen wie z. B. "IR_59" und "IR_60", welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen.* Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.

Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 lit. b der geltenden VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grosse[n] Teil ihrer

Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. *Damit fallen auch Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz.*

Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Auch hiermit werden neue Hürden für Innovation geschaffen. Die Regelung ist unverhältnismässig und nicht sachdienlich.

Auch Non-Profit-Organisationen geraten unter die verschärften Vorgaben. Unter den neuen Kriterien wird aber allein auf die Anzahl der Nutzer:innen abgestellt für die Einstufung als AAKD. Dieses Kriterium greift jedoch zu kurz: Es berücksichtigt insbesondere nicht die wirtschaftliche Tragfähigkeit der Anbieter:innen. Gerade bei Open-Source- und Non-Profit-Lösungen mit grosser Reichweite, aber geringem Budget, führt dies zu einer verheerenden finanziellen Belastung: Anbieter:innen mit solchen Projekten würden gezwungen, umfangreiche Überwachungsmassnahmen einzuführen. Solche Anbieter:innen würden gezielt aus dem Schweizer Markt gedrängt, während gleichzeitig bestehende Monopole wie WhatsApp (96% Marktanteil in der Schweiz) gestärkt würden.

Es muss ausserdem klar festgehalten werden, dass sich das BÜPF und die VÜPF nur auf Anbieter:innen beziehen können, die in der Schweiz tatsächlich tätig sind. Die Erlasse dürfen nicht so ausgelegt werden, dass sie eine extraterritoriale Wirkung entfalten und internationale Dienste wie Signal, WhatsApp oder Microsoft Teams erfasst sind.

Das Kriterium der reinen Nutzer:innenzahl ist ungeeignet und muss gestrichen werden.

Die Regelung schwächt auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade us-amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger:innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, End-zu-End-verschlüsselter Kommunikation ist heute wichtiger denn je und fällt in den Bereich grundrechtlich geschützter Ansprüche, die es zu wahren gilt. Diese Ansprüche dürfen nicht aufs Spiel gesetzt werden, um ein knallhartes Überwachungsregime der Kommunikation in der Schweiz durchzusetzen – die Prioritäten werden höchst fragwürdig gesetzt.

Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade illegal ist (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer:innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, diese zu erhebenden Datenmengen sind von enormem Ausmass und bergen folglich massive Risiken für Hackerangriffe.

Des Weiteren ist nicht belegt, dass die Speicherung der betreffenden Daten zu spürbar mehr erfolgreichen Ermittlungen führt. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisshandlung via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfüge, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.

Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren. Diese Handhabe bedeutet einen Verstoss gegen das Legalitätsprinzip und untergräbt legislative Kompetenzen. Ausserdem verfügt die Schweiz bereits über reichlich Mittel zur Aufklärung und Verfolgung von Straftaten, die Behörden können bereits heute auf sicherheitsrelevante Daten zurückgreifen. Unternehmen wie Proton (s. «Positionspapier zur Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)» von Proton) kooperieren seit Jahren mit den Schweizer Strafverfolgungsbehörden und dem Nachrichtendienst des Bundes (NDB). Wenn nun solche Unternehmen aus bereits genannten Gründen zur Abwanderung gezwungen werden, bewirkt die Revision auch hier das genaue Gegenteil ihrer erklärten Ziele: Anstatt der Schaffung besserer Möglichkeiten zur Strafverfolgung würden die Schweizer Behörden wie etwa Fedpol den Zugriff auf wichtige Partner bei der Beschaffung sicherheitsrelevanter Daten verlieren.

Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Integrität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.

Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das DSG. Der Entwurf bringt nicht, wie der Begleitbericht den Leser:innen weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit, steht in direktem Gegensatz zum besagten Postulat 19.4031 und bedeutet massive Eingriffe in grundrechtlich geschützte Sphären, sowohl von Unternehmen als auch von Nutzer:innen.

Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen und das bestehende System muss beibehalten werden.

Antrag: Streichung der Artikel und Beibehaltung der bestehenden Kriterien und der zwei Kategorien von AAKD. + Ausnahmen für Pilotprojekte (auch von grossen Firmen) und Non-Profits per se. Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).

Art. 16h

Art. 16h konkretisiert die Kategorie der «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» aus Art. 2 lit. e BÜPF. Die Vorschrift verfehlt ihr Ziel – anstatt Unsicherheiten darüber zu beheben, wer unter diese Kategorie fällt, schafft sie weitere Unklarheiten. Der schwammig formulierte Verordnungstext könnte dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist:innen, Whistleblower:innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber:innen solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer:innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen.

Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt. Die Unklarheit bezüglich der Einordnung von TOR-Servers wirft weitere Fragen auf, denn wenn TOR nicht als PZD zu qualifizieren

ist, müsste TOR – gleich wie die VPNs – der Kategorie der AAKD zugeordnet werden. Somit stünden Betreiber:innen von TOR-Servern – wie etwa die Digitale Gesellschaft – unter der Identifikationspflicht. Diese ist jedoch, wie dargelegt, nicht umsetzbar.

Es braucht somit entweder die Zusicherung, dass Betreiberinnen von TOR-Nodes nicht dem BÜPF und der VÜPF unterstellt sind oder aber Kategorien von Mitwirkungspflichten, die so gestaltet sind, dass ein:e Betreiber:in eines TOR-Nodes nicht einer Identifikationspflicht unterstellt wird – z. B. indem die Schwelle für das Auferlegen der Identifikationspflicht auf 1 Mio. Nutzer:innen angehoben wird.

Wären Betreiber:innen von TOR-Nodes von der Identifikationspflicht erfasst, würde dies fundamentale Grundrechte wie das Recht auf Privatsphäre und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK), die Meinungs- und Informationsfreiheit (Art. 16 BV, Art. 10 EMRK) gefährden. Ebenso würde das datenschutzrechtliche Prinzip der Datensicherheit (Art. 8 DSG) komplett unterlaufen. Diese Eingriffe in national und international geschützte Rechtsansprüche sind nicht hinzunehmend.

Dieser potentielle Angriff auf die genannten Grundrechte ist hochproblematisch und setzt ein politisches Statement: Die Schweiz bewegt sich weg von Grundrechtsschutz hin zum hochgerüsteten Überwachungsstaat.

Antrag: Es muss sichergestellt werden, dass Technologien wie TOR oder I2P nicht vom Anwendungsbereich der VÜPF erfasst sind.

Art. 16h Abs. 2

Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Endbenutzer:innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 VE-VÜPF: Gemäss diesem Artikel trägt die das WLAN erschliessenden FDA die Verantwortung zur Identifikation der Nutzer:innen. Die Regelung führt also dazu, dass FDA, die einen Vertrag haben mit «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» (PZD), sehr schnell für die Identifikation der Endnutzer:innen ihrer Vertragspartner zuständig sind. Diese Regelung ist unsinnig und schlicht nicht umsetzbar.

Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer:innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24), die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22) oder der Verwendung von IPv6. Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDA unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden.

Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten: FDA resp. Anbieterinnen von öffentlichen WLAN-Zugängen dürfen nur unter einer Identifikationspflicht stehen, wenn die PZD, die den Zugang der FDA nutzt, «professionell betrieben» ist – und zwar nach der aktuellen Auslegungsform (s. Erläuternder Bericht zur (letzten)Totalrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs):

«Mit «professionell betrieben» ist gemeint, dass eine FDA oder eine auf öffentliche WLAN-Zugangspunkte spezialisierte IT-Dienstleisterin den technischen Betrieb des öffentlichen WLAN-

Zugangspunktes durchführt, die dies auch noch für andere öffentliche WLAN-Zugangspunkte an anderen Standorten macht. Wenn eine natürliche oder juristische Person an ihrem Internetzugang selbst einen öffentlichen WLAN-Zugangspunkt technisch betreibt und diesen Zugang Dritten zur Verfügung stellt, muss die FDA, die den Internetzugang anbietet, keine Identifikation der Endbenutzenden sicherstellen.»

So wird sichergestellt, dass FDA nicht unmöglich umzusetzenden Pflichten unterstellt werden.

Antrag: Streichung der Ausführung im erläuternden Bericht. Das Kriterium «professionell betrieben» ist nach der bislang geltenden Regelung zu verstehen. Art. 16h Abs. 2 ist ersatzlos zu streichen und im Zusammenhang mit Art. 19 Abs. 2 ist auf die aktuelle Definition von «professionell betrieben» abzustellen.

Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2

Bei Konzernen knüpft die VE-VÜPF nicht mehr an die Umsatz- und Nutzer:innenzahlen des betroffenen Unternehmens an, neu sind die Zahlen des Konzerns ausschlaggebend für eine Hoch- oder Herunterstufung. Die Begründung, dies diene der Vereinfachung, ist unlogisch und irreführend: Unternehmen müssen ihre Zahlen ohnehin produktbezogen ausweisen, die nötigen Daten liegen also längst vor. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.

Antrag: Streichung des «Konzernatbestand» und Beibehaltung der bestehenden Regelung.

Art. 19 Abs. 1

Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD – erfasst sind die AAKD mit reduzierten und mit vollen Pflichten – widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht. Durch die neuen Schwellenwerte zur Einstufung findet eine beachtliche Ausweitung der Identifikationspflicht statt.

Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des DSG, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch insbesondere der Grundrechtsschutz von Nutzer:innen in der Schweiz massiv beeinträchtigt wird. Die Identifikationspflicht greift immens in das Recht auf informationelle Selbstbestimmung ein und hält einer Grundrechtsprüfung nach Art. 36 BV schon allein aufgrund ihrer Unverhältnismässigkeit nicht stand.

Bezüglich einschneidender Pflichten, die potentiell schwere Grundrechtseingriffe bedeuten – wie es bei Identifikationspflichten zweifellos der Fall ist – muss Rechtsetzung in jedem Fall mit äusserster Sorgfalt und unter strenger Beachtung des Verhältnismässigkeitsgebots erfolgen. Außerdem darf sich eine solche Pflicht nicht über gesetzliche Vorgaben, wie in diesem Fall vom BÜPF vorgegeben, hinwegsetzen.

Durch die breite Auferlegung einer solchen Pflicht werden datenschutzfreundliche Unternehmen bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird. Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Nur so können datenschutzrechtliche Vorgaben und die Rechte Betroffener gewahrt werden.

Antrag: Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation von Teilnehmenden.

Art. 18

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 19 Abs. 2

Das Kriterium «professionell betrieben» ist nach der bestehenden Regelung auszulegen (s. vorstehen). Es sei ausserdem darauf hingewiesen, dass sich aus dieser Regelung eine vertragsrechtliche Problematik zwischen den FDA und den PZD ergeben würde, die nicht tragbar ist.

Antrag: Auslegung des Kriteriums «professionell betrieben» nach der bestehenden Regelung und nicht i. S. v. Art. 16h Abs. 2.

Art. 21 Abs. 1 lit. a

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.

Antrag: Streichung

Art. 22

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.

Antrag: beibehalten

Art. 11 Abs. 4

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.

Antrag: Streichung

Art. 16b

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.

Antrag: Streichung

Art. 31 Abs. 1

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 51 und 52

Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.

Antrag: beibehalten

Art. 60a

Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde laut den Erläuterungen bewusst auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten. Art. 60a ist zu streichen.

Antrag: Streichung des Artikels

Art. 42a und 43a

Die Art. 42a und 43a führen neu die Abfragetypen «IR_59» und «IR_60» ein, über die sensible Daten automatisiert abgefragt werden können. Sie verlangen von Anbietern, dass sie jederzeit Auskunft geben können bezüglich des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Auch für das Auferlegen dieser Pflicht gilt die fragliche Schwelle von 5'000 Nutzer:innen. Erfasst ist somit nahezu die gesamte AAKD-Landschaft der Schweiz.

Das Problem liegt darin, dass die «IR_»-Abfragen zu Informationen nach Art. 42a und 43a neu automatisiert abgerufen werden können – im Gegensatz zu den «HD_»- (historische Daten) und «RT»- (Echtzeitüberwachung) Abfragen, die strengeren Regeln und einer juristischen Kontrolle unterliegen.

Bei den «IR_59»- und «IR_60»-Abfragen handelt es sich allerdings um sensible Informationen wie etwa das Abrufen einer IP-Adresse. Solche Informationen mussten bislang zurecht über strengere Abfragetypen eingeholt werden. Es ist nicht nachvollziehbar, warum Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber. Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser automatisierten Auskünfte ergibt. Unternehmen sind daher nur unzulänglich geschützt vor missbräuchlichen Anfragen und vor Kosten, die ihnen durch die Pflicht, diese Auskünfte automatisch weiterzugeben, entstehen wird.

Künftig könnten so umfangreiche Informationen über die neuen Abfragetypen beschafft werden, die bislang zurecht den strengerem Regeln der rechtlich sichereren Informations-/Überwachungstypen «HD_» und «RT_» unterworfen waren. «IR_59» und «IR_60» ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne den erforderlichen Kontrollen dieser invasiven Überwachungstypen unterworfen zu sein.

Die Entwicklung, dass mittels «IR_»-Abfragen neu auch personenbezogene sensible Nutzungsdaten eingeholt werden können, widerspricht der Logik der unterschiedlichen Abfragetypen und öffnet Tür und Tor für missbräuchliche Abfragen und eine Echtzeitüberwachung von Millionen von Nutzer:innen. Auch hier stehen grundrechtlich geschützte Ansprüche auf dem Spiel, die mit einer solchen Regelung auf nicht nachvollziehbare Weise untergraben und missachtet werden.

Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind. Die AAKD müssten künftig gewisse Datenkategorien systematisch erheben, um dieser Pflicht nachzukommen. Art. 27 Abs. 2 BÜPF erklärt allerdings, dass AAKD «auf Verlangen die *ihnen zur Verfügung stehenden* Randdaten des Fernmeldeverkehrs der überwachten Person liefern» müssen. Bei einer dahingehenden Auslegung des Bestimmungen bedeutete dies einen weiteren Verstoss gegen das BÜPF.

Unter rechtsstaatlichen Gesichtspunkten gilt es ausserdem die geplante Schwächung der Institution des Zwangsmassnahmengerichts auf das Schärfste zu kritisieren. Mit der Schaffung der zwei neuen Auskunftstypen, die mittels einfacher Auskunftsanfrage automatisch abgerufen werden können, werden rechtliche Kontrollmechanismen wie das Zwangsmassnahmengericht umgangen und der Einflussbereich der Staatsanwaltschaft noch weiter ausgebaut. Art. 42a und 43a sind daher vollumfänglich zu streichen.

Antrag: Streichung der Artikel

Art. 50a

Art. 50a sieht vor, dass Anbieter:innen verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Auch diese Pflicht soll eine Vielzahl neuer Unternehmen erfassen: Betroffen sind nicht mehr nur FDA (Art. 26 BÜPF) und ausnahmsweise AAKD (Art. 27 BÜPF), sondern sämtliche Anbieter:innen mit mehr als 5'000 Nutzer:innen. Im Ergebnis wäre fast die gesamte Schweizer AAKD-Branche betroffen (kaum ein Produkt ist lebensfähig mit weniger als 5'000 Teilnehmer:innen).

Die Ausdehnung dieser Pflicht auf AAKD stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar: Es findet keine Einzelfallprüfung statt und die AAKD werden dieser Pflicht unterworfen, auch wenn sie keineswegs «Dienstleistungen von grosser

wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten», was jedoch gesetzliche Vorgabe ist (Art. 27 Abs. 3 BÜPF).

Problematisch ist zudem, dass aufgrund dieser Vorgabe Anbieter:innen ihrer Verschlüsselungen so konfigurieren müssen, dass sie von ihnen aufgehoben werden können – eine durch Anbieter:innen aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung allerdings in jedem Fall. Dies führt zu schwächeren Verschlüsselungen und der Abnahme der Sicherheit von Kommunikationsdiensten.

Daraus ergibt sich eine Grundrechtsproblematik von erheblicher Tragweite: Das Verhältnismässigkeitsgebot aus Art. 36 BV kann nicht eingehalten werden, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Die Interessenabwägung darf hier nicht zuungunsten der Grundrechtsträger:innen erfolgen, da es sich bei deren Interessen um solche von fundamentalem Gewicht – dem Zugang zu sicherer Kommunikation und damit direkt verbunden dem Recht auf freie Meinungsäusserung – handelt.

Wichtig ist, dass Verschlüsselungen, die auf dem Endgerät der Nutzer:innen erfolgen – also End-zu-End-Verschlüsselungen – nicht unter die Pflicht zur Aufhebung gemäss Art. 50a VE-VÜPF fallen dürfen. Diese Form der Verschlüsselung liegt ausschliesslich in der Sphäre der Nutzer:innen und es wäre untragbar, die Pflicht zur Aufhebung von Verschlüsselungen in dieser Sphäre zu verlangen. Die Anbieter:innen dürfen daher nicht dazu verpflichtet werden, diese Inhalte zu entschlüsseln und zugänglich zu machen. Im Gegensatz dazu betrifft die Transportverschlüsselung «lediglich» die Verbindung zwischen Client und Server und kann von Anbieter:innen kontrolliert werden. Es ist wichtig, dass diese technischen Unterscheidungen und unterschiedlichen Schutzwirkungen und -richtungen bei rechtlichen Umsetzungen beachtet werden. Wir begrüssen die Klarstellung im erläuternden Bericht, dass die End-zu-End-Verschlüsselung vom Anwendungsbereich ausgenommen ist. Es muss jedoch ebenso klar sein, dass das ganze Endgerät von Nutzer:innen aus dem Anwendungsbereich von Art. 50a VE-VÜPF ausgenommen ist.

Es braucht im Übrigen auch eine Klarstellung darüber, dass eine rückwirkende Möglichkeit zur Aufhebung klar ausgeschlossen ist. Eine solche würde de facto eine Vorratsdatenspeicherung verschlüsselter Inhalte und Keys darstellen, die mit dem Prinzip der Datenminimierung (Art. 6 Abs. 3 DSG) und dem Schutz der Privatsphäre (Art. 13 BV) unvereinbar ist.

Antrag: Streichung der «Anbieterin mit reduzierten Pflichten» aus dem Anwendungsbereich sowie eine Klarstellung darüber, dass die Aufhebung von Verschlüsselungen auf dem Endgerät der Nutzer:innen sowie eine rückwirkende Verpflichtung zur Aufhebung ausgeschlossen sind.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Art. 14 Abs. 3 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und wirtschaftlich nicht tragbar, was das Einführen von Fristen obsolet werden lässt. Der Absatz ist daher ersatzlos zu streichen.

Antrag: Streichung

Art. 14 Abs. 4 VD-ÜPF

Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der Unterworfenen AAKD – da auch AAKD mit reduzierten Pflichten erfasst sind – massiv. Dies ist wie bereits ausgeführt weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.

Antrag: Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten»

Art. 20 Abs. 1 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen, ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.

Antrag: Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»

Schlussbemerkung

Trotz des Umfangs dieser Stellungnahme gilt: Das Ausbleiben einer expliziten Bemerkung zu einzelnen Bestimmungen bedeutet keine Zustimmung der Digitalen Gesellschaft. Die Ablehnung der Revision bleibt volumnäiglich bestehen.

Freundliche Grüsse

Erik Schönenberger
Geschäftsleiter

Bundesrat
Beat Jans
Vorsteher
Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundeshaus West
CH-3003 Bern

per E-Mail an ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 2. Mai 2025

Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat Jans

Sehr geehrte Mitarbeitende des Eidgenössischen Justiz- und Polizeidepartements

Am 29. Januar 2025 eröffnete der Bundesrat die Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) und hat die Stiftung für Konsumentenschutz zur Stellungnahme eingeladen.

Die Stiftung für Konsumentenschutz ist eine Nichtregierungs-Organisation, die sich seit 1964 für die Rechte und Interessen von Konsument:innen einsetzt.

Wir bedanken uns für die Einladung zur Vernehmlassung und nehmen wie folgt Stellung:

Vorbemerkungen

Die geplante Revision der VÜPF ist ein Frontalangriff auf unsere Grundrechte, die Rechtsstaatlichkeit sowie den IT- und Innovationsstandort Schweiz.

Mit ihrer Umsetzung würde geltendes Recht in einem Ausmass verletzt, das alarmieren muss: Die Revision ist in vielerlei Hinsicht unvereinbar mit dem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), verstösst gegen das Datenschutzgesetz (DSG), steht in klarem Widerspruch zu den verfassungsmässigen Grundrechten und verstösst gegen Völkerrecht.

Die vorgesehenen Änderungen führen zu einer flächendeckenden und massiv ausgeweiteten Überwachung. Dies ist mit der Ausrichtung des BÜPF, mit seiner austarierten Interessenabwägung zwischen Freiheit und Privatsphäre einerseits und Sicherheit durch Überwachungsmassnahmen andererseits, absolut nicht vereinbar.

Gemäss Statistik des Dienst Überwachung Post- und Fernmeldeverkehr ÜPF sind die Überwachungsmassnahmen 2024 um mehr als das Doppelte angestiegen. Gerade die beiden Kategorien der rückwirkenden Überwachungen sind im Vergleich zu 2023 deutlich gestiegen. Mit den in die Vernehmlassung gegebenen Vorlagen würden zukünftig noch mehr Daten bei mehr Dienstleister:innen gesammelt und aufbewahrt. Entsprechend würde die Anzahl

Überwachungsmassnahmen durch diese Vorlagen mit an Sicherheit grenzender Wahrscheinlichkeit weiter ansteigen – vermutlich deutlich. Und das, obwohl der behauptete Mehrwert durch solche Überwachungsmassnahmen bei der Strafverfolgung einer empirischen Grundlage entbehrte.

Auch die Auswirkungen auf den Wirtschafts- und Innovationsstandort Schweiz wären verheerend: Die Ausweitung der Überwachung und die damit verbundenen, übermässigen Mitwirkungspflichten machen die Schweiz für IT-Anbieter äusserst unattraktiv. Denn die prophylaktische Datenspeicherung auf Vorrat für ein halbes Jahr ist für die IT-Dienstleister:innen ein hoher Kostenfaktor. Renommierte Unternehmen wie Proton oder Threema, deren Geschäftsmodelle durch die Vorlage direkt ins Visier geraten, würden in ihrer Existenz bedroht. Proton hat bereits angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen (Tages-Anzeiger vom 1. April 2025). Ähnlich äusserte sich Threema-Chef Robin Simon (Tages-Anzeiger vom 8. April 2025).

Neben den verheerenden wirtschaftlichen Auswirkungen wird gleichzeitig der grundrechtlich garantierte Anspruch auf sichere und vertrauliche Kommunikation ausgehöhlt. Konsument:innen, die bisher auf Schweizer Dienstleister:innen wie Threema, Proton oder Infomaniak vertrauen, können sich zukünftig möglicherweise gar nicht mehr für Schweizer Dienstleister:innen entscheiden, weil es keine mehr gibt. Falls kein Wegzug stattfindet, werden die verpflichteten Schweizer Dienstleister:innen die Kosten für die Vorratsdatenspeicherung auf die Konsument:innen abwälzen (müssen). Letzten Endes zahlen also die Schweizer Kund:innen erhöhte Preise, damit sie besser rückwirkend überwacht werden können.

Wenn Anbieterinnen abwandern, bleibt jedoch – als wäre dies nicht genug – nicht nur den privaten Nutzer:innen der Zugang zu geschützten Kommunikationsmitteln verwehrt. Ebenso betroffen sind Personen, die einem Berufsgeheimnis unterstehen und schutzbedürftige Personengruppen wie Whistleblower:innen, Menschen ohne geklärten Aufenthaltsstatus oder ohne Papiere, sowie Aktivist:innen.

Hinzu kommt: Die geplanten Regelungen sind technisch unausgereift, unnötig komplex und in Teilen schlicht nicht umsetzbar. Vielmehr wird ein kaum noch durchschaubares Normengeflecht geschaffen, das weder den Mitwirkungspflichtigen noch den Betroffenen ein Mindestmass an Rechtsklarheit bietet. Von Transparenz kann nicht die Rede sein.

Es ist im Übrigen unhaltbar, dass eine dermassen breit angelegte Ausweitung von Pflichten für Anbieter:innen auf Verordnungsstufe angelegt wird. Solch einschneidende Veränderungen in Grundrechte sind in Gesetzesform zu erlassen. Der Bundesrat überschreitet mit dieser Vorlage seine Kompetenzen.

Diese Vorlage schadet nicht nur den Konsument:innen und Bürger:innen sondern schwächt auch noch den Innovations- und Wirtschaftsstandort Schweiz. Aus grundrechtlicher, datenschutzrechtlicher und gesellschaftspolitischer Sicht ist sie schlicht inakzeptabel. Die geplanten Änderungen stehen dem erklärten Ziel von mehr KMU-Freundlichkeit, allgemeinen rechtsstaatlichen Grundsätzen sowie Schutzbedürfnissen Einzelner diametral entgegen.

Deshalb lehnt der Konsumentenschutz die Revision volumnfänglich und in aller Deutlichkeit ab.

Bemerkungen zu einzelnen Artikeln der VÜPF

Alle Artikel

Um den im Datenschutzgesetz verankerten Grundsatz der Zweckmässigkeit (Art. 6 Abs. 3 DSG) gerecht zu werden, dürfen Unternehmen nicht gezwungen werden, mehr Daten über ihre Kund:innen auf Vorrat zu sammeln, als für ihre Geschäftstätigkeit notwendig ist. Selbstverständlich soll dennoch bei allen Auskunftstypen die Datenherausgabe im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können.

Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar», «sofern vorhanden» o.ä. hinzugefügt werden, damit mit der Vorlage keine unangemessenen und teuren Aufbewahrungspflichten geschaffen werden.

Antrag: Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.

Art. 16b Abs. 1

Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Das Abstellen auf das Kriterium des Gesamtumsatzes des Unternehmens statt der relevanten Teile (Art. 16b Abs. 1 lit. b Ziff. 2 VE-VÜPF) führt dazu, dass bestehende Unternehmen mit entsprechendem Umsatz Dienstleistungen und Features die zur Klassierung als FDA führen gar nicht erst auf den Markt bringen. Bestehende Unternehmen können entweder komplett auf solche Neuerungen verzichten oder direkt die unverhältnismässigen Mitwirkungspflichten erfüllen.

Dazu kommt, dass das Kriterium bezüglich der Überwachungsaufträge nicht vom BÜPF gestützt wird, denn: Die Anzahl von Überwachungsaufträgen ist von der wirtschaftlichen Bedeutung einer FDA völlig losgelöst. Die wirtschaftliche Bedeutung ist aber gemäss Art. 26 Abs. 6 BÜPF ausschlaggebend dafür, ob eine FDA von den vollen Pflichten (teilweise) befreit werden kann. E contrario ist die wirtschaftliche Bedeutsamkeit somit Erfordernis für die Auferlegung von vollen Pflichten. Wenn FDA nun aber rein aufgrund der Anzahl von Überwachungsaufträgen nach Art. 16b Abs. 1 lit. b Ziff. 1 VE-VÜPF als vollpflichtige FDA qualifiziert werden, steht dies im Widerspruch zum BÜPF und entbehrt damit einer Rechtsgrundlage.

Dieses bereits in der aktuellen Version der VÜPF vorhandene Problem sollte im Zuge einer Revision nicht bestehen bleiben, sondern muss behoben werden.

Antrag: Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren». Es ist auf die Regelung in Art. 26 Abs. 6 BÜPF abzustellen und eine Einzelfallbetrachtung zur Einstufung vorzunehmen.

Art. 16c Abs. 3

Die durch die neue Verordnung einmal mehr – deutlich – ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als «natürliche» Schutzmechanismen gegen eine übermässige oder missbräuchliche Nutzung

solcher Massnahmen durch die Untersuchungsbehörden. Die automatisierte Erteilung von Auskünften ist unverhältnismässig und widerspricht dem Grundsatz der Zweckmässigkeit. Die pauschale und undifferenzierte Regel beeinträchtigt zwangsläufig den Grundrechtsschutz. Der vorgesehene Umsetzungszeitraum von 12 Monaten zur Umsetzung ausserdem aufgrund der Komplexität unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.

Antrag: Streichung von lit. a «automatisierte Erteilung der Auskünfte» (ebenso in Art. 18 Abs. 2).

Art. 16d

Gemäss erläuterndem Bericht stellen Kommunikationsdienste, die nicht zu den in Art. 16a Abs. 1 aufgezählten Fernmeldediensten gehören und auf welche die Ausnahmen nach Art. 16a Abs. 2 nicht zutreffen, abgeleitete Kommunikationsdienste dar. Diese klarere Definition der Bezeichnung «Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD)» ist begrüssenswert, doch ist die Konkretisierung im erläuternden Bericht einerseits rechtsstaatlich problematisch und andererseits geht die neue Auslegung nach den Ausführungen im erläuterndem Bericht weit über den gesetzlichen Zweck hinaus.

Besonders problematisch ist die generelle Nennung von Onlinespeicherdiensten wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter etc.) genutzt werden. Konsument:innen nutzen diese regelmässig, um auf einfache und sichere Weise Datenbackups zu erstellen. So stellen sie sicher, dass ein Geräteverlust nicht mit einem vollständigen Datenverlust einhergeht.

Art. 2 lit. c BÜPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft jedoch auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug in die Auslegung unrechtmässig ist – auch hier setzt sich die Revision über die gesetzlichen Vorgaben des BÜPF hinweg, was inakzeptabel ist.

Onlinespeicherdienste sind deshalb aus Art. 16d zu streichen.

Zudem anerkennt der erläuternde Bericht zwar, dass VPNs zur Anonymisierung der Nutzer:innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil angebrachte Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internets, verunmöglichen. Der Konsumentenschutz weist darauf hin, dass der EGMR in seinem Urteil vom 13. Mai 2024 (Podchasov v. Russia) zum Schluss kam, dass die Verpflichtung zur Entfernung von Verschlüsselung bei Kommunikationsdienstleister:innen gegen Art. 8 EMRK verstösst. Das Bedürfnis, auch künftig VPN-Dienste in Anspruch nehmen zu können, ist zu schützen und darf nicht vereitelt werden. Anbieter:innen von VPNs sind daher ebenfalls aus Art. 16d auszunehmen.

Es ist irritierend, dass die bewusst separat ausgestalteten Kategorien AAKD und FDA einander zunehmend angeglichen werden, und zwar zuungunsten der AAKD, die als Kategorie mit grundsätzlich weniger weitreichenden Pflichten als die FDA konzipiert wurde. Dies missachtet den Willen der Gesetzgeber:innen, den es zu wahren gilt.

Antrag: Streichung von Onlinespeicherdiensten und VPN-Anbieter:innen aus der Aufzählung der möglichen abgeleiteten Kommunikationsdienste in den Ausführungen zu Art. 16d im erläuternden Bericht und in der Auslegung.

Art. 16e, Art. 16f und Art. 16g

Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich wirkt der

vorgelegte Entwurf diesem erklärten Ziel jedoch komplett entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung mit deutlich erweiterten Pflichten. Entscheidend ist, dass neuerdings das Kriterium von 5'000 Nutzer:innen allein zum Auferlegen massiver Überwachungspflichten ausreicht: Erreicht eine AAKD diese Grösse, fällt sie neu in die Kategorie der AAKD mit reduzierten Pflichten und untersteht somit bereits sehr weitgehenden Mitwirkungspflichten, insbesondere der Identifikationspflicht.

Die Einführung von 5'000 Nutzer:innen als gesondert zu beurteilende Untergrenze verletzt Art. 27 Abs. 3 BÜPF. Max. 5'000 Personen (1 Person kann mehrere Nutzer:innen darstellen) sind keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strengeren Überwachungsmassnahmen, gerechtfertigt wären. 5'000 Nutzer:innen werden in der digitalen Welt vielmehr sehr rasch erreicht – die Revision verkennt technische Realitäten.

Zusätzlich führt das Einführen eines Konzernatbestandes in Art. 16f Abs. 3 zu massiven Problemen: Produkte und Dienste müssen nicht mehr für sich allein bestimmte Schwellenwerte erreichen – es genügt, wenn das Mutterunternehmen oder verbundene Gesellschaften diese überschreiten. Insbesondere bei Unternehmen mit Beteiligungsstrukturen führt dies dazu, dass sämtliche Angebote pauschal der höchsten Überwachungsstufe unterstellt werden – unabhängig davon, ob sich einzelne Dienste noch im frühen Entwicklungsstadium befinden oder faktisch kaum genutzt werden. Somit müsste jedes neue Projekt von Beginn an mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden, was Innovation behindert. Zudem missachtet der Konzernatbestand das Verhältnismässigkeitsgebot: Unterschiedliche organisatorische Einheiten mit eigenständigen Angeboten werden unrechtmässig zusammengefasst, obwohl sie individuell zu prüfen wären. Die Anwendung starrer Schwellen auf ganze Konzerne statt auf einzelne Dienste umgeht eine notwendige Einzelfallprüfung.

Eine solche Regelung stünde sodann im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali, das die zu seltene Anwendung von Downgrades kritisierte: «Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»

Statt KMU zu entlasten, führt die Revision neu zu einem «automatischen» *Upgrade per Verordnung ohne Verfügung* (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.

Eine Analyse der offiziellen VÜPF-Statistik unterstreicht diese offensichtliche Unverhältnismässigkeit. Im Jahr 2023 betrafen 98,97% der total 9'430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter:innen – übrig bleiben nur 1,03% für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,74% wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100% des Marktes inklusive der KMU und Wiederverkäufer:innen unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.

Die neue Vorlage schliesst nun ebenfalls sowohl die Registrierung via normaler E-Mail als auch die komplett anonyme Registrierung (z. B. Signal oder Telegram) aus, da AAKD bereits mit reduzierten Pflichten neu automatisch zwingend die Endnutzer:innen identifizieren müssen. Hiervon betroffen sind nicht nur alle AAKD mit reduzierten Pflichten, sondern auch all deren Wiederverkäufer:innen. Faktisch resultiert das Gesetz somit darin, dass Konsument:innen sich bei keinem Dienst mehr anmelden können sollen, ohne den Pass,

Führerschein oder die ID entweder direkt oder indirekt zu hinterlegen. Dass Nutzer:innen künftig hierzu gezwungen wären, stellt einen massiven Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 BV) dar und ist unzumutbar.

Ein weiteres Kernproblem, das die automatische Hochstufung mit sich bringt, ist die Rechtsunsicherheit. Die Vorlage will mit klarer definierten Kategorien und Pflichten eine übersichtlichere Situation schaffen, verfehlt dieses Ziel jedoch gänzlich. Bislang fand die Hochstufung per Verfügung statt, wodurch es für die Mitwirkungspflichtigen klar erkennbar war, wann sie unter welche Pflichten fallen. Außerdem bewirkt diese Praxis eine sinnvolle Einzelfallbetrachtung anstelle pauschaler und unzweckmässiger automatischer Hochstufungen. Unter dem revidierten System entfällt dieser Schritt, und ein:e AAKD wird automatisch hochgestuft, sobald sie den massgebenden Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes kann aber im Zweifelsfall nur schwer zu beantworten sein. Gerade deshalb besteht ein schutzwürdiges Interesse der Anbieter:innen an Klarheit über ihre Pflichten, da sie fortan eventuell die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Diese Umstrukturierung lässt ich nicht mit der Funktionsweise von Verwaltungsverfahren vereinbaren. Die Pflicht zur Abklärung, wann eine Hochstufung vorliegt und was diese für das Unternehmen bedeutet, darf nicht in die Verantwortung der Unternehmen fallen. Der Staat zieht sich hier aus der Verantwortung und schiebt diese den Unternehmen zu, wodurch diesen zwangsläufig zeitlicher und finanzieller Mehraufwand entsteht. Von einer automatischen Hochstufung von AAKD ist daher abzusehen. Verschärfend wirkt sich hier die kaum verständliche Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMU (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.

Gegenüber der geltenden VÜPF erweitert die Revision die Pflichten zur Automatisierung noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragetypen wie z. B. "IR_59" und "IR_60", welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.

Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 lit. b der geltenden VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grosse[n] Teil ihrer Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. Damit fallen auch Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz. Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Auch hiermit werden neue Hürden für Innovation geschaffen. Die Regelung ist unverhältnismässig und nicht sachdienlich.

Auch Non-Profit-Organisationen geraten unter die verschärften Vorgaben. Unter den neuen Kriterien wird allein auf die Anzahl der Nutzer:innen abgestellt für die Einstufung als AAKD. Dieses Kriterium greift jedoch zu kurz: Es berücksichtigt insbesondere nicht die wirtschaftliche Tragfähigkeit der Anbieter:innen. Gerade bei Open-Source- und Non-Profit-Lösungen mit grosser Reichweite, aber geringem Budget, führt dies zu einer verheerenden finanziellen Belastung: Anbieter:innen mit solchen Projekten würden gezwungen, umfangreiche Überwachungsmassnahmen einzuführen. Solche Anbieter:innen würden gezielt aus dem Schweizer Markt gedrängt, während gleichzeitig bestehende Monopole wie WhatsApp (96% Marktanteil in der Schweiz) gestärkt würden.

Es muss ausserdem klar festgehalten werden, dass sich das BÜPF und die VÜPF nur auf Anbieter:innen beziehen können, die in der Schweiz tatsächlich tätig sind. Die Erlasse dürfen nicht so ausgelegt werden, dass sie eine extraterritoriale Wirkung entfalten und internationale Dienste wie Signal, WhatsApp oder Microsoft Teams miterfasst sind.

Das alleinige Kriterium der Nutzer:innenzahl ist ungeeignet und muss gestrichen werden.

Die Regelung schwächt auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade US-amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Schweizer Konsument:innen den Zugang zu bewährten und sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, Ende-zu-Ende-verschlüsselter Kommunikation ist heute wichtiger denn je und fällt in den Bereich grundrechtlich geschützter Ansprüche, die es zu wahren gilt. Diese Ansprüche dürfen nicht aufs Spiel gesetzt werden, um ein knallhartes Überwachungsregime der Kommunikation in der Schweiz durchzusetzen – die Prioritäten werden höchst fragwürdig gesetzt.

Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade illegal ist (EuGH Urteil vom 21.12.2016, Az. C-203/15 und C-698/15) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer:innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, diese sind zudem von enormem Ausmass und bergen folglich massive Risiken für Hackerangriffe.

Des Weiteren ist nicht belegt, dass die Speicherung der betreffenden Daten zu spürbar mehr erfolgreichen Ermittlungen führt. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisshandlung via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfüge, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden. Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren. Diese Handhabe bedeutet einen Verstoss gegen das Legalitätsprinzip und untergräbt legislative Kompetenzen. Außerdem verfügt die Schweiz bereits über reichlich Mittel zur Aufklärung und Verfolgung von Straftaten, die Behörden können bereits heute auf sicherheitsrelevante Daten zurückgreifen. Unternehmen wie Proton (s. «Positionspapier zur Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)» von Proton) kooperieren seit Jahren mit den Schweizer Strafverfolgungsbehörden und dem Nachrichtendienst des Bundes (NDB). Wenn nun solche Unternehmen aus bereits genannten Gründen zur Abwanderung gezwungen werden, bewirkt die Revision auch hier das genaue Gegenteil ihrer erklärten Ziele: Anstatt der Schaffung besserer Möglichkeiten zur Strafverfolgung würden die Schweizer Behörden wie etwa Fedpol den Zugriff auf wichtige Partner bei der Beschaffung sicherheitsrelevanter Daten verlieren.

Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Integrität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.

Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das DSG. Der Entwurf bringt nicht, wie im Begleitbericht behauptet, eine Entlastung der KMU (geschweige denn eine Entspannung der Hochstufungsproblematik) sondern verengt den Markt, fördert bereits bestehende Monopole von US-Tech-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit, steht in direktem Gegensatz zum besagten Postulat 19.4031 und bedeutet massive Eingriffe in grundrechtlich geschützte Sphären, sowohl von Unternehmen als auch von Nutzer:innen.

Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen und das bestehende System muss beibehalten werden.

Antrag: Streichung der Artikel und Beibehaltung der bestehenden Kriterien und der zwei Kategorien von AAKD und Ausnahmen für Pilotprojekte (auch von grossen Firmen) und Non-Profits per se. Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).

Art. 16h

Art. 16h konkretisiert die Kategorie der «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» aus Art. 2 lit. e BÜPF. Die Vorschrift verfehlt ihr Ziel – anstatt Unsicherheiten darüber zu beheben, wer unter diese Kategorie fällt, schafft sie weitere Unklarheiten. Der schwammig formulierte Verordnungstext könnte dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist:innen, Whistleblower:innen und unterdrückten Personen zum Schutz ihrer Privatsphäre genutzt. Betreiber:innen solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer:innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen. Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt. Die Unklarheit bezüglich der Einordnung von TOR-Servern wirft weitere Fragen auf, denn wenn TOR nicht als PZD zu qualifizieren ist, müsste TOR – gleich wie die VPNs – der Kategorie der AAKD zugeordnet werden. Somit stünden Betreiber:innen von TOR-Servern – wie etwa die Digitale Gesellschaft – unter der Identifikationspflicht. Diese ist jedoch, wie dargelegt, nicht umsetzbar.

Es braucht somit entweder die Zusicherung, dass Betreiberinnen von TOR-Nodes nicht dem BÜPF und der VÜPF unterstellt sind oder aber Kategorien von Mitwirkungspflichten, die so gestaltet sind, dass ein:e Betreiber:in eines TOR-Nodes nicht einer Identifikationspflicht unterstellt wird – z. B. indem die Schwelle für das Auferlegen der Identifikationspflicht auf 1 Mio. Nutzer:innen angehoben wird.

Wären Betreiber:innen von TOR-Nodes von der Identifikationspflicht erfasst, würde dies fundamentale Grundrechte wie das Recht auf Privatsphäre und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK), die Meinungs- und Informationsfreiheit (Art. 16 BV, Art. 10 EMRK) gefährden. Ebenso würde das datenschutzrechtliche Prinzip der Datensicherheit (Art. 8 DSG) komplett unterlaufen. Diese Eingriffe in national und international geschützte Rechtsansprüche sind nicht hinzunehmen.

Dieser potenzielle Angriff auf die genannten Grundrechte ist hochproblematisch und setzt ein politisches Statement: Die Schweiz bewegt sich weg von Grundrechtsschutz hin zum hochgerüsteten Überwachungsstaat.

Antrag: Es muss sichergestellt werden, dass Technologien wie TOR oder I2P nicht vom Anwendungsbereich der VÜPF erfasst sind.

Art. 16h Abs. 2

Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Endbenutzer:innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 VE-VÜPF: Gemäss diesem Artikel trägt die das WLAN erschliessenden FDA die Verantwortung zur Identifikation der Nutzer:innen. Die Regelung führt also dazu, dass FDA, die einen Vertrag haben mit «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» (PZD), sehr schnell für die Identifikation der Endnutzer:innen ihrer Vertragspartner:in zuständig sind. Diese Regelung ist unsinnig und schlicht nicht umsetzbar.

Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer:innen zulassen kann. Bereits mit handelsüblichen Routern für den Privatkund:innenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDA unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden.

Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten.

FDA resp. Anbieter:innen von öffentlichen WLAN-Zugängen dürfen nur unter einer Identifikationspflicht stehen, wenn die PZD, die den Zugang der FDA nutzt, «professionell betrieben» ist – und zwar nach der aktuellen Auslegungsform (s. Erläuternder Bericht zur (letzten) Totalrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs):

«Mit "professionell betrieben" ist gemeint, dass eine FDA oder eine auf öffentliche WLAN-Zugangspunkte spezialisierte IT-Dienstleisterin den technischen Betrieb des öffentlichen WLAN-Zugangspunktes durchführt, die dies auch noch für andere öffentliche WLAN-Zugangspunkte an anderen Standorten macht. Wenn eine natürliche oder juristische Person an ihrem Internetzugang selbst einen öffentlichen WLAN-Zugangspunkt technisch betreibt und diesen Zugang Dritten zur Verfügung stellt, muss die FDA, die den Internetzugang anbietet, keine Identifikation der Endbenutzenden sicherstellen.»

So wird sichergestellt, dass FDA nicht unmöglich umzusetzenden Pflichten unterstellt werden.

Antrag: Streichung der Ausführung im erläuternden Bericht. Das Kriterium «professionell betrieben» ist nach der bislang geltenden Regelung zu verstehen. Art. 16h Abs. 2 ist ersatzlos zu streichen und im Zusammenhang mit Art. 19 Abs. 2 ist auf die aktuelle Definition von «professionell betrieben» abzustellen.

Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2

Bei Konzernen knüpft die VE-VÜPF nicht mehr an die Umsatz- und Nutzer:innenzahlen des betroffenen Unternehmens an, neu sind die Zahlen des Konzerns ausschlaggebend für eine Hoch- oder Herunterstufung. Die Begründung, dies diene der Vereinfachung, ist unlogisch und irreführend: Unternehmen müssen ihre Zahlen ohnehin produktbezogen ausweisen, die nötigen Daten liegen also längst vor. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.

Antrag: Streichung des «Konzerntatbestand» und Beibehaltung der bestehenden Regelung.

Art. 19 Abs. 1

Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD – erfasst sind die AAKD mit reduzierten und vollen Pflichten – widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht. Durch die neuen Schwellenwerte zur Einstufung findet eine beachtliche Ausweitung der Identifikationspflicht statt.

Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des DSG, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch insbesondere der Grundrechtsschutz von Konsument:innen in der Schweiz massiv beeinträchtigt wird. Die Identifikationspflicht greift immens in das Recht auf informationelle Selbstbestimmung ein und hält einer Grundrechtsprüfung nach Art. 36 BV schon allein aufgrund ihrer Unverhältnismässigkeit nicht stand.

Bezüglich einschneidender Pflichten, die potentiell schwere Grundrechtseingriffe bedeuten – wie es bei Identifikationspflichten zweifellos der Fall ist – muss Rechtsetzung in jedem Fall mit äusserster Sorgfalt und unter strenger Beachtung des Verhältnismässigkeitsgebots erfolgen. Ausserdem darf sich eine solche Pflicht nicht über gesetzliche Vorgaben, wie in diesem Fall vom BÜPF vorgegeben, hinwegsetzen.

Durch die breite Auferlegung einer solchen Pflicht werden datenschutzfreundliche Unternehmen bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.

Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Nur so können datenschutzrechtliche Vorgaben und die Rechte Betroffener gewahrt werden.

Antrag: Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen ohne Einführung einer Pflicht zur Identifikation von Teilnehmenden.

Art. 18

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 19 Abs. 2

Das Kriterium «professionell betrieben» ist nach der bestehenden Regelung auszulegen (s. Ausführungen zu Art. 16h Abs. 2). Es sei ausserdem darauf hingewiesen, dass sich aus dieser Regelung eine vertragsrechtliche Problematik zwischen den FDA und den PZD ergeben würde, die nicht tragbar ist.

Antrag: Auslegung des Kriteriums «professionell betrieben» nach der bestehenden Regelung und nicht i. S. v. Art. 16h Abs. 2.

Art. 21 Abs. 1 lit. a

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.

KONSUMENTEN SCHUTZ

engagiert. unabhängig.

Antrag: Streichung

Art. 22

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.

Antrag: beibehalten

Art. 11 Abs. 4

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.

Antrag: Streichung

Art. 16b

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.

Antrag: Streichung

Art. 31 Abs. 1

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 51 und 52

Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.

Antrag: beibehalten

Art. 60a

Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde laut den Erläuterungen bewusst auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten. Art. 60a ist zu streichen.

Antrag: Streichung

Art. 42a und 43a

Die Art. 42a und 43a führen neu die Abfragetypen «IR_59» und «IR_60» ein, über die sensible Daten automatisiert abgefragt werden können. Sie verlangen von Anbieter:innen, dass sie jederzeit Auskunft geben können bezüglich des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Auch für das Auferlegen dieser Pflicht gilt die fragliche Schwelle von 5'000 Nutzer:innen. Erfasst ist somit nahezu die gesamte AAKD-Landschaft der Schweiz.

Das Problem liegt darin, dass die «IR_»-Abfragen zu Informationen nach Art. 42a und 43a neu automatisiert abgerufen werden können – im Gegensatz zu den «HD_»- (historische Daten) und «RT_» (Echtzeitüberwachung) Abfragen, die strengeren Regeln und einer juristischen Kontrolle unterliegen. Bei den «IR_59»- und «IR_60»-Abfragen handelt es sich allerdings um

sensible Informationen wie etwa das Abrufen einer IP-Adresse. Solche Informationen mussten bislang zurecht über strengere Abfragetypen eingeholt werden. Es ist nicht nachvollziehbar, warum Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen.

Hinzu kommt, dass sich aus dem Verordnungstext keine Limiten für die Frequenz der Stellung dieser automatisierten Auskünfte ergeben. Unternehmen sind daher nur unzulänglich geschützt vor missbräuchlichen Anfragen und vor Kosten, die ihnen durch die Pflicht, diese Auskünfte automatisch weiterzugeben, entstehen wird.

Künftig könnten so umfangreiche Informationen über die neuen Abfragetypen beschafft werden, die bislang zurecht den strenger Regeln der rechtlich sichereren Informations-/Überwachungstypen «HD_» und «RT_» unterworfen waren. «IR_59» und «IR_60» ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne den erforderlichen Kontrollen dieser invasiven Überwachungstypen unterworfen zu sein.

Die Entwicklung, dass mittels «IR_»-Abfragen neu auch personenbezogene sensible Nutzungsdaten eingeholt werden können, widerspricht der Logik der unterschiedlichen Abfragetypen und öffnet Tür und Tor für missbräuchliche Abfragen und eine Echtzeitüberwachung von Millionen von Nutzer:innen. Auch hier stehen grundrechtlich geschützte Ansprüche auf dem Spiel, die mit einer solchen Regelung auf nicht nachvollziehbare Weise untergraben und missachtet werden.

Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind. Die AAKD müssten künftig gewisse Datenkategorien systematisch erheben, um dieser Pflicht nachzukommen. Art. 27 Abs. 2 BÜPF erklärt allerdings, dass AAKD «auf Verlangen die *ihnen zur Verfügung stehenden* Randdaten des Fernmeldeverkehrs der überwachten Person liefern» müssen. Bei einer dahingehenden Auslegung des Bestimmungen bedeutete dies einen weiteren Verstoß gegen das BÜPF.

Unter rechtsstaatlichen Gesichtspunkten gilt es außerdem die geplante Schwächung der Institution des Zwangsmassnahmengerichts auf das Schärfste zu kritisieren. Mit der Schaffung der zwei neuen Auskunftstypen, die mittels einfacher Auskunftsanfrage automatisch abgerufen werden können, werden rechtliche Kontrollmechanismen wie das Zwangsmassnahmengericht umgangen und der Einflussbereich der Staatsanwaltschaft noch weiter ausgebaut. Art. 42a und 43a sind daher vollumfänglich zu streichen.

Antrag: Streichung

Art. 50a

Art. 50a sieht vor, dass Anbieter:innen verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Auch diese Pflicht soll eine Vielzahl neuer Unternehmen erfassen: Betroffen sind nicht mehr nur FDA (Art. 26 BÜPF) und ausnahmsweise AAKD (Art. 27 BÜPF), sondern sämtliche Anbieter:innen mit mehr als 5'000 Nutzer:innen. Im Ergebnis wäre fast die gesamte Schweizer AAKD-Branche betroffen (kaum ein Produkt ist lebensfähig mit weniger als 5'000 Teilnehmer:innen).

Die Ausdehnung dieser Pflicht auf AAKD stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar: Es findet keine Einzelfallprüfung statt und die AAKD werden dieser Pflicht unterworfen, auch wenn sie keineswegs «Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten», was jedoch gesetzliche Vorgabe ist (Art. 27 Abs. 3 BÜPF).

Problematisch ist zudem, dass aufgrund dieser Vorgabe Anbieter:innen ihre Verschlüsselungen so konfigurieren müssen, dass sie von ihnen aufgehoben werden können

– eine durch Anbieter:innen aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung allerdings in jedem Fall. Dies führt zu schwächeren Verschlüsselungen und der Abnahme der Sicherheit von Kommunikationsdiensten.

Daraus ergibt sich eine Grundrechtsproblematik von erheblicher Tragweite: Das Verhältnismässigkeitsgebot aus Art. 36 BV kann nicht eingehalten werden, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Die Interessenabwägung darf hier nicht zu Ungunsten der Grundrechtsträger:innen erfolgen, da es sich bei deren Interessen um solche von fundamentalem Gewicht – dem Zugang zu sicherer Kommunikation und damit direkt verbunden dem Recht auf freie Meinungsäußerung – handelt.

Wichtig ist, dass Verschlüsselungen, die auf dem Endgerät der Nutzer:innen erfolgen – also Ende-zu-Ende-Verschlüsselungen – nicht unter die Pflicht zur Aufhebung gemäss Art. 50a VE-VÜPF fallen dürfen. Diese Form der Verschlüsselung liegt ausschliesslich in der Sphäre der Nutzer:innen und es wäre untragbar, die Pflicht zur Aufhebung von Verschlüsselungen in dieser Sphäre zu verlangen. Die Anbieter:innen dürfen daher nicht dazu verpflichtet werden, diese Inhalte zu entschlüsseln und zugänglich zu machen. Im Gegensatz dazu betrifft die Transportverschlüsselung «lediglich» die Verbindung zwischen Client und Server und kann von Anbieter:innen kontrolliert werden. Es ist wichtig, dass diese technischen Unterscheidungen und unterschiedlichen Schutzwirkungen und -richtungen bei rechtlichen Umsetzungen beachtet werden. Wir begrüssen die Klarstellung im erläuternden Bericht, dass die Ende-zu-Ende-Verschlüsselung vom Anwendungsbereich ausgenommen ist. Es muss jedoch ebenso klar sein, dass das ganze Endgerät von Nutzer:innen aus dem Anwendungsbereich von Art. 50a VE-VÜPF ausgenommen ist.

Es braucht im Übrigen auch eine Klarstellung darüber, dass eine rückwirkende Möglichkeit zur Aufhebung klar ausgeschlossen ist. Eine solche würde de facto eine Vorratsdatenspeicherung verschlüsselter Inhalte und Keys darstellen, die mit dem Prinzip der Datenminimierung (Art. 6 Abs. 3 DSG) und dem Schutz der Privatsphäre (Art. 13 BV) unvereinbar ist.

Antrag: Streichung der «Anbieterin mit reduzierten Pflichten» aus dem Anwendungsbereich sowie eine Klarstellung darüber, dass die Aufhebung von Verschlüsselungen auf dem Endgerät der Nutzer:innen sowie eine rückwirkende Verpflichtung zur Aufhebung ausgeschlossen sind.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Art. 14 Abs. 3 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und wirtschaftlich nicht tragbar, was das Einführen von Fristen obsolet werden lässt. Der Absatz ist daher ersatzlos zu streichen.

Antrag: Streichung

Art. 14 Abs. 4 VD-ÜPF

Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der unterworfenen AAKD – da auch AAKD mit reduzierten Pflichten erfasst sind – massiv. Dies ist wie bereits ausgeführt weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.

Antrag: Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten»

Art. 20 Abs. 1 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen, ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.

Antrag: Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»

Schlussbemerkung

Trotz des Umfangs dieser Stellungnahme gilt: Das Ausbleiben einer expliziten Bemerkung zu einzelnen Bestimmungen bedeutet keine Zustimmung der Stiftung für Konsumentenschutz. Die vollumfängliche Ablehnung der Revision bleibt davon unangetastet.

Freundliche Grüsse



Sara Stalder
Geschäftsleiterin



Lucien Jucker
Leiter Datenschutz

Eidgenössisches Justiz-und Polizeidepartement EJPD

Per Mail:

ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 2. Mai 2025

Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF). Teilrevisionen: Vernehmlassungsverfahren

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zur erwähnten Vorlage Stellung nehmen zu können. Aus datenschutzrechtlicher Sicht ergeben sich die nachfolgenden Anträge und Hinweise.

Verfassungsmässigkeit der Regelungen zu den AAKD

Zur Wahrung der Privatsphäre sind abgeleitete Kommunikationsdienste (wie beispielsweise Threema), die eine möglichst anonyme Nutzung ermöglichen, zentral. Der Anbieter (AAKD) kann seinen Dienst datensparsam gestalten, was das Risiko eines Missbrauchs von Personendaten massiv reduziert. Nach Art. 22 Abs. 3 BÜPF müssen die AAKD den Behörden grundsätzlich nur die ihnen vorliegenden Angaben liefern, und in begründeten Fällen kann der Bundesrat die Pflichten AAKD erhöhen (Abs. 4). Dabei darf die Erhöhung der Pflichten nur dann erfolgen, wenn die Ziele der Behörden nicht anders erreicht werden können (Notwendigkeit als Teilgehalt der Verhältnismässigkeit, Art. 5 Abs. 2 und Art. 36 Abs. 3 BV). Aus den vorliegenden Informationen ist jedoch weder ersichtlich noch nachvollziehbar, warum mit einer Kombination der Überwachung durch Fernmeldedienstanbieter (FDA) und AAKD das Ziel der Behörden nicht mit einem geringeren Eingriff in die Grundrechte der Betroffenen erreicht werden könnte. Dass der Aufwand für die Behörde etwas höher wäre, liegt in der Natur der Rechtsstaatlichkeit. Deshalb empfiehlt privatim, die Regelungen betreffend die AAKD insgesamt (Schwellenwerte und mit deren Erreichen verbundene Pflichten zur

Aufbewahrung und Bekanntgabe von Personendaten) auf ihre Verfassungsmässigkeit hin zu prüfen und so weit als erforderlich anzupassen.

Entfernung von Verschlüsselungen (Art. 50a E-VÜPF)

Da die Verschlüsselung eine zentrale Sicherheitsmassnahme darstellt, erachten wir eine pauschale Pflicht zur Entschlüsselung als kritisch. Einerseits nimmt Art. 50a die Ende-zu-Ende-Verschlüsselung zwischen Endkunden von der Pflicht aus. Bei der im erläuternden Bericht genannten Beispiel einer Transportverschlüsselung muss diese sowohl beim FDA als auch beim AAKD technologiebedingt terminiert werden, die Bearbeitung erfolgt danach unverschlüsselt. Es ist nicht ersichtlich, weshalb zusätzlich geeignete Punkte zur Entschlüsselung festgelegt werden müssen; diese ergeben sich bei der Anbieterin ohne weiteres. Wir beantragen deshalb, Art. 50a E-VÜPF zu streichen.

Risikobeurteilung / DSFA

Dem erläuternden Bericht zur Eröffnung des Vernehmlassungsverfahrens (EB) ist zu entnehmen, dass eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt wurde und «für diese Vorlage kein hohes Risiko vorliegt» (Kapitel 5.7).

Nach Kapitel 7.8 des Botschaftsleitfadens (Leitfaden zum Verfassen von Botschaften des Bundesrates, Stand April 2024) müsste somit eine Risikovorprüfung durchgeführt worden sein, die zum Schluss kam, dass ein hohes Risiko für die Grundrechte der betroffenen Personen besteht (andernfalls hätte es keine DSFA gebraucht). Dann wäre es aber erforderlich, dass in der Botschaft und somit auch bereits im EB dargelegt wird, aus welchen Gründen ein hohes Risiko vorliegt, worin dieses besteht, mit welchen Massnahmen ihm begegnet wird und welche Restrisiken verbleiben. Ebenso müsste die Stellungnahme des EDÖB (soweit eine solche vorliegt) im EB abgebildet sein.

Die Vorgabe im Botschaftsleitfaden, dass das Risiko für die Grundrechte der betroffenen Personen, die ergriffenen Massnahmen und die verbleibenden Restrisiken ausgewiesen werden müssen, begrüßt privatim ausdrücklich. Diese Informationen sind für die Beurteilung einer Vorlage wesentlich. Ungeachtet der methodischen Frage, ob die DSFA das geeignete Instrument für eine «Regulierungsfolgenabschätzung Persönlichkeitsrechte» darstellt, fehlen diese Informationen im EB vollständig.

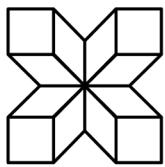
Gesetzesvorhaben im Bereich der Überwachung bergen per se hohe Risiko für die Grundrechte der betroffenen Personen. Sollte die federführende Verwaltungseinheit im EB irrtümlich festgehalten haben, dass eine DSFA durchgeführt wurde, obwohl tatsächlich lediglich

eine Risikovorprüfung mit der Feststellung eines geringen Risikos erfolgte, so sollte eine solche Einschätzung im vorliegenden Fall dennoch begründet werden.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Ueli Buri
Präsident privatim



Universal Privacy Alliance

To: Jean-Louis Biberstein

(responsable suppléant Service SCPT, responsable Droit et contrôle de gestion)
Service Surveillance de la correspondance par poste et télécommunication

T +41 58 462 26 27

jean-louis.biberstein@isc-ejpd.admin.ch

Response to: Surveillance des télécommunications et entreprises obligées de collaborer:
ouverture d'une consultation

Deadline: 6 May 2025

Date of submission: 22 April 2025

Respondent: Universal Privacy Alliance (UPA)

UID: CHE333772329

The Universal Privacy Alliance is a global alliance of entities in the financial privacy space, currently based in Switzerland. Our members value the use of privacy enhancing technologies for all individuals and provide the technical architecture that makes privacy enhancements possible in an increasingly surveilled world.

We wish to thank the Post and Telecommunications Surveillance Services (PTSS) for the opportunity to participate in this call for comments. It is an important matter to our industry that Switzerland remains the attractive place for business and technology development that it has been to date.

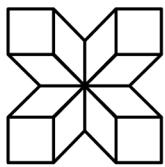
Many aspects of the new law pose a business and technological risk to our members. In particular, obligations to identify users for AAKD, collecting data and to remove encryption would fundamentally undermine the business models and society value that our members are trying to provide. Indeed, members of our industry have already left Switzerland over similar concerns and the current proposed surveillance measures add fuel to the fire.

The changes as proposed would make Switzerland a weaker technology nation.

Companies would leave Switzerland, reducing the local base of technological expertise and increasing Switzerland's reliance on providers from other nations. In addition, any supporting services for technology services such as legal expertise, regulatory expertise and accounting, would disappear. Indeed we believe that several Swiss companies, including from our member ranks¹, have already made this intention clear to the PTSS². At a time when digital sovereignty is an issue not just for Switzerland but also for the broader community of countries in Europe, this seems particularly ill-advised.

¹ Note the submission from NYMTech SA, Neuchatel.

² Note submissions from Proton and Threema.



Universal Privacy Alliance

It is a fallacy to consider content more privacy-sensitive than metadata. In fact, metadata determines what a person's community looks like. It is frequently nothing other than a forceful continuation of discrimination by other means. **The same harmful profiling that occurs when e.g. someone in religious attire or with a particular skin colour is given worse treatment than another peer, happens when a person whose social graph is unsavory is given such worse treatment.** As a community we need to deal with positive protection of group privacy to combat such discrimination³. A starting point is to not remove protection for such group privacy, or worse, declare such group privacy irrelevant.

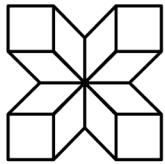
We believe the PTSS will find that their proposals additionally fall foul of adequate human rights protections, including the right to digital integrity and the right to security in the digital space which was recently voted into the fundamental law of Geneva and Neuchatel. The same cantons has adopted an article about digital sovereignty.

We propose that PTSS reconsiders the current categorisation of AAKD. In particular, **that it removes the obligation of identifying users** (Art. 19 para. 1 Rev.VÜPF, Art. 21 para. 1 Rev.VÜPF) **and collecting data for any size of AAKD** (Art. 18 para. 3 Rev.VÜPF, Art. 25 VÜPF, Art. 31 Rev.VÜPF). Swiss companies should not be punished for being successful and popular providers of technologies that individuals all over the world need to protect their own person and their communities.

In addition, and obviously, no AAKD should be forced to remove encryption (Art. 27 para. 3 BÜPF and Art. 50a Rev.VÜPF). In fact, the opposite encouragement is needed – AAKDs should be encouraged by applicable laws and regulations to adopt encryption for both metadata and for communication (end-to-end). When the opportunity arises, **Switzerland should be consulting with local operators to see how any currently licensed business** (such as a wired or wireless provider of electronic communications providers) **can be encouraged to require better and stronger security at the network equipment layer through their equipment purchase procedures.** We need not only to refrain from banning technologies necessary to defend sovereignty, human rights, and the right to digital integrity but also to create active encouragement to develop and deploy these technologies.

Finally, we note that the federal tribunal has always sided with businesses and individuals in cases that have been brought before them. The changes proposed by the PTSS are indeed a way to circumvent that consistent and user-friendly jurisprudence. **We hope that the PTSS upon closer consideration will reconsider the introduction of these changes and keep Switzerland a business-friendly country which can serve privacy enhancing technologies for an entire, sovereign European region and, indeed, the world.**

³ See e.g. Katja de Vries. Mireille Hildebrandt, Privacy, Due Process and the Computational Turn (2013) Routledge.



Universal Privacy Alliance

To: Jean-Louis Biberstein

(responsable suppléant Service SCPT, responsable Droit et contrôle de gestion)

Service Surveillance de la correspondance par poste et télécommunication

T +41 58 462 26 27

jean-louis.biberstein@isc-ejpd.admin.ch

Response to: Surveillance des télécommunications et entreprises obligées de collaborer:
ouverture d'une consultation

Deadline: 6 May 2025

Date of submission: 22 April 2025

Respondent: Universal Privacy Alliance (UPA)

UID: CHE333772329

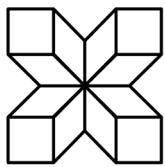
L'Alliance Universelle pour la Vie Privée est une alliance mondiale d'entités actives dans le domaine de la confidentialité financière, actuellement basée en Suisse. Nos membres valorisent l'usage des technologies de renforcement de la vie privée pour tous les individus et fournissent l'architecture technique qui rend ces améliorations possibles dans un monde de plus en plus surveillé.

Nous remercions les Services de Surveillance Postale et des Télécommunications (PTSS) pour l'opportunité de participer à cet appel à commentaires. Il est important pour notre secteur que la Suisse demeure un lieu attractif pour les affaires et le développement technologique, comme elle l'a été jusqu'à présent.

De nombreux aspects de la nouvelle loi représentent un risque commercial et technologique pour nos membres. En particulier, les obligations d'identification des utilisateurs pour l'AAKD, de collecte de données et de suppression du chiffrement compromettent fondamentalement les modèles économiques et la valeur sociétale que nos membres s'efforcent d'apporter. En effet, certains acteurs de notre secteur ont déjà quitté la Suisse pour des préoccupations similaires, et les mesures de surveillance actuellement proposées ne font qu'aggraver la situation.

Les modifications proposées affaibliraient la position de la Suisse en tant que nation technologique. **Des entreprises quitteraient le pays, réduisant ainsi la base locale d'expertise technologique et augmentant la dépendance de la Suisse envers des prestataires étrangers. De plus, tous les services de soutien aux technologies, tels que l'expertise juridique, réglementaire ou comptable, disparaîtraient.** Nous croyons d'ailleurs que plusieurs entreprises suisses, y compris parmi nos membres¹, ont déjà

¹ Note the submission from NYMTech SA, Neuchatel.



Universal Privacy Alliance

clairement exprimé cette intention auprès des PTSS². À une époque où la souveraineté numérique est un enjeu non seulement pour la Suisse mais aussi pour l'ensemble des pays européens, cela semble particulièrement mal avisé.

Il est fallacieux de considérer que le contenu est plus sensible en matière de vie privée que les métadonnées. En réalité, ce sont les métadonnées qui déterminent à quoi ressemble la communauté d'une personne. Elles deviennent souvent un vecteur insidieux de discrimination, une continuation brutale de traitements inéquitables par d'autres moyens. **Le même profilage préjudiciable que l'on observe, par exemple, lorsqu'une personne portant une tenue religieuse ou ayant une certaine couleur de peau est traitée moins favorablement qu'un pair, se produit également lorsqu'une personne dont le graphe social est jugé « indésirable » reçoit un traitement discriminatoire.** En tant que communauté, nous devons oeuvrer à la protection active de la vie privée collective pour lutter contre ce type de discrimination³. Un point de départ consiste à ne pas supprimer cette protection, voire pire, à ne pas déclarer la vie privée collective comme étant sans pertinence.

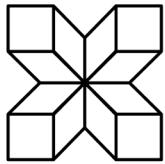
Nous pensons que les PTSS constateront que leurs propositions enfreignent également les protections adéquates des droits humains, y compris le droit à l'intégrité numérique et le droit à la sécurité dans l'espace numérique, récemment intégrés dans les lois fondamentales des cantons de Genève et de Neuchâtel. Ces mêmes cantons ont adopté un article relatif à la souveraineté numérique.

Nous proposons que les PTSS reconsidèrent la catégorisation actuelle des AAKD. En particulier, **nous recommandons la suppression de l'obligation d'identifier les utilisateurs** (Art. 19 para. 1 Rev.VÜPF, Art. 21 para. 1 Rev.VÜPF) **ainsi que celle de collecter des données quelle que soit la taille de l'AAKD** (Art. 18 para. 3 Rev.VÜPF, Art. 25 VÜPF, Art. 31 Rev.VÜPF). Les entreprises suisses ne devraient pas être pénalisées pour leur succès ni pour être des fournisseurs populaires de technologies dont les individus du monde entier ont besoin pour protéger leur personne et leurs communautés.

Par ailleurs, et cela va de soi, aucune AAKD ne devrait être contrainte de supprimer le chiffrement (Art. 27 para. 3 BÜPF and Art. 50a Rev.VÜPF). Bien au contraire, les AAKD devraient être encouragées par les lois et règlements applicables à adopter le chiffrement, tant pour les métadonnées que pour les communications (end-to-end). Lorsqu'une opportunité se présente, **la Suisse devrait consulter les opérateurs locaux afin d'examiner comment toute entreprise actuellement autorisée** (telle qu'un fournisseur câblé ou sans fil de services de communications électroniques) **pourrait être incitée à**

² Note submissions from Proton and Threema.

³ See e.g. Katja de Vries. Mireille Hildebrandt, Privacy, Due Process and the Computational Turn (2013) Routledge.



Universal Privacy Alliance

exiger une sécurité accrue au niveau des équipements réseau, notamment via leurs procédures d'achat. Il ne s'agit pas seulement de ne pas interdire les technologies essentielles à la défense de la souveraineté, des droits humains et du droit à l'intégrité numérique, mais aussi de promouvoir activement leur développement et leur déploiement.

Enfin, nous rappelons que le Tribunal fédéral s'est toujours rangé du côté des entreprises et des individus dans les affaires qui lui ont été soumises. Les modifications proposées par les PTSS constituent en effet une tentative de contournement de cette jurisprudence constante et favorable aux utilisateurs. **Nous espérons que les PTSS, à la lumière d'un examen approfondi, renonceront à introduire ces modifications et maintiendront la Suisse comme un pays accueillant pour les entreprises, capable de soutenir les technologies de protection de la vie privée pour une région européenne souveraine – et, en réalité, pour le monde entier.**

*Vernehmlassungsantwort zu den Teilrevisionen der VÜPF und der VD-ÜPF
gemäss Schreiben des EJPD vom 29. Januar 2025*

Datum	4. Mai 2025
Verfasser (Unternehmen)	SwissIX Internet Exchange (Verein)
Kontaktperson bei Fragen (Name/Tel./E-Mail)	Luzi von Salis, 079 432 46 43, luzi.vonsalis@swissix.ch

Dieses Dokument geht an:

Eidgenössisches Justiz- und Polizeidepartement EJPD, ptss-aemterkonsultationen@isc-eipd.admin.ch

Sehr geehrter Herr Bundesrat Jans, sehr geehrte Damen und Herren

Wir beziehen uns auf das am 29. Januar 2025 eröffnete Vernehmlassungsverfahren zu Teilrevisionen von VÜPF und VD-ÜPF und bedanken uns für die Möglichkeit einer Stellungnahme.

Wir lehnen die geplante Teilrevisionen der VÜPF und der VD-ÜPF in aller Deutlichkeit und vollumfänglich ab.

Im Bericht des Bundesrates zur aktuellen Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF und der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) ist zu lesen, dass die Revision im Wesentlichen auf die Anpassung der Verordnungen an die KMU-Freundlichkeit abziele. Ein grosser Teil der vorgeschlagenen Änderungen *verfolgt aber gerade das Gegenteil*.

Die Geschäftsgrundlagen von Schweizer Unternehmen wie Threema, Proton und anderer KMU, die weltweit einen hervorragenden Ruf als Anbieterinnen sicherer Kommunikationsdienste im Internet geniessen, drohen durch die Vorlage zerstört zu werden. Die Sicherheit des Internets in der Schweiz soll mit der Revision der Überwachung jeglichen Internetverkehrs regelrecht untergeordnet werden: «**Sicherheit vor Freiheit» ist das neue Paradigma**. Dieses zieht sich wie ein roter Faden quer durch diese völlig verunglückte Reform. KMU, die aus der Schweiz heraus Internet-Dienste anbieten («abgeleitete Kommunikationsdienste» in der Terminologie des Gesetzes), soll die Schweiz als Standort geradezu vergällt werden. Dies scheint denn auch zu gelingen: **Erste der betroffenen Unternehmen haben bereits angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen** (siehe Tages-Anzeiger vom 1. April 2025).

Ein derartiger Paradigmenwechsel, weg von KMU-Schutz und Überwachung mit Augenmass, hin zu knallharter Überwachung, die alle anderen Interessen unterordnet, wird durch das geltende Gesetz (BÜPF) keineswegs gestützt. Der Paradigmenwechsel widerspricht vielmehr geradezu dem Geist des ursprünglichen BÜPF, das Internetdienste, die in der Schweiz meist von KMU betrieben werden, gerade von der Implementierung teurer Überwachungsmassnahmen schützen wollte, und das eine austarierte Interessenabwägung vorsah zwischen Privatsphäre und Freiheit auf der einen Seite und staatlicher Überwachung auf der anderen Seite.

Entgegen dem im Begleitbericht zum vorgelegten Entwurf erklärten Ziel, die «finanzielle Belastung der KMU gering zu halten», stuft die Vorlage eine grosse Mehrheit der Schweizer Anbieterinnen von Internetdiensten in eine höhere Stufe auf, und zwingt sie neu auch in jenen Bereichen zu einer kostspieligen aktiven Überwachungstätigkeit, wo bisher nur eine KMU-freundliche Duldungspflicht bestand. Dies verschiebt das bisherige Gleichgewicht der Interessen zwischen Strafverfolgung und betroffenen Anbieterinnen in drastischer Weise zulasten der betroffenen Anbieterinnen.

Die vorgeschlagenen Anpassungen bringen ganz erhebliche Risiken für den Innovations- und Wirtschaftsstandort Schweiz mit sich und erfüllen die Kernziele der Revision, die Entlastung von KMU, gerade nicht. Der Ruf der Schweiz als sicherer Hafen für vertrauenswürdige IT-Anbieter droht durch die Revision nachhaltig beschädigt zu werden. Deshalb lehnen wir die Revision vollumfänglich ab.

Auch **die Schweizer Armee** nutzt solche Dienste, wie beispielsweise Threema, und zwar gerade aufgrund des hohen gebotenen Sicherheitsstandards. Die Annahme dieser Revision, welche dieses Sicherheitsniveau gezielt untergraben will, verletzt damit indirekt auch das direkte Interesse der Schweiz an lokal betriebenen Hochsicherheitsanwendungen. Gerade in der heutigen Zeit, in der die Zuverlässigkeit der grossen US-Anbieter in ihrer Abhängigkeit von einer zunehmend erratisch agierenden US-Regierung mehr und mehr in Frage steht, erscheint dies als **inakzeptable Hochrisikostrategie**.

Nicht zuletzt ist mit Nachdruck darauf hinzuweisen, dass die Revision die Überwachung ganz allgemein stark ausweitet. Dies ist mit der durch den Gesetzgeber im BÜPF festgelegten, fein austarierten Interessenabwägung zwischen Freiheit und Privatsphäre der Einwohner der Schweiz einerseits und Sicherheit durch Überwachungsmassnahmen andererseits absolut nicht vereinbar. Die Revision entpuppt sich geradezu als eine Art Wunschkonzert für Überwachungsbehörden. Insbesondere ist künftig auch **eine komplette inhaltliche Überwachung des gesamten Internetverkehrs** der Schweiz vorgesehen. Dies ohne dass eine solche inhaltliche Überwachung durch die gesetzlichen Grundlagen des BÜPF in irgend einer Weise gedeckt wäre: Zulässig ist gemäss BÜPF einzig und allein die Überwachung von Randdaten des Fernmeldeverkehrs, und selbst die Zulässigkeit der in diesem Kontext angewendeten anlasslosen Vorratsdatenspeicherung von Randdaten ist bis heute umstritten und Gegenstand von Gerichtsverfahren, ja in der EU bereits höchstrichterlich als menschenrechtswidrig erkannt. Die durch die Verordnungsrevision eingeführte *Inhaltsüberwachung* ist in der Schweiz damit erst recht **offensichtlich illegal und verfassungswidrig**.

Abschliessend sei noch der Hinweis angebracht, dass wir die Gesetzgebungstechnik des Entwurfs für überaus schlecht halten. **Sowohl der Verordnungstext als auch der zugehörige erläuternde Bericht sind über weite Strecken höchst verwirrend und unverständlich formuliert**, unter anderem mit einer Vielzahl von Querverweisen, technischen Fehlern und unklarer Begrifflichkeit (für ein Beispiel hierfür siehe unten, Bemerkungen zu Art. 43a). Die Texte sind in dieser Form selbst für Fachleute über weite Strecken nicht zu verstehen, geschweige denn als Ganzes zu überblicken. Für KMU, die durch die Revision neu mit erheblich strengerem Pflichten konfrontiert werden, ist eine rechtskonforme Umsetzung dieser Vorlage daher ein schlicht aussichtloses Unterfangen.

Das Legalitätsprinzip gemäss Art. 5 Bundesverfassung fordert vom Gesetzgeber, dass Gesetzestexte für die Adressaten verständlich formuliert sind. Die Texte der Verordnungsrevision genügen dieser Anforderung offensichtlich in keiner Weise. Nur schon aufgrund der völlig fehlenden Verständlichkeit ist die Verfassungsmässigkeit der Revision insgesamt *höchst zweifelhaft*. Wir fordern nur schon deshalb einen Rückzug der vorgelegten Texte, eine komplette Überarbeitung zur Verbesserung der Verständlichkeit und eine erneute Auflage zur Vernehmlassung.

Mit freundlichen Grüßen



■■ SwissIX Internet Exchange, Luzi von Salis

Bemerkungen zu einzelnen Artikeln der VÜPF

Nr.	Artikel	Antrag	Begründung / Bemerkung
VÜPF / OSCPT / OSCPT			
0.	Alle Artikel	Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.	<p>Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kunden auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.</p> <p>Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.dgl. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.</p>
1.	16b, Abs. 1	Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.»	Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile, wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Anforderungen in Kauf nehmen.
2.	16c, Abs. 3	Streichung von lit. a «automatisierte Erteilung der Auskünfte (Art. 18 Abs. 2);»	Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Dies untergräbt rechtsstaatliche Prinzipien doppelt: Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>«natürliche» Schutzmechanismen gegen eine überschiessende, missbräuchliche oder zumindest unverhältnismässige Nutzung solcher Massnahmen durch die Untersuchungsbehörden.</p> <p>Der vorgesehene Umsetzungszeitraum von 12 Monaten für die rechtssichere Implementierung eines derart komplexen Systems völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.</p>
3.	Art. 16d	<p>Streichung von Online-speicherdiensten und VPN-Anbietern in der Auslegung</p>	<p>Eine klarere Definition des Begriffs AAKD ist begrüssenswert, doch die neue Auslegung gemäss erläuterndem Bericht geht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdiensten wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter, etc.) genutzt werden.</p> <p>Art. 2 lit. c BüPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug den gesetzlichen Rahmen sprengt. Onlinespeicherdiene sind deshalb aus Art. 16d zu streichen.</p> <p>Zudem anerkennt der erläuternde Bericht, dass VPNs zur Anonymisierung der Nutzer*innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Anbieter von VPNs sind daher ebenfalls aus dem Geltungsbereich von Art. 16d auszunehmen.</p>
4.	Art. 16e, Art. 16f und Art. 16g	<p>Streichung der Artikel und Beibehaltung der bestehenden Kriterien</p> <p>Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).</p>	<p>Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch diametral entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung. Dies daher, weil neu KMU bereits mit mehr als 5'000 Nutzern erfasst werden.</p> <p>Die Einführung von 5000 Nutzern als gesondert zu beurteilende Untergrenze verletzt aus unserer Sicht bereits Art. 27 Abs. 3 BüPF, denn 5000 Personen keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strenger Überwachungsmassnahmen, gerechtfertigt wären. 5000 Nutzer werden in der digitalen Welt vielmehr sehr rasch erreicht.</p> <p>Zusätzlich führt das Einführen eines «Konzerntatbestandes» in Art. 16f Abs. 3 zu massiven Problemen, da die Produkte nun nicht mehr für sich alleine eine bestimmte Grösse erreichen müssen, sondern die rele-</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>vanten Zahlen anhand des Umsatzes des Unternehmens, bzw. in Konzernverhältnissen sogar des Konzerns bestimmt werden. Vor allem bei Unternehmen mit Beteiligungsfirmen im Hintergrund fallen nun neu alle Dienstleistungen und Produkte automatisch unter die härteste Stufe, egal ob sie sich erst in einem frühen Entwicklungsstadium befinden. Dies behindert Innovation, da jedes Projekt bereits mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden müsste. Durch diese extreme Einstieghürde wird der Innovationsstandort Schweiz nachhaltig geschädigt.</p> <p>Gleichzeitig wird auch der Wirkungsbereich der VÜPF stark erweitert. Während heute ein Unternehmen einen grossen Teil seiner Geschäftstätigkeit durch abgeleitete Kommunikationsdienste erbringen muss (Art. 22 Abs. 1 lit. b und Art. 52 Abs. 1 lit. b VÜPF), fällt dieses Kriterium neu weg. Dadurch können künftig auch Unternehmen, deren Geschäftstätigkeit nur am Rande auf abgeleiteten Kommunikationsdiensten basiert, wie Onlineshops, Marktplätze, Auktionsplattformen, Zeitungen, Computerspielhersteller und zahlreiche weitere Unternehmen, unter die VÜPF fallen – allein deshalb, weil ihre Produkte irgendeine Form privater Kommunikation zwischen Nutzer*innen und/oder Drittanbietern ermöglichen.</p> <p>Die vorgeschlagene Regelung stünde sodann im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali, das die zu weite Betroffenheit und die seltene Anwendung von Downgrades kritisierte: «Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»</p> <p>Statt KMU zu entlasten, führt die Revision neu sogar zu einer «automatischen Hochstufung per Verordnung ohne konkretisierende Verfügung (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.</p> <p>Die neue Regelung steht zudem in offensichtlichem Widerspruch zur bisherigen Praxis, denn bis heute wurde gemäss Angaben des Dienst-ÜPF keine einzige AAKD hochgestuft. Auch der Bundesrat stützte sich ausdrücklich auf die geltende Kombination von drei Schranken – einem Unternehmensfokus auf Kommunikationsdienste, einer Umsatzgrenze von 100 Millionen Franken sowie einer grossen Nutzerzahl – als er noch 2023 begründete, die Umsetzung des BÜPF sei gerade wegen der genannten Schranken als KMU-freundlich zu verstehen. Die vorliegende Revision hebt jedoch genau diese Kombination kumulativer Kriterien auf und will die einzelnen Kriterien künftig alternativ anwenden bzw. streicht sie sogar vollständig. Dadurch verlieren die bisherigen Schutzmechanismen ihre Wirkung, und das BÜPF soll neu auf viele KMU Anwendung finden, die früher nicht unter Gesetz und Verordnung fielen.</p> <p>Die Analyse der offiziellen Statistik des Dienstes ÜPF macht die offensichtliche Unverhältnismässigkeit dieses Ansinnens deutlich. Im Jahr 2023 betrafen 98,95 % der total 9'430 Überwachungen allein</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,05 % für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,73 % wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100 % des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.</p> <p>Wesentlich ist insbesondere eine neue Pflicht zur Identifikation der Nutzer: Hiervon betroffen sind nicht nur alle AAKD mit reduzierten oder vollen Pflichten (und damit de facto fast alle AAKD der Schweiz), sondern auch all deren Wiederverkäufer. Im Ergebnis führt die neue Verordnung aus unserer Sicht dazu, dass man sich bei keinem marktrelevanten Dienst mehr anmelden kann, ohne den Pass, Führerschein oder ID zu hinterlegen oder zumindest Daten wie eine Telefonnummer anzugeben, die man ohne Pass oder ID nicht erhalten kann.</p> <p>Die automatische Hochstufung an sich führt bereits zu erheblicher Rechtsunsicherheit bei den betroffenen Unternehmen. Unter dem bestehenden System werden die generell-abstrakten Normen der VÜPF mittels Verfügung auf einen konkreten Einzelfall angewendet. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes ist aber im Zweifelsfall möglicherweise nur schwer zu beantworten. Zweifelsohne besteht hier ein schutzwürdiges Interesse seitens der AAKD daran, zu wissen, ob sie die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Nur das bisherige System entspricht den allgemeinen Grundsätzen des Verwaltungsverfahrens, welches für die Anwendung einer generell-abstrakten Norm eine Konkretisierung durch die Verwaltung voraussetzt. Von einer automatischen Hochstufung von AAKD ist daher aus Gründen der Rechtssicherheit abzusehen. Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.</p> <p>Gegenüber der alten VÜPF erweitert die Revision die Pflichten zur Automatisierung sodann noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragen wie z.B. IR_59 und IR_60, welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen. Genau diese Möglichkeit einer manuellen Intervention ist aber für die Provider kritisch, um Missbräuche zu verhindern, die wiederum die Verträge mit ihren Kunden und das Fernmeldegeheimnis verletzen könnten. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente damit erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 Bst. b der alten VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grossen[n] Teil ihrer Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. Damit fallen insbesondere bereits Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz. Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Dies setzt der Innovation in der Schweiz neue riesige Hürden entgegen.</p> <p>Auch Non-Profit-Organisationen wie die Signal Foundation, die kaum Umsätze erwirtschaften, geraten unter diese verschärften Vorgaben. Während sie bisher unter Duldungspflichten verbleiben konnten, solange sie Art. 22 Abs. 1 VÜPF nicht erfüllten, wird neu allein auf die Anzahl der Nutzer*innen abgestellt, womit z.B. Signal neu als AAKD mit vollen Pflichten erfasst würde. Dies würde dazu führen, dass Signal in der Schweiz entweder zu einem Rückzug aus dem Markt gezwungen wird oder erhebliche rechtliche Konsequenzen riskiert, da Signal keine IP-Adressen speichert und somit gegen Art. 19 RevVÜPF verstößt.</p> <p>Die Regelung ignoriert zudem wirtschaftliche Realitäten: Ein hoher Nutzerkreis bedeutet bei Non-Profits keine finanzielle Tragfähigkeit für umfangreiche Überwachungsmassnahmen. Damit werden Open-Source- und Non-Profit-Lösungen gezielt aus dem Markt gedrängt, während bestehende Monopole wie WhatsApp (96 % Marktanteil in der Schweiz) gestärkt werden. Die neue Regelung ist daher aus ökonomischer Sicht zu verwerfen. Das Kriterium der reinen Nutzerzahl ist ungeeignet und muss gestrichen werden.</p> <p>Nicht zuletzt schwächt die Regelung auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger*innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, Ende-zu-Ende-verschlüsselter Kommunikation ist heute wichtiger denn je.</p> <p>Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade als rechtswidrig gilt (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer*innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, sondern allein diese Anhäufung an Daten malt eine Zielscheibe auf den Rücken von Schweizer Unternehmen und Dienstleistungen für Hackerangriffe aus der ganzen Welt.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Weiters ist zu erwähnen, dass es gar nicht erwiesen ist, dass die Speicherung der fraglichen Daten eine merklich höhere Quote erfolgreicher Ermittlungen durch die Strafverfolgungsbehörden mit sich bringen würde. Im Gegenteil müssen die bereits existierenden Sekundärdaten, die allein durch die Bereitstellung eines Dienstes für den Nutzer entstehen, besser genutzt werden. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisbrauch via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfügt, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden. Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren.</p> <p>Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Souveränität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.</p> <p>Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das Datenschutzgesetz. Der Entwurf bringt nicht, wie der Begleitbericht dem Leser in geradezu in Orwell'scher Manier weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit und steht in direktem Gegensatz zum besagten Postulat 19.4031.</p> <p>Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen, und das bestehende System muss beibehalten werden.</p>
5.	Art. 16h Abs. 2	Streichung der Ausführung im erläuternden Bericht und ein Abstellen der Formulierung auf die gleichzeitige Anzahl Nutzer.	Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Nutzer*innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 Rev.VÜPF, gemäss dem die das WLAN erschliessenden FDA die Verantwortung für die Identifikation der Nutzer der WLANs tragen.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer*innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24) oder die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22). Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDAs unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden. Unter der bestehenden Regelung konnte eine FDA anhand der Lokation (z.B. Bibliothek, Flughafen) eine Einschätzung treffen. Die neue Definition hingegen würde von ihr verlangen, Zugriff auf jedes private Netzwerk zu erhalten, um Hardware und Einstellungen zu prüfen – ein offensichtlich verfassungswidriges und auch praktisch unmögliches Unterfangen. Diese vage Formulierung führt zu anhaltender Rechtsunsicherheit für FDA.</p> <p>Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten.</p> <p>Zudem könnte Art. 16h dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist*innen, Whistleblower*innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer*innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen. Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt.</p>
	Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2	Streichung des «Konzernatbestand» und Beibehaltung der bestehenden Regelung	<p>Die Verordnung nimmt neu nicht mehr die Umsatz- und Nutzerzahlen der betroffenen Unternehmen, sondern die Zahlen des jeweiligen Konzerns als Basis für Up- und Downgrades. Die Begründung zur Einführung dieses «Konzernatbestands», wonach die neue Regelung für die betroffenen Unternehmen zu einer Vereinfachung führe, ist kontraintuitiv, ja offensichtlich falsch und irreführend. In der Praxis sind die betroffenen Unternehmen nämlich schon heute verpflichtet, ihre Buchhaltung nach Produkten aufzugliedern. Somit können die Kennzahlen bereits heute sehr einfach festgestellt werden. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.</p>
6.	Art. 19 Abs. 1	Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation	<p>Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vor sieht.</p> <p>Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des Schweizer Datenschutzgesetzes, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch der Schutz der Schweizer Kundschaft massiv</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
		von Teilnehmenden.	<p>beeinträchtigt wird. Datenschutzfreundliche Unternehmen werden bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.</p> <p>Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Dies wahrt nicht nur den Datenschutz, sondern schützt auch die Wettbewerbsfähigkeit von KMU, stärkt den Innovationsstandort Schweiz und die digitale Souveränität unseres Landes.</p>
7.	Art. 18	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.
8.	Art. 19 Abs. 2	Ersatzlose Streichung zugunsten bestehender Regelung	Eine Überwachung von Kunden durch FDA, ob diese die neuen Vorgaben der VÜPF zu WLANs einhalten (Art. 19 Abs. 2 Rev. VÜPF), und erst recht die dazu gelieferte Erklärung im erläuternden Bericht, wonach die FDA die Identifikation der WLAN-Nutzer vorzunehmen hätten, ist weder gesetzeskonform noch zumutbar (siehe vorstehend). Art. 19 Abs. 2 ist ersatzlos zu streichen.
9.	Art. 21 Abs. 1 lit. a	Streichung	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.
10.	Art. 22	beibehalten	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.
11.	Art. 11 Abs. 4	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.
12.	Art. 16b	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.
13.	Art. 31 Abs. 1	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.
14.	Art. 51 und 52	beibehalten	Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.
15.	Art. 60a	Streichung des Artikels	Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Art. 60a VÜPF (Erläuterung Bundesrat: «...lediglich redaktionelle Änderungen....») sieht vor, dass Fernmelddenstanbieterinnen über einen rückwirkenden Zeitraum von 6 Monaten alle Ziel-IP-Adressen liefern müssen, welche ihre Kunden besucht haben. Damit wird einerseits das Surfverhalten der gesamten schweizerischen Bevölkerung anlasslos und völlig unverhältnismässig ausspioniert. Andererseits wird die klare Vorgabe des BÜPF umgangen, das nur die Speicherung von Randdaten, aber nicht die Speicherung von Inhaltsdaten vorsieht.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Die geplante Überwachung des Internetverkehrs führt zu einer Überwachung, wer im Internet welche Adressen besucht hat. Dies geht zweifellos über die Schranken der gesetzlichen Regelung hinaus, dies insbesondere nachdem bereits die Aufzeichnung reiner Randdaten höchst umstritten und Gegenstand laufender Gerichtsverfahren ist. Hinzu kommt folgendes: Während bislang die Überwachung einer IP-Adresse nur im Rahmen einer sog. Echtzeit-Überwachung zulässig war, welche entsprechende Bewilligungen durch ein Gericht erforderte, muss neu nur noch ein einfaches Auskunftsbegehren durch die zuständige Behörde genehmigt werden. Die Abfragen erfolgen automatisiert.</p> <p>Art. 60a sieht weiter vor, dass bei nicht exakt zuordenbaren IP-Adressen die kompletten Listen aller Nutzerinnen und Nutzer zu liefern ist. IP-Adressen sind ein rares Gut. Alle FDA teilen diese den Nutzenden im Millisekunden-Takt zu. Da die Zeitstempel der Systemanbieter nicht immer übereinstimmen, sind diese IP-Adressen nicht immer eindeutig einem Nutzenden zuzuordnen. Neu müssen Provider nun komplettene Listen aller Nutzenden liefern. Dies bringt Zehntausende in den Fokus von Überwachungsbehörden, was auf eine Art Rasterfahndung nach Delikten über grosse Teile der Bevölkerung hinausläuft. Entdecken Strafverfolger dabei zufälligerweise etwas, können sie umgehend Strafverfahren einleiten.</p> <p>Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde sodann gemäss Bericht gezielt auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten.</p> <p>Art. 60a ist zu streichen.</p>
16.	Art. 42a und Art. 43a	Streichung des Artikels	<p>Sowohl Art. 42a als auch Art. 43a fordern die Abrufbarkeit des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Nicht nur gilt auch hier wieder die Limite von 5'000 Nutzern, was somit fast die gesamte AAKD-Landschaft der Schweiz flächendeckend umfasst, sondern solche Abfragen sollen nun auch durch eine einfach «IR_» Abfrage gemacht werden können, welche im Gegensatz zu den «HD_»-Abfragen und den «RT_»-Überwachungen ohne weitere juristische Aufsicht automatisiert abgerufen werden können, obwohl es sich auch hier um das Abrufen einer IP-Adresse in der Vergangenheit handelt, genau wie bei den «HD_» abfragen, welche deutlich strenger reglementiert sind. Es ist nicht nachvollziehbar und verletzt aus unserer Sicht die gesetzliche Grundlage des BÜPF, dass Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber.</p> <p>Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser Automatisierten Auskünfte ergibt. Durch das Fehlen solcher Limiten könnte daher z.B. alle 5 Minuten eine solche Anfrage automatisiert gestellt werden. Zunächst können sich dadurch lärmende Kosten für die betroffenen AAKD ergeben. Sodann können die Anfragen an ein automatisiertes Auskunftssystem gestellt werden, und es können auf diese Weise viele der Informationen welche ursprünglich über die juristisch</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>sichereren HD_ und RT_ Auskunfts-/Überwachungstypen liefern, neu über den rechtlich unsicheren IR_- Typ eingeholt werden. IR_59 und IR_60 ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne dass sie den benötigten Kontrollen dieser invasiven Überwachungsarten unterliegen würden.</p> <p>Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind, wie dies das BÜPF vorsieht.</p> <p>Die beiden Artikel sind daher vollumfänglich zu streichen.</p> <p>Diese neue Regelung und der zugehörige erläuternde Bericht sind im Übrigen eklatante Beispiele für die eingangs bemängelte überaus verwirrende und unverständliche Darstellung von Verordnungstext und erläuterndem Bericht.</p> <p>Im erläuternden Bericht steht auf S. 39 wörtlich:</p> <p><i>«In Absatz 1 sind die zu liefernden Angaben geregelt. Gemäss Buchstabe a ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin der oder dem Teilnehmenden einen solchen zugeteilt hat. Der «eindeutige Dienstidentifikator» gemäss Buchstabe b bezeichnet den Fernmelde- oder abgeleiteten Kommunikationsdienst, auf den sich die Antwort bezieht, eindeutig im Bereich der Anbieterin. In Buchstabe c werden die zu liefernden Angaben über den Ursprung der Verbindung bei der letzten zugriffsrelevanten Aktivität aufgezählt. Diese Angaben können für die Identifikation der Benutzerinnen und Benutzer nützlich sein.»</i></p> <p>Der Leser bzw. die Leserin urteile selber über die Verständlichkeit.</p> <p>Folgende Begriffe sind auch für den fachkundigen Leser nicht nachvollziehbar, bzw. es stellen sich folgende Verständnisfragen:</p> <ul style="list-style-type: none"> - Eindeutiger Identifikator: Was ist gemeint? Ist die Kundennummer des Internetproviders gemeint? Oder jene des genutzten dritten Fernmeldedienstes oder abgeleiteten Kommunikationsdienstes? Wie soll der Internetprovider überhaupt an diese Daten herankommen? - Eindeutiger Dienstidentifikator: Muss der Internetprovider eine Liste aller möglichen durch seine Kunden im Internet genutzten Kommunikationsdienste führen und aufzeichnen, muss er zudem aufzeichnen welcher Kunde welchen Dienst wann genau genutzt hat? Woher hat er diese Liste? Wie kann er herausfinden, ob ein Kunde gerade einen bestimmten Dienst nutzt? Gilt dies auch für ausländische Dienste? Nur für AAKD, für ausländische Fernmeldedienste, oder für alle Internetangebote weltweit? Der erläuternde Bericht bleibt hier völlig unklar.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<ul style="list-style-type: none"> - Was ist mit «Antwort» gemeint? Die Antwort des Servers des abgeleiteten Kommunikationsdienstes, den der Kunde besucht hat, oder die Antwort des Kundengeräts auf eine Nachricht von diesem Kommunikationsdienst? - Was ist mit «eindeutig im Bereich der Anbieterin» gemeint? Die Formulierung ist auch hier unverständlich. - Wie soll man sich eine «Antwort von einem anderen Fernmeldedienst» vorstellen? Muss ein Internetprovider die Herkunft sämtlicher auf seinem Netz eintreffenden Datenpakete aufzeichnen und dem Dienst ÜPF auf Anfrage diese Aufzeichnungen herausgeben? Wie soll die gigantische Masse an Daten, die durch ein solches Logging anfällt, durch die Internetprovider gemanaged werden? - Was ist mit «letzter zugriffsrelevanter Aktivitäten» gemeint? Geht es hier um die durch Kunden des Internetproviders aufgerufenen AAKD und andere Internetangebote? Wie soll der Internetprovider wissen, ob eine durch den Kunden aufgerufene IP-Adresse zu einem überwachungspflichtigen AAKD gehört, oder allenfalls zu einem nicht überwachungspflichtigen Dienst? Muss er einfach den ganzen Verkehr aufzeichnen? Wie weit zurück gehen die «zugriffsrelevanten» Aktivitäten? Müssen alle Daten für sechs Monate aufbewahrt werden? - Abgesehen davon: Wo wäre die gesetzliche Grundlage im BüPF für die vorgesehene inhaltliche Überwachung des Internetverkehrs? Das BüPF selber regelt bisher ausschliesslich die Überwachung der Randdaten, nicht aber von Inhaltsdaten, und spätestens dann, wenn Randdaten einen passant auch Auskunft über die vom Kunden abgerufenen Inhalte geben, handelt es sich dabei um Inhaltsdaten, deren Sammlung erst recht gesetzes- und verfassungswidrig wäre, nachdem schon das Sammeln reiner Randdaten als menschenrechtswidrig taxiert wurde.
17.	50a	Artikel streichen	<p>Art. 50a sieht neu vor, dass Anbieter verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Diese Pflicht gilt nicht mehr nur für FDA (Art. 26 BüPF) oder ausnahmsweise für ausgewählte AAKD von hoher wirtschaftlicher Bedeutung (Art. 27 BüPF), sondern soll nun vorgabemässig und ohne Differenzierung auf sämtliche Anbieter mit mehr als 5'000 Teilnehmern angewendet werden, womit wohl fast die gesamte Schweizer AAKD-Branche betroffen ist (kaum ein Produkt ist lebensfähig mit weniger als 5000 Teilnehmern).</p> <p>Dies stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar.</p> <p>Diese Ausweitung ist nicht nur unverhältnismässig, sondern gefährdet aktiv nahezu die gesamte Schweizer IT-Branche: Indem de facto alle Anbieter vorgabemässig gezwungen werden, ihre Verschlüsselungssysteme für Behörden jederzeit entschlüsselbar zu gestalten, entstehen enorme Sicherheitsrisiken, denn</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Verschlüsselung ist wie eine Eierschale: Unversehrt ist sie stark, aber der kleinste Riss führt zu einer erheblichen Schwächung. Die betroffenen Systeme werden durch den vom Verordnungsgeber nun verpflichtend vorgesehenen Einbau von Hintertüren anfälliger für Hackerangriffe, Datenmissbrauch und Spionage. Dies widerspricht Art. 13 BV und dem diesen konkretisierenden Datenschutzgesetz, das den Schutz personenbezogener Daten ausdrücklich durch wirksame technische Massnahmen – insbesondere Verschlüsselung – vorschreibt. Eine durch den Anbieter aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung in jedem Fall.</p> <p>Genau eine solche Schwächung der Verschlüsselung wurde kürzlich vom Europäischen Gerichtshof für Menschenrechte im Fall PODCHASOV gegen Russland (33696/19) als Verstoss gegen Grundrechte gewertet. Art. 50a verstösst somit auch gegen geltendes Völkerrecht.</p> <p>Nebst diesem Verstoss gegen das Völkerrecht wird aber auch das Gebot der Verhältnismässigkeit aus Art. 36 BV nicht eingehalten, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördendarbeit steht. Wie bereits bei Art. 16e, Art. 16f und Art. 16g erwähnt, müssen zuerst die einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.</p> <p>Zusätzlich, und wie bereits bei Art. 16d erwähnt, verhindert Art. 50a die effektive Erbringung von VPN-Diensten. Bei solch einem VPN kontrolliert der Betreiber sowohl den Eingangs- als auch den Endpunkt. Da die Kommunikation vom Endpunkt zu einer Webseite aufgrund der vorherrschenden Struktur im allgemeinen Internet nicht End-zu-End-Verschlüsselt erfolgen kann, werden schon kleine VPNs (mit 5000 Nutzern) dazu gezwungen ihre eigene Verschlüsselung zu entfernen und ihre Kunden zu überwachen. Da der Schutz der Privatsphäre der Nutzer*innen von VPNs just den Kernpunkt oder USP der Dienstleistung darstellt, werden Schweizer VPN-Anbieterinnen hierdurch am internationalen Markt übermässig benachteiligt, ja ihres eigentlichen Daseinszwecks beraubt.</p> <p>Wesentlich ist zudem, dass Anbieter von Mail- oder Messaging-Apps zwangsläufig die Nachricht in der App in einer menschenlesbaren Version anzeigen muss, und dass an dieser Stelle die End-zu-End-Verschlüsselung notwendigerweise bereits entfernt ist. Der Wortlaut von Art. 50a lässt entgegen sämtlichen Beteuerungen des Dienstes ÜPF bereits anlässlich der letzten Revision der VÜPF weiterhin offen, ob eine Entfernung der Verschlüsselung auch an dieser Stelle gefordert werden können soll. Angesichts der seit</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			Jahren erkennbaren Tendenz der Schweizer Überwachungsbehörden, die Anwendbarkeit des Überwachungsrechts laufend weiter auszudehnen und sich dabei nur durch Gerichte bremsen zu lassen, ist bei dieser Gelegenheit erneut die Klarstellung zu fordern, wonach die Entfernung von Verschlüsselungen, die erst in der Sphäre des Benutzers angebracht werden (wenngleich auch durch Software der Anbieterin) nicht verlangt werden darf. Dies ist zumindest im erläuternden Bericht zu erwähnen. Der erneute Verzicht wäre nichts anderes als eine Einladung an die Überwachungsbehörden, die Einführung einer offensichtlich illegalen und vom BÜPF keineswegs vorgesehenen «Chatkontrolle» auf dem «Auslegungsweg» vorzunehmen.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Artikel	Antrag	Begründung / Bemerkung	
VD-ÜPF / OME-SCPT / OE-SCPT			
Art. 14 Abs. 3 VD-ÜPF	Streichung	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit 5000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Absatz ist daher ersatzlos zu streichen.	
Art. 14 Abs. 4 VD-ÜPF	Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten.	Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der unterworfenen AAKD massiv. Dies ist wie beschrieben weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.	
Art. 20 Abs. 1 VD-ÜPF	Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.	



Die Schweizerische Post AG

Stab CEO

Regulatory Affairs

Wankdorffallee 4

3030 Bern

Telefon +41 58 341 15 64

Fax +41 58 667 33 73

www.post.ch

Die Schweizerische Post AG, Stab CEO RA, Wankdorffallee 4, 3030 Bern

Eidg. Justiz- und Polizeidepartement EJPD

Herr Bundesrat Beat Jans

Bundesrain 20

3003 Bern

Als PDF/Word an:

ptss-aemterkonsultationen@isc-ejpd.admin.ch

Datum 5. Mai 2025
Kontaktperson Patrizia Rentsch
E-Mail patrizia.rentsch@post.ch
Direktwahl 058 341 22 21

Stellungnahme der Schweizerischen Post zur Vernehmlassung über die Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, im Rahmen der Vernehmlassung über die Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs Stellung nehmen zu können.

Unser Alltag wird immer digitaler und die Bedürfnisse der Menschen ändern sich. Daten und der einfache, sorgsame Umgang mit ihnen werden immer wichtiger. Die Post sieht in der Digitalisierung grosse Chancen für die Schweiz. Die Post baut daher ihre Rolle als relevante Anbieterin von digitalen Kommunikationsplattformen für einen intuitiven, vertrauensvollen Austausch und sicheren Umgang mit Daten für alle Menschen, Unternehmen und Behörden aus und leistet damit einen Beitrag zu einer digital vernetzten Schweiz. Digitale Sicherheit hat für die Post dabei höchste Priorität, denn Cyberangriffe und Betrugsfälle im Internet nehmen stetig zu.

Mit der Teilrevision der Verordnung zur Überwachung des Post- und Fernmeldeverkehrs will der Bund die Kompetenzen des Dienstes ÜPF ausweiten. Strafvermittler erhalten neue Überwachungsarten und Zugriff auf weitere Kommunikationsanbieter. Mit den neuen Verordnungsbestimmungen führt der Bundesrat weitere Kategorien von Kommunikationsanbietern ein. Zudem werden die Art und der Umfang der Mitwirkungspflichten angepasst.

Im Zusammenhang mit dem BÜPF bzw. der VÜPF steht für die Post ihr Kommunikationsdienst IncaMail im Fokus. IncaMail ist eine Lösung, die heute von der Firma Tresorit – einer Tochtergesellschaft der Post – betrieben wird. IncaMail stellt den einfachen und sicheren Versand von sensiblen Nachrichten und Dokumenten sicher. Für IncaMail gelten minimale Mitwirkungspflichten gemäss der Kategorie «Anbieter abgeleiteter Kommunikationsdienste» (AAKD). Mit den neuen Vorgaben für AAKD weitet der Bundesrat die Zahl der Firmen mit Mitwirkungspflichten bei der Überwachung klar aus und stellt an sie höhere Anforderungen bezüglich Datenüberwachung. Zudem deutet eine breite Auslegung der neuen Verordnungsbestimmungen darauf hin, dass neben Kommunikationsdiensten auch weitere Lösungen (bspw. Speicherlösungen) in den Geltungsbereich der Überwachung fallen könnten. Die Tragweite der Anwendung und die Definitionen, was für Dienste am Ende alles unter den Pflichtenkatalog (bspw. Vorratsdatenspeicherung, Öffnung von Verschlüsselungen etc.) fallen,

Datum 5. Mai 2025

Seite 2

ist unklar und unpräzise, wodurch eine Unsicherheit geschaffen wird. Auch ist unklar, was eine allfällige Unterstellung weiterer Dienste für Effekte in Sachen Anpassung anderer gesetzlicher Vorgaben hätte, beispielsweise im Zusammenhang mit Datenschutzfragen.

Aus unserer Sicht schwächen die Neuerungen unverhältnismässig den Technologiestandort Schweiz.

Wir bitten Sie um Berücksichtigung insbesondere folgender Punkte:

1. Heute gilt die höchste Stufe der Verpflichtungen für AAKD ab 5000 Nutzern. Neu ist, dass die Präzisierung «ein grosser Teil ihrer Geschäftstätigkeit im Anbieten abgeleiteter Kommunikationsdienste besteht» (Art. 52 VÜPF) wegfällt und nur noch der Gesamtumsatz der Unternehmung in der Schweiz massgebend ist. Für die Unternehmen gilt neu eine 6-monatige Aufbewahrungspflicht für Metadaten. Diese Regelung birgt die Gefahr, geltendem EU-Recht entgegenzulaufen. Zudem löst sie enorme Kosten bei den betroffenen Unternehmungen aus.
Durch die neu auf Unternehmensebene berechneten Schwellenwerte für Verpflichtungen, werden betroffene Unternehmungen in ihrer Innovationstätigkeit gehemmt, denn neu werden alle Dienste berücksichtigt und es werden allen Diensten Verpflichtungen auferlegt, sobald die Schwellenwerte erreicht sind. Dies stellt für eine Unternehmung ein Hindernis dar, neue Produkte zu lancieren.
2. Es wird eine neue Verpflichtungsebene für AAKD geschaffen, die bei Unternehmen mit 5'000 Nutzern beginnt und sie zur Vorratsdatenspeicherung verpflichtet (möglicherweise Identifizierung der Nutzer und Protokollierung der letzten IP der Verbindungen). Im Endefekt bedeutet dies eine umfassende Überwachung des gesamten Schweizer Internet-Sektors, was auch zu verstärkter Unsicherheit bei den Nutzenden führen kann. Die Verpflichtung zur Vorratsdatenspeicherung wird den ganzen Sektor international benachteiligen mit starken wirtschaftlichen Folgen.
3. Durch die Verpflichtung zur „automatischen“ Beantwortung bestimmter Anfragen entfallen die rechtliche Prüfung und das Recht der Unternehmen, möglicherweise rechtswidrige Massnahmen anzufechten.

Wir sind der Meinung, dass die vorgesehenen Regelungen über das eigentliche Ziel hinausgehen und dem Wirtschaftsstandort Schweiz schaden bzw. die Wettbewerbsfähigkeit der Schweizer Unternehmen in der Telekommunikationsbranche mindern. Die neuen Anforderungen lösen immensen technischen und finanziellen Aufwand bei den betroffenen Unternehmungen aus – ohne nachweisliche Verbesserung der strafrechtlichen Ermittlungen. Überdies schaden sie dem Vertrauen in eine sichere und vertrauliche digitale Kommunikation und somit am Ende dem Ziel der digitalen Transformation der Schweiz. In keinem anderen westlichen Land unterliegen private Kommunikationsanbieter ähnlich strengen Verpflichtungen – namentlich zur Vorratsdatenspeicherung für Überwachungszwecke oder zur technischen Öffnung von vertraulichen und gesicherten Systemen.

Datum 5. Mai 2025

Seite 3

Wir bedanken uns für Ihre Kenntnisnahme und bitten Sie, die Vorlage entsprechend unseren Bedenken anzupassen.

Freundliche Grüsse

Die Schweizerische Post AG

Post CH Digital Services AG

Matthias Dietrich
Co-Leiter Stab CEO

Tecla Solari
Mitglied der Geschäftsleitung
Verwaltungsratspräsidentin Tresorit



Malzgasse 18, 4052 Basel
Switzerland
www.hygiaso.ch

Dominik Geller
Geschäftsführer,
dominik@hygiaso.ch
+41794317822

Eidgenössisches Justiz- und
Polizeidepartement EJPD
ptss-aemterkonsultationen@isc-ejpd.admin.ch

5. Mai 2025

Vernehmlassung der Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Wir haben die vorgeschlagenen Teilrevisionen der VÜPF und VD-ÜPF zur Kenntnis genommen. Wir anerkennen die Ziele der Revisionen, beanstanden aber spezifische Aspekte, welche negative Auswirkungen haben werden.

Unsere Beurteilung reflektiert die Sicht eines Startups im Gesundheitsdatenbereich, dass den Bürgern den Zugang zu Ihren eigenen Gesundheitsdaten und deren selbst-bestimmte weitere Teilung mit Vertrauenspersonen ermöglicht, einschliesslich einer Ende-zu-Ende verschlüsselten Übertragung ihrer persönlichen Gesundheitsdaten mit ihrem Smartphone. Wir ermöglichen es den Bürgern Ihre persönlichen Daten mittels Auskunftsbegehren zu sammeln. Hierzu muss sich der Nutzer beim Gesundheitsdienstleister mit digitalem Ausweis legitimieren. Wir als AAKD kennen aber per dezentralem und datensparsamen Design weder unsere Nutzer, noch deren Daten, und der Nutzer braucht in der Konsequenz auch kein Nutzerkonto.

1. Zu breite Definition der AAKD

Die Definition der AAKD ist extrem weit gefasst, so dass jede nicht öffentliche Datenübermittlung unabhängig von Bereich und Kontext erfasst wird. Die Schutzziele der Überwachung bedingen aber nicht eine allumfassende Überwachung jeglicher digitaler Prozessinteroperabilität und aller Anwendungsbereiche, sondern müssen in geeigneter Weise eingeschränkt werden im Einklang mit dem Datenschutzgesetz und der gebotenen Datensparsamkeit. Es darf nicht sein, dass jedes digitale Dienstleistungsangebot in Zukunft die Identifikation deren Nutzer verlangt.

2. Datenschutzfolgeabschätzung: Unnötige Vorratsdatenspeicherung

Wir teilen Ihre Datenschutzfolgeabschätzung nicht. Die Pflicht zur Identifizierung der Nutzer eines AAKD mit reduzierten Pflichten ab 5000 monatlichen Nutzern unabhängig der Anwendung und Art der Daten führt – wohl nicht bei den Behörden, aber bei den AAKD – zu einer weitreichenden Vorratsdatenhaltung von Nutzungsdaten und Interaktionsprofilen einer Vielzahl von Bürgern in allen Bereichen, ohne dass hierfür ein verhältnismässiges Schutzziel geboten ist.

3. Pflicht, die im Datenschutzgesetz geforderte Datensparsamkeit proaktiv zu verletzen

In unserem Fall wären wir gezwungen mit Erreichen des Schwellwertes unsere Applikation zweckfremd abzuändern und einzig für die gesetzlich verlangten Überwachungsziele eine Nutzeridentifikation und Tracking einzuführen. Dies ist in umliegenden Ländern und international

nicht gegeben und würde zu einem wesentlichen Standortnachteil führen und wäre eine zusätzliche Adoptionshürde für potentielle Nutzer.

4. Aktive Unterstützungsmassnahmen nur für AAKD mit reduzierten Pflichten, die eine hinreichende Grösse und Reife haben

Digitale Business Cases bedingen typischerweise eine kritische Masse, die oft über 5000 Nutzern liegt. Zusätzliche Auflagen vor Erreichen einer kritischen Masse sind unbedingt zu vermeiden. Die Belastung mit zusätzlichen Pflichten riskiert die Innovationsfähigkeit und Finanzierbarkeit der KMU und Startups im unnötig weit gefassten AAKD Bereich abzuwürgen und nur noch grössere Unternehmen könnten sich den geforderten Überwachungsaufwand leisten.

5. Legitimer Schutz der Privatsphäre wird verunmöglicht

Neben unserem eigenen Anwendungsfall gibt es eine Reihe weiterer Beispiele, in denen die anonyme digitale Kommunikation und/oder die Kommunikation ohne dass der Übermittler die involvierten Parteien identifiziert und erfasst durchaus sinnvoll gerechtfertigt ist. Hierzu zählen beispielsweise die durch Amtsgeheimnis oder Berufsgeheimnis geschützte Kommunikation (z.B. Mandantenkommunikation von Anwälten). Compliance Hotlines, Eingangskanäle für investigative Medien oder digitale Hilfsangebote für Minoritäten oder vulnerable Gruppen. Man stelle sich nur einmal vor, ein digitales Beratungsangebot für Patienten (z.B. übertragbare Krankheiten) würde zwingend die Identifikation der Nutzer durch den AAKD verlangen. Niederschwellige Angebote könnten in der Schweiz nicht mehr angeboten werden, bzw. auf Übermittlungsdienstleistungen müsste verzichtet werden oder die digitale Kommunikation mit Nutzern von jedem einzelnen Anbieter in ineffizienter Eigenleistung umgesetzt werden. Dies würde die Digitalisierung in der Schweiz behindern.

6. Empfehlungen

Wir empfehlen deshalb geeignete Änderungen zu prüfen:

- Verzicht auf eine Nutzeridentifikation, wenn solche für die erbrachte Dienstleistung nicht notwendig ist oder nicht durch existierende spezifische Sorgfaltspflichten (z.B. im Bereich Geldwäscherei) gefordert ist. Gegebenenfalls wäre eine Geräteidentifikation in gebotenen Fällen ein hinreichendes Instrument.
- Es wäre zu prüfen, welche Massnahmen für AAKD mit reduzierten Pflichten nicht zwingend wären und ob auf Massnahmen, welche nicht durch den Applikationszweck selbst gefordert werden zu verzichten.
- Die Auflagen für AAKD mit reduzierten Pflichten sind auf juristische Personen zu beschränken, welche nachhaltig wirtschaftliche Position erreicht haben und die geforderten Pflichten auch schultern können, ansonsten ihnen dadurch das wirtschaftliche Aus droht. KMU und Startups müssen hier vor zweckfremden Aufwänden geschützt werden und ein Schwellwert eingeführt werden, der die Unternehmensgrösse und deren Reifegrad berücksichtigt.

Mit freundlichen Grüßen

Dominik Geller



Eidgenössisches Justiz- und Polizeidepartement
Bundeshaus West
3003 Bern

Ausschliesslich per E-Mail an:
ptss-aemterkonsultationen@isc-ejp.admin.ch

SIX Group AG
Pfingstweidstrasse 110
CH-8005 Zürich

Postanschrift:
Postfach
CH-8021 Zürich

T +41 58 399 34 60
www.six-group.com

Kontaktperson:
Urs Reich
urs.reich@six-group.com

Zürich, 5. Mai 2025

Stellungnahme zur Vernehmlassung über die Teilrevisionen zweier Ausführungsverlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die am 29. Januar 2025 eröffnete Vernehmlassung über zwei Ausführungsverlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF). Als Betreiberin der Schweizer Börse und weiterer Finanzmarktinfrastrukturen ist SIX sehr an Rahmenbedingungen gelegen, die die Schweiz für Firmen in innovativen Branchen und Sektoren attraktiv machen. Dies sehen wir durch die vorliegenden Teilrevisionen der Ausführungsverlasse stark bedroht. Gerne nehmen wir die daher die Gelegenheit wahr und unterbreiten Ihnen nachfolgend unsere Stellungnahme.

In Kürze

- **Wir lehnen die Vorlagen entschieden ab, da sie die Attraktivität der Schweiz als Standort für innovative Unternehmen des Technologiesektors gegenüber dem angrenzenden Ausland deutlich verschlechtern.**
 - Dies bedroht die Wettbewerbsfähigkeit der direkt betroffenen Unternehmen erheblich. Im Falle einer Umsetzung der Entwürfe ist anzunehmen, dass etliche bereits in der Schweiz ansässige Unternehmen ihren Sitz ins Ausland verlagern könnten und im Ausland ansässige Unternehmen auf einen Zuzug in die Schweiz verzichten.
 - Der Schaden reicht weit über die direkt betroffenen Unternehmen hinaus, da die Schweiz damit für Unternehmen in innovativen Sektoren insgesamt negative Signale aussendet. Während andere Standorte wie die EU derzeit stark darauf fokussieren, die Rahmenbedingungen und damit ihre Wettbewerbsfähigkeit und Standortattraktivität zu verbessern, würde die Schweiz diese bei einer Umsetzung der Vorlagen mutwillig gefährden und somit die Entwicklung des Wirtschaftsstandorts und des Kapitalmarkts schädigen.
- **Wir bitten Sie daher, die Vorlage insbesondere hinsichtlich des Mandats zur Speicherung von Randdaten grundlegend und unter Einbezug der betroffenen Branche zu überarbeiten.**

1. Grosse gesamtwirtschaftliche Bedeutung der Vorlagen

Wir werden im Moment Zeuge der Entstehung einer neuen und eigenständigen Kategorie globaler Technologiedienstleistungen zur Bereitstellung von sicheren und datenschutzorientierten Kommunikationsdiensten. Diese Branche spielt eine entscheidende Rolle in der heutigen digitalen Welt, in der Datenschutz und -sicherheit immer wichtiger werden. Europa und insbesondere die Schweiz haben dank der Tradition liberaler Werte und der Achtung der Privatsphäre beste Voraussetzungen als Standort für die Entwicklung dieser neuen Dienste.

Deren Bedeutung für die wirtschaftliche Entwicklung reicht weit über den Sektor hinaus, da diese Kommunikationsdienste das Potenzial haben, die zukünftige digitale Landschaft neu zu definieren. Eine erfolgreiche Etablierung Europas und der Schweiz als Standort für zukunftsträchtige Technologien ist unerlässlich, um den bestehenden Rückstand gegenüber anderen Technologiestandorten wie den USA oder asiatischen Staaten wettzumachen.

Der Wettbewerb spielt sich jedoch nicht nur zwischen Europa und Staaten außerhalb ab, sondern auch innerhalb Europas. Es ist davon auszugehen, dass sich dieser in nächster Zeit weiter intensivieren wird. Angesichts der jüngsten geopolitischen Entwicklungen legt die Europäische Union ihren Fokus auf die Stärkung der Wettbewerbsfähigkeit als Wirtschafts- und Technologiestandort. Indem die Schweiz ihre inhärenten Stärken – innovationsfreundliche Rahmenbedingungen, etablierte liberale Prinzipien und ein führendes Finanzzentrum – nutzt, kann sie innerhalb Europas eine Vorreiterrolle übernehmen und bedeutendes Wirtschaftswachstum generieren.

Um diese gute Ausgangslage nachhaltig zu nutzen, gilt es, die Rahmenbedingungen zu wahren bzw. wo nötig und möglich weiter zu stärken und gleichzeitig wirtschaftliche Interessen, die Wahrung von Grundwerten und Maßnahmen zur Durchsetzung öffentlicher Interessen (im vorliegenden Fall die öffentliche Sicherheit) sorgfältig auszutarieren. Diese Interessensabwägung ist mit den Vernehmlassungsvorlagen nicht gelungen, sondern einseitig zugunsten sicherheitspolitischer Überlegungen ausgefallen. Die beiden Verordnungen bedürfen daher einer grundlegenden Überarbeitung.

2. Überarbeitungsbedarf infolge Gefährdung der Wettbewerbsfähigkeit

Seitens der betroffenen Branche und der Wirtschaft bestehen erhebliche Bedenken hinsichtlich spezifischer Bestimmungen – hauptsächlich die Verpflichtung zur breiten Speicherung von Randdaten.

Die Ausweitung der Überwachung und die damit verbundenen übermäßigen Mitwirkungspflichten gehen weit über die Ansätze in Jurisdiktionen wie der EU und den USA hinaus. Diese auferlegen den betroffenen Anbietern keine vergleichbaren pauschalen Verpflichtungen. Diese Abweichung setzt Schweizer Unternehmen einem erheblichen Wettbewerbsnachteil aus. Dieser wirkt sich auf zwei wesentlichen Ebenen aus:

- Erstens verursachen umfangreiche Speicheranforderungen erhebliche administrative und finanzielle Belastungen, die die Agilität und das Wachstum – insbesondere von KMUs, Start-ups und Scale-ups, die für das Innovationsökosystem der Schweiz von entscheidender Bedeutung sind – unverhältnismäßig behindern, indem sie kritische Ressourcen binden.

- Zweitens kann die obligatorische breite Speicherung bei Unternehmen, die auf Nutzervertrauen und Datenminimierung aufbauen, die „Core Value Proposition“ gegenüber ihren Kundinnen und Kunden grundlegend untergraben.

Die berechtigten Interessen der betroffenen Unternehmen sowie von deren Kundinnen und Kunden wurden demnach nur ungenügend berücksichtigt. Es ist zu erwarten, dass betroffene Unternehmen aus der Schweiz wegziehen oder Pläne für einen Zuzug in die Schweiz auf Eis legen, um die aus einer Umsetzung der Vernehmlassungsvorlagen resultierenden Wettbewerbsnachteile zu vermeiden. Da die Schweiz bereits heute namhafte Anbieter beheimatet, handelt es sich hierbei nicht um ein theoretisches Szenario, sondern um eine reale Gefahr. Auch Forschung und Entwicklung sowie Gründung neuer Unternehmen in direkt betroffenen und angrenzenden Branchen würden negativ beeinflusst.

3. Festhalten schwächt Sicherheit anstatt sie zu stärken

Das Argument, die Anpassungen seien notwendig, um die öffentliche Sicherheit zu stärken, mag nicht zu überzeugen. Durch die Verlagerung der Geschäftsaktivitäten ins Ausland bzw. einen Verzicht auf die Ansiedelung in der Schweiz entziehen sich diese Aktivitäten dem Einflussbereich der Schweizer Behörden. Damit wird die Sicherheit geschwächt anstatt wie angestrebt gestärkt.

Indem alle Anbieter verpflichtet werden, den Behörden jederzeit einen Zugang zu den gespeicherten Metadaten zu gewähren, entstehen zudem enorme Sicherheitsrisiken, die ein Einfallstor für Hackerangriffe, Datenmissbrauch und Spionage schaffen. Nach Einschätzung unserer Experten für Cyber Security macht die Verpflichtung zur Sammlung von Randdaten Schweizer Unternehmen zu lukrativen Zielen krimineller Akteure.

Werden die Verordnungen umgesetzt wie vorgeschlagen, entstehen neue Risiken, die keineswegs im Interesse des Datenschutzes und des Schutzes der verfassungsmäßigen Grundrechte sind. Zu den Grundprinzipien von Datenschutz und -sicherheit gehört auch das Prinzip der Datenminimierung. Dieses zentrale Prinzip sehen wir mit der starken Ausweitung der Pflichten als besonders verletzt.

Eine Anpassung, welche allen berechtigten Anliegen bestmöglich Rechnung trägt, ist damit auch im Interesse der Sicherheitsorgane in der Schweiz.

Schlussfolgerung

Die vorgeschlagenen Verordnungsanpassungen gefährden die Schaffung eines innovativen und hochkompetitiven Wirtschaftsclusters im Bereich der sicheren und datenschutzorientierten Kommunikationsdienste und schädigen damit letztendlich die Wirtschaftsentwicklung insgesamt, da die Schweiz die Positionierung als Standort innovativer und neuer Geschäftsmodelle verpasst. Die Effekte werden somit in der Gesamtwirtschaft und auch dem Finanzplatz spürbar sein. Aus Sicht der SIX bzw. der Schweizer Börse ist beispielsweise zu befürchten, dass Kotierungen von Unternehmen mit internationaler Strahlkraft verpasst werden. Neben den direkten Auswirkungen der nicht realisierten Börsenkotierung in der Schweiz sind insbesondere auch die indirekten Effekte wie



Verunmöglichung der Schaffung eines Technologie-Clusters von internationalem Rang bedeutsam. Gleichzeitig werden die Sicherheitsinteressen der Schweiz wie geschildert ebenfalls geschwächt.

Abschliessend ist festzuhalten, dass eine dermaßen breit angelegte Ausweitung von Pflichten auf Verordnungsstufe nicht haltbar ist und unseres Erachtens über die Bestrebungen des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) hinausgeht. Angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre sind die Massnahmen auf Ebene des Gesetzes und nicht durch eine reine Verordnung zu implementieren. Solch einschneidende Änderungen sind – wenn überhaupt – auf Gesetzesebene zu erlassen.

Wir bitten Sie daher, die Verordnungen nochmals grundlegend zu überarbeiten und dabei insbesondere im Bereich der ausgeweiteten Mitwirkungspflichten die Anliegen der betroffenen Unternehmen zu berücksichtigen. Wir sind der festen Überzeugung, dass eine schlankere Regulierung mit weniger erfassten Unternehmen und risikobasierten Pflichten mindestens vergleichbaren Nutzen für die Strafvollzugsbehörden bringt, allerdings ohne einen wirtschaftlichen Kollateralschaden. Für Details verweisen wir dazu auf die Stellungnahmen von economiesuisse, Digitalswitzerland und insbesondere Swico, welche wir volumnfänglich unterstützen. Wir bitten Sie zudem, die Hauptbetroffenen Wirtschaftsakteure bei der Überarbeitung eng in die Arbeiten miteinzubeziehen.

Wir danken Ihnen für die Kenntnisnahme unserer Stellungnahme und die Berücksichtigung unserer Überlegungen. Gerne stehen wir Ihnen für ergänzende Auskünfte zur Verfügung.

Freundliche Grüsse

DocuSigned by:

Urs Reich

9B21DA9B28374A9...

Urs Reich
Head Public Affairs & Market Structure

DocuSigned by:

Simon Pabst

0202F4A900A24BF...

Simon Pabst
Senior Specialist Market Structure

*Vernehmlassungsantwort zu den Teilrevisionen der VÜPF und der VD-ÜPF
gemäss Schreiben des EJPD vom 29. Januar 2025*

Datum	02. Mai 2025
Verfasser (Unternehmen)	NTS Workspace AG
Kontaktperson bei Fragen (Name/Tel./E-Mail)	Niklaus Hug / 031 517 77 01 / nh@nts.ch

Dieses Dokument geht an:

Eidgenössisches Justiz- und Polizeidepartement EJPD, ptss-aemterkonsultationen@isc-ejpd.admin.ch

Sehr geehrter Herr Bundesrat Jans, sehr geehrte Damen und Herren

Wir beziehen uns auf das am 29. Januar 2025 eröffnete Vernehmlassungsverfahren zu Teilrevisionen von VÜPF und VD-ÜPF und bedanken uns für die Möglichkeit einer Stellungnahme.

Wir lehnen die geplante Teilrevisionen der VÜPF und der VD-ÜPF in aller Deutlichkeit und vollumfänglich ab.

Im Bericht des Bundesrates zur aktuellen Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF und der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) ist zu lesen, dass die Revision im Wesentlichen auf die Anpassung der Verordnungen an die KMU-Freundlichkeit abziele. Ein grosser Teil der vorgeschlagenen Änderungen verfolgt aber gerade das Gegenteil.

Die Geschäftsgrundlagen von Schweizer Unternehmen wie Threema, Proton und anderer KMU, die weltweit einen hervorragenden Ruf als Anbieterinnen sicherer Kommunikationsdienste im Internet geniessen, drohen durch die Vorlage zerstört zu werden. Die Sicherheit des Internets in der Schweiz soll mit der Revision der Überwachung jeglichen Internetverkehrs regelrecht untergeordnet werden: «**Sicherheit vor Freiheit**» ist das neue Paradigma. Dieses zieht sich wie ein roter Faden quer durch diese völlig verunglückte Reform. KMU, die aus der Schweiz heraus Internet-Dienste anbieten («abgeleitete Kommunikationsdienste» in der Terminologie des Gesetzes), soll die Schweiz als Standort geradezu vergällt werden. Dies scheint denn auch zu gelingen: **Erste der betroffenen Unternehmen haben bereits angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen** (siehe Tages-Anzeiger vom 1. April 2025).

Ein derartiger Paradigmenwechsel, weg von KMU-Schutz und Überwachung mit Augenmass, hin zu knallharter Überwachung, die alle anderen Interessen unterordnet, wird durch das geltende Gesetz (BÜPF) keineswegs gestützt. Der Paradigmenwechsel widerspricht vielmehr geradezu dem Geist des ursprünglichen BÜPF, das Internetdienste, die in der Schweiz meist von KMU betrieben werden, gerade von der Implementierung teurer Überwachungsmassnahmen schützen wollte, und das eine austarierte Interessenabwägung vorsah zwischen Privatsphäre und Freiheit auf der einen Seite und staatlicher Überwachung auf der anderen Seite.

Entgegen dem im Begleitbericht zum vorgelegten Entwurf erklärten Ziel, die «finanzielle Belastung der KMU gering zu halten», stuft die Vorlage eine grosse Mehrheit der Schweizer Anbieterinnen von Internetdiensten in eine höhere Stufe auf, und zwingt sie neu auch in jenen Bereichen zu einer kostspieligen aktiven Überwachungstätigkeit, wo bisher nur eine KMU-freundliche Duldungspflicht bestand. Dies verschiebt das bisherige Gleichgewicht der Interessen zwischen Strafverfolgung und betroffenen Anbieterinnen in drastischer Weise zulasten der betroffenen Anbieterinnen.

Die vorgeschlagenen Anpassungen bringen ganz erhebliche Risiken für den Innovations- und Wirtschaftsstandort Schweiz mit sich und erfüllen die Kernziele der Revision, die Entlastung von KMU, gerade nicht. Der Ruf der Schweiz als sicherer Hafen für vertrauenswürdige IT-Anbieter droht durch die Revision nachhaltig beschädigt zu werden. Deshalb lehnen wir die Revision vollumfänglich ab.

Auch die **Schweizer Armee** nutzt solche Dienste, wie beispielsweise Threema, und zwar gerade aufgrund des hohen gebotenen Sicherheitsstandards. Die Annahme dieser Revision, welche dieses Sicherheitsniveau gezielt untergraben will, verletzt damit indirekt auch das direkte Interesse der Schweiz an lokal betriebenen Hochsicherheitsanwendungen. Gerade in der heutigen Zeit, in der die Zuverlässigkeit der grossen US-Anbieter in ihrer Abhängigkeit von einer zunehmend erratisch agierenden US-Regierung mehr und mehr in Frage steht, erscheint dies als **inakzeptable Hochrisikostrategie**.

Nicht zuletzt ist mit Nachdruck darauf hinzuweisen, dass die Revision die Überwachung ganz allgemein stark ausweitet. Dies ist mit der durch den Gesetzgeber im BÜPF festgelegten, fein austarierten Interessenabwägung zwischen Freiheit und Privatsphäre der Einwohner der Schweiz einerseits und Sicherheit durch Überwachungsmassnahmen andererseits absolut nicht vereinbar. Die Revision entpuppt sich geradezu als eine Art Wunschkonzert für Überwachungsbehörden. Insbesondere ist künftig auch **eine komplette inhaltliche Überwachung des gesamten Internetverkehrs** der Schweiz vorgesehen. Dies ohne dass eine solche inhaltliche Überwachung durch die gesetzlichen Grundlagen des BÜPF in irgend einer Weise gedeckt wäre: Zulässig ist gemäss BÜPF einzig und allein die Überwachung von Randdaten des Fernmeldeverkehrs, und selbst die Zulässigkeit der in diesem Kontext angewendeten anlasslosen Vorratsdatenspeicherung von Randdaten ist bis heute umstritten und Gegenstand von Gerichtsverfahren, ja in der EU bereits höchstrichterlich als menschenrechtswidrig erkannt. Die durch die Verordnungsrevision eingeführte *Inhaltsüberwachung* ist in der Schweiz damit erst recht **offensichtlich illegal und verfassungswidrig**.

Abschliessend sei noch der Hinweis angebracht, dass wir die Gesetzgebungstechnik des Entwurfs für überaus schlecht halten. **Sowohl der Verordnungstext als auch der zugehörige erläuternde Bericht sind über weite Strecken höchst verwirrend und unverständlich formuliert**, unter anderem mit einer Vielzahl von Querverweisen, technischen Fehlern und unklarer Begrifflichkeit (für ein Beispiel hierfür siehe unten, Bemerkungen zu Art. 43a). Die Texte sind in dieser Form selbst für Fachleute über weite Strecken nicht zu verstehen, geschweige denn als Ganzes zu überblicken. Für KMU, die durch die Revision neu mit erheblich strenger Pflichten konfrontiert werden, ist eine rechtskonforme Umsetzung dieser Vorlage daher ein schlicht aussichtloses Unterfangen.

Das Legalitätsprinzip gemäss Art. 5 Bundesverfassung fordert vom Gesetzgeber, dass Gesetzestexte für die Adressaten verständlich formuliert sind. Die Texte der Verordnungsrevision genügen dieser Anforderung offensichtlich in keiner Weise. Nur schon aufgrund der völlig fehlenden Verständlichkeit ist die Verfassungsmässigkeit der Revision insgesamt *höchst zweifelhaft*. Wir fordern nur schon deshalb einen Rückzug der vorgelegten Texte, eine komplette Überarbeitung zur Verbesserung der Verständlichkeit und eine erneute Auflage zur Vernehmlassung.

Mit freundlichen Grüissen



NTS Workspace AG
Niklaus Hug

Bemerkungen zu einzelnen Artikeln der VÜPF

Nr.	Artikel	Antrag	Begründung / Bemerkung
VÜPF / OSCPT / OSCPT			
0.	Alle Artikel	Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.	<p>Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kunden auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.</p> <p>Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.dgl. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.</p>
1.	16b, Abs. 1	Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.»	Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile, wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Anforderungen in Kauf nehmen.
2.	16c, Abs. 3	Streichung von lit. a «automatisierte Erteilung der Auskünfte (Art. 18 Abs. 2);»	Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Dies untergräbt rechtsstaatliche Prinzipien doppelt: Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>«natürliche» Schutzmechanismen gegen eine überschiessende, missbräuchliche oder zumindest unverhältnismässige Nutzung solcher Massnahmen durch die Untersuchungsbehörden.</p> <p>Der vorgesehene Umsetzungszeitraum von 12 Monaten für die rechtssichere Implementierung eines derart komplexen Systems ist völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.</p>
3.	Art. 16d	<p>Streichung von Onlinespeicherdiensten und VPN-Anbietern in der Auslegung</p>	<p>Eine klarere Definition des Begriffs AAKD ist begrüssenswert, doch die neue Auslegung gemäss erläuterndem Bericht geht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdiensten wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter, etc.) genutzt werden.</p> <p>Art. 2 lit. c BüPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug den gesetzlichen Rahmen sprengt. Onlinespeicherdienste sind deshalb aus Art. 16d zu streichen.</p> <p>Zudem anerkennt der erläuternde Bericht, dass VPNs zur Anonymisierung der Nutzer*innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Anbieter von VPNs sind daher ebenfalls aus dem Geltungsbereich von Art. 16d auszunehmen.</p>
4.	Art. 16e, Art. 16f und Art. 16g	<p>Streichung der Artikel und Beibehaltung der bestehenden Kriterien</p> <p>Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).</p>	<p>Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch diametral entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung. Dies daher, weil neu KMU bereits mit mehr als 5'000 Nutzern erfasst werden.</p> <p>Die Einführung von 5000 Nutzern als gesondert zu beurteilende Untergrenze verletzt aus unserer Sicht bereits Art. 27 Abs. 3 BüPF, denn 5000 Personen keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strengereren Überwachungsmassnahmen, gerechtfertigt wären. 5000 Nutzer werden in der digitalen Welt vielmehr sehr rasch erreicht.</p> <p>Zusätzlich führt das Einführen eines «Konzerntatbestandes» in Art. 16f Abs. 3 zu massiven Problemen, da</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>die Produkte nun nicht mehr für sich alleine eine bestimmte Grösse erreichen müssen, sondern die relevanten Zahlen anhand des Umsatzes des Unternehmens, bzw. in Konzernverhältnissen sogar des Konzerns bestimmt werden. Vor allem bei Unternehmen mit Beteiligungsfirmen im Hintergrund fallen nun neu alle Dienstleistungen und Produkte automatisch unter die härteste Stufe, egal ob sie sich erst in einem frühen Entwicklungsstadium befinden. Dies behindert Innovation, da jedes Projekt bereits mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden müsste. Durch diese extreme Einstiegshürde wird der Innovationsstandort Schweiz nachhaltig geschädigt.</p> <p>Gleichzeitig wird auch der Wirkungsbereich der VÜPF stark erweitert. Während heute ein Unternehmen einen grossen Teil seiner Geschäftstätigkeit durch abgeleitete Kommunikationsdienste erbringen muss (Art. 22 Abs. 1 lit. b und Art. 52 Abs. 1 lit. b VÜPF), fällt dieses Kriterium neu weg. Dadurch können künftig auch Unternehmen, deren Geschäftstätigkeit nur am Rande auf abgeleiteten Kommunikationsdiensten basiert, wie Onlineshops, Marktplätze, Auktionsplattformen, Zeitungen, Computerspielhersteller und zahlreiche weitere Unternehmen, unter die VÜPF fallen – allein deshalb, weil ihre Produkte irgendeine Form privater Kommunikation zwischen Nutzer*innen und/oder Drittanbietern ermöglichen.</p> <p>Die vorgeschlagene Regelung stünde sodann im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali, das die zu weite Betroffenheit und die seltene Anwendung von Downgrades kritisierte: «Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»</p> <p>Statt KMU zu entlasten, führt die Revision neu sogar zu einer «automatischen Hochstufung per Verordnung ohne konkretisierende Verfügung (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.</p> <p>Die neue Regelung steht zudem in offensichtlichem Widerspruch zur bisherigen Praxis, denn bis heute wurde gemäss Angaben des Dienst ÜPF keine einzige AAKD hochgestuft. Auch der Bundesrat stützte sich ausdrücklich auf die geltende Kombination von drei Schranken – einem Unternehmensfokus auf Kommunikationsdienste, einer Umsatzgrenze von 100 Millionen Franken sowie einer grossen Nutzerzahl – als er noch 2023 begründete, die Umsetzung des BÜPF sei gerade wegen der genannten Schranken als KMU-freundlich zu verstehen. Die vorliegende Revision hebt jedoch genau diese Kombination kumulativer Kriterien auf und will die einzelnen Kriterien künftig alternativ anwenden bzw. streicht sie sogar vollständig. Dadurch verlieren die bisherigen Schutzmechanismen ihre Wirkung, und das BÜPF soll neu auf viele KMU Anwendung finden, die früher nicht unter Gesetz und Verordnung fielen.</p> <p>Die Analyse der offiziellen Statistik des Dienstes ÜPF macht die offensichtliche Unverhältnismässigkeit</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>dieses Ansinnens deutlich. Im Jahr 2023 betrafen 98,95 % der total 9'430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,05 % für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,73 % wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100 % des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.</p> <p>Wesentlich ist insbesondere eine neue Pflicht zur Identifikation der Nutzer: Hiervon betroffen sind nicht nur alle AAKD mit reduzierten oder vollen Pflichten (und damit de facto fast alle AAKD der Schweiz), sondern auch all deren Wiederverkäufer. Im Ergebnis führt die neue Verordnung aus unserer Sicht dazu, dass man sich bei keinem marktrelevanten Dienst mehr anmelden kann, ohne den Pass, Führerschein oder ID zu hinterlegen oder zumindest Daten wie eine Telefonnummer anzugeben, die man ohne Pass oder ID nicht erhalten kann.</p> <p>Die automatische Hochstufung an sich führt bereits zu erheblicher Rechtsunsicherheit bei den betroffenen Unternehmen. Unter dem bestehenden System werden die generell-abstrakten Normen der VÜPF mittels Verfügung auf einen konkreten Einzelfall angewendet. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes ist aber im Zweifelsfall möglicherweise nur schwer zu beantworten. Zweifelsohne besteht hier ein schutzwürdiges Interesse seitens der AAKD daran, zu wissen, ob sie die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Nur das bisherige System entspricht den allgemeinen Grundsätzen des Verwaltungsverfahrens, welches für die Anwendung einer generell-abstrakten Norm eine Konkretisierung durch die Verwaltung voraussetzt. Von einer automatischen Hochstufung von AAKD ist daher aus Gründen der Rechtssicherheit abzusehen. Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.</p> <p>Gegenüber der alten VÜPF erweitert die Revision die Pflichten zur Automatisierung sodann noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragen wie z.B. IR_59 und IR_60, welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen. Genau diese Möglichkeit einer manuellen Intervention ist aber für die Provider kritisch, um Missbräuche zu verhindern, die wiederum die Verträge mit ihren Kunden und das Fernmeldegeheimnis verletzen könnten. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente damit erheblich, und damit auch das Risiko für die Grundrechte</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.</p> <p>Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 Bst. b der alten VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grosse[n] Teil ihrer Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. Damit fallen insbesondere bereits Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz. Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Dies setzt der Innovation in der Schweiz neue riesige Hürden entgegen.</p> <p>Auch Non-Profit-Organisationen wie die Signal Foundation, die kaum Umsätze erwirtschaften, geraten unter diese verschärften Vorgaben. Während sie bisher unter Duldungspflichten verbleiben konnten, so lange sie Art. 22 Abs. 1 VÜPF nicht erfüllten, wird neu allein auf die Anzahl der Nutzer*innen abgestellt, womit z.B. Signal neu als AAKD mit vollen Pflichten erfasst würde. Dies würde dazu führen, dass Signal in der Schweiz entweder zu einem Rückzug aus dem Markt gezwungen wird oder erhebliche rechtliche Konsequenzen riskiert, da Signal keine IP-Adressen speichert und somit gegen Art. 19 RevVÜPF verstösst.</p> <p>Die Regelung ignoriert zudem wirtschaftliche Realitäten: Ein hoher Nutzerkreis bedeutet bei Non-Profits keine finanzielle Tragfähigkeit für umfangreiche Überwachungsmassnahmen. Damit werden Open-Source- und Non-Profit-Lösungen gezielt aus dem Markt gedrängt, während bestehende Monopole wie WhatsApp (96 % Marktanteil in der Schweiz) gestärkt werden. Die neue Regelung ist daher aus ökonomischer Sicht zu verwerfen. Das Kriterium der reinen Nutzerzahl ist ungeeignet und muss gestrichen werden.</p> <p>Nicht zuletzt schwächt die Regelung auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger*innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, Ende-zu-Ende-verschlüsselter Kommunikation ist heute wichtiger denn je.</p> <p>Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade als rechtswidrig gilt (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer*innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, sondern allein diese</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Anhäufung an Daten malt eine Zielscheibe auf den Rücken von Schweizer Unternehmen und Dienstleistungen für Hackerangriffe aus der ganzen Welt.</p> <p>Weiter ist zu erwähnen, dass es gar nicht erwiesen ist, dass die Speicherung der fraglichen Daten eine merklich höhere Quote erfolgreicher Ermittlungen durch die Strafverfolgungsbehörden mit sich bringen würde. Im Gegenteil müssen die bereits existierenden Sekundärdaten, die allein durch die Bereitstellung eines Dienstes für den Nutzer entstehen, besser genutzt werden. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisshandlung via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfügt, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden. Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren.</p> <p>Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Souveränität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.</p> <p>Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das Datenschutzgesetz. Der Entwurf bringt nicht, wie der Begleitbericht dem Leser in geradezu in Orwell'scher Manier weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit und steht in direktem Gegensatz zum besagten Postulat 19.4031.</p> <p>Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen, und das bestehende System muss beibehalten werden.</p>
5.	Art. 16h Abs. 2	Streichung der Ausführung im erläuternden Bericht und ein Abstellen der Formulierung auf die	Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Nutzer*innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare

Nr.	Artikel	Antrag	Begründung / Bemerkung
		gleichzeitige Anzahl Nutzer.	<p>Risiken für die FDA in Kombination mit Art. 19 Abs. 2 Rev.VÜPF, gemäss dem die das WLAN erschliessenden FDA die Verantwortung für die Identifikation der Nutzer der WLANs tragen.</p> <p>Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer*innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24) oder die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22). Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDAs unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden. Unter der bestehenden Regelung konnte eine FDA anhand der Lokation (z.B. Bibliothek, Flughafen) eine Einschätzung treffen. Die neue Definition hingegen würde von ihr verlangen, Zugriff auf jedes private Netzwerk zu erhalten, um Hardware und Einstellungen zu prüfen – ein offensichtlich verfassungswidriges und auch praktisch unmögliches Unterfangen. Diese vage Formulierung führt zu anhaltender Rechtsunsicherheit für FDA.</p> <p>Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten.</p> <p>Zudem könnte Art. 16h dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist*innen, Whistleblower*innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer*innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen. Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt.</p>
	Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2	Streichung des «Konzernatbestand» und Beibehaltung der bestehenden Regelung	<p>Die Verordnung nimmt neu nicht mehr die Umsatz- und Nutzerzahlen der betroffenen Unternehmen, sondern die Zahlen des jeweiligen Konzerns als Basis für Up- und Downgrades. Die Begründung zur Einführung dieses «Konzernatbestands», wonach die neue Regelung für die betroffenen Unternehmen zu einer Vereinfachung führe, ist kontraintuitiv, ja offensichtlich falsch und irreführend. In der Praxis sind die betroffenen Unternehmen nämlich schon heute verpflichtet, ihre Buchhaltung nach Produkten aufzugliedern. Somit können die Kennzahlen bereits heute sehr einfach festgestellt werden. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.</p>
6.	Art. 19 Abs. 1	Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber	<p>Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vor sieht.</p> <p>Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des Schweizer Daten-</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
		OHNE Einführung einer Pflicht zur Identifikation von Teilnehmenden.	<p>schutzgesetzes, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch der Schutz der Schweizer Kundschaft massiv beeinträchtigt wird. Datenschutzfreundliche Unternehmen werden bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.</p> <p>Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Dies wahrt nicht nur den Datenschutz, sondern schützt auch die Wettbewerbsfähigkeit von KMU, stärkt den Innovationsstandort Schweiz und die digitale Souveränität unseres Landes.</p>
7.	Art. 18	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.
8.	Art. 19 Abs. 2	Ersatzlose Streichung zugunsten bestehender Regelung	Eine Überwachung von Kunden durch FDA, ob diese die neuen Vorgaben der VÜPF zu WLANs einhalten (Art. 19 Abs. 2 Rev.VÜPF), und erst recht die dazu gelieferte Erklärung im erläuternden Bericht, wonach die FDA die Identifikation der WLAN-Nutzer vorzunehmen hätten, ist weder gesetzeskonform noch zumutbar (siehe vorstehend). Art. 19 Abs. 2 ist ersatzlos zu streichen.
9.	Art. 21 Abs. 1 lit. a	Streichung	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.
10.	Art. 22	beibehalten	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.
11.	Art. 11 Abs. 4	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.
12.	Art. 16b	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.
13.	Art. 31 Abs. 1	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.
14.	Art. 51 und 52	beibehalten	Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.
15.	Art. 60a	Streichung des Artikels	<p>Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen.</p> <p>Art. 60a VÜPF (Erläuterung Bundesrat: «...lediglich redaktionelle Änderungen....») sieht vor, dass Fernmeldedienstanbieterinnen über einen rückwirkenden Zeitraum von 6 Monaten alle Ziel-IP-Adressen liefern müssen, welche ihre Kunden besucht haben. Damit wird einerseits das Surfverhalten der gesamten schweizerischen Bevölkerung anlasslos und völlig unverhältnismässig ausspioniert. Andererseits wird die klare Vorgabe des BÜPF umgangen, das nur die Speicherung von Randdaten, aber nicht die Speicherung von Inhaltsdaten vorsieht.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Die geplante Überwachung des Internetverkehrs führt zu einer Überwachung, wer im Internet welche Adressen besucht hat. Dies geht zweifellos über die Schranken der gesetzlichen Regelung hinaus, dies insbesondere nachdem bereits die Aufzeichnung reiner Randdaten höchst umstritten und Gegenstand laufender Gerichtsverfahren ist. Hinzu kommt folgendes: Während bislang die Überwachung einer IP-Adresse nur im Rahmen einer sog. Echtzeit-Überwachung zulässig war, welche entsprechende Bewilligungen durch ein Gericht erforderte, muss neu nur noch ein einfaches Auskunftsbegehren durch die zuständige Behörde genehmigt werden. Die Abfragen erfolgen automatisiert.</p> <p>Art. 60a sieht weiter vor, dass bei nicht exakt zuordnbaren IP-Adressen die kompletten Listen aller Nutzerinnen und Nutzer zu liefern ist. IP-Adressen sind ein rares Gut. Alle FDA teilen diese den Nutzenden im Millisekunden-Takt zu. Da die Zeitstempel der Systemanbieter nicht immer übereinstimmen, sind diese IP-Adressen nicht immer eindeutig einem Nutzenden zuzuordnen. Neu müssen Provider nun komplett Listen aller Nutzenden liefern. Dies bringt Zehntausende in den Fokus von Überwachungsbehörden, was auf eine Art Rasterfahndung nach Delikten über grosse Teile der Bevölkerung hinausläuft. Entdecken Strafverfolger dabei zufälligerweise etwas, können sie umgehend Strafverfahren einleiten.</p> <p>Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde sodann gemäss Bericht gezielt auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten.</p> <p>Art. 60a ist zu streichen.</p>
16.	Art. 42a und Art. 43a	Streichung des Artikels	<p>Sowohl Art. 42a als auch Art. 43a fordern die Abrufbarkeit des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Nicht nur gilt auch hier wieder die Limite von 5'000 Nutzern, was somit fast die gesamte AAKD-Landschaft der Schweiz flächendeckend umfasst, sondern solche Abfragen sollen nun auch durch eine einfach «IR_» Abfrage gemacht werden können, welche im Gegensatz zu den «HD_»-Abfragen und den «RT_»-Überwachungen ohne weitere juristische Aufsicht automatisiert abgerufen werden können, obwohl es sich auch hier um das Abrufen einer IP-Adresse in der Vergangenheit handelt, genau wie bei den «HD_» abfragen, welche deutlich strenger reglementiert sind. Es ist nicht nachvollziehbar und verletzt aus unserer Sicht die gesetzliche Grundlage des BÜPF, dass Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber.</p> <p>Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser Automatisierten Auskünfte ergibt. Durch das Fehlen solcher Limiten könnte daher z.B. alle 5 Minuten eine solche Anfrage automatisiert gestellt werden. Zunächst können sich dadurch lärmende Kosten für die betroffenen AAKD ergeben. Sodann können die Anfragen an ein automatisiertes Auskunftssystem gestellt</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>werden, und es können auf diese Weise viele der Informationen welche ursprünglich über die juristisch sichereren HD_ und RT_ Auskunfts-/Überwachungstypen liegen, neu über den rechtlich unsicheren IR_- Typ eingeholt werden. IR_59 und IR_60 ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne dass sie den benötigten Kontrollen dieser invasiven Überwachungsarten unterliegen würden.</p> <p>Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind, wie dies das BÜPF vorsieht.</p> <p>Die beiden Artikel sind daher volumfänglich zu streichen.</p> <p>Diese neue Regelung und der zugehörige erläuternde Bericht sind im Übrigen eklatante Beispiele für die eingangs bemängelte überaus verwirrende und unverständliche Darstellung von Verordnungstext und erläuterndem Bericht.</p> <p>Im erläuternden Bericht steht auf S. 39 wörtlich:</p> <p><i>«In Absatz 1 sind die zu liefernden Angaben geregelt. Gemäss Buchstabe a ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin der oder dem Teilnehmenden einen solchen zugeteilt hat. Der «eindeutige Dienstidentifikator» gemäss Buchstabe b bezeichnet den Fernmelde- oder abgeleiteten Kommunikationsdienst, auf den sich die Antwort bezieht, eindeutig im Bereich der Anbieterin. In Buchstabe c werden die zu liefernden Angaben über den Ursprung der Verbindung bei der letzten zugriffsrelevanten Aktivität aufgezählt. Diese Angaben können für die Identifikation der Benutzerinnen und Benutzer nützlich sein.»</i></p> <p>Der Leser bzw. die Leserin urteile selber über die Verständlichkeit.</p> <p>Folgende Begriffe sind auch für den fachkundigen Leser nicht nachvollziehbar, bzw. es stellen sich folgende Verständnisfragen:</p> <ul style="list-style-type: none"> - Eindeutiger Identifikator: Was ist gemeint? Ist die Kundennummer des Internetproviders gemeint? Oder jene des genutzten dritten Fernmeldedienstes oder abgeleiteten Kommunikationsdienstes? Wie soll der Internetprovider überhaupt an diese Daten herankommen? - Eindeutiger Dienstidentifikator: Muss der Internetprovider eine Liste aller möglichen durch seine Kunden im Internet genutzten Kommunikationsdienste führen und aufzeichnen, muss er zudem aufzeichnen welcher Kunde welchen Dienst wann genau genutzt hat? Woher hat er diese Liste? Wie kann er herausfinden, ob ein Kunde gerade einen bestimmten Dienst nutzt? Gilt dies auch für ausländische Dienste? Nur für AAKD, für ausländische Fernmeldedienste, oder für alle Internetangebote weltweit? Der erläuternde Bericht bleibt hier völlig unklar.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<ul style="list-style-type: none"> - Was ist mit «Antwort» gemeint? Die Antwort des Servers des abgeleiteten Kommunikationsdienstes, den der Kunde besucht hat, oder die Antwort des Kundengeräts auf eine Nachricht von diesem Kommunikationsdienst? - Was ist mit «eindeutig im Bereich der Anbieterin» gemeint? Die Formulierung ist auch hier unverständlich. - Wie soll man sich eine «Antwort von einem anderen Fernmeldedienst» vorstellen? Muss ein Internetprovider die Herkunft sämtlicher auf seinem Netz eintreffenden Datenpakete aufzeichnen und dem Dienst ÜPF auf Anfrage diese Aufzeichnungen herausgeben? Wie soll die gigantische Masse an Daten, die durch ein solches Logging anfällt, durch die Internetprovider gemanaged werden? - Was ist mit «letzter zugriffsrelevanter Aktivitäten» gemeint? Geht es hier um die durch Kunden des Internetproviders aufgerufenen AAKD und andere Internetangebote? Wie soll der Internetprovider wissen, ob eine durch den Kunden aufgerufene IP-Adresse zu einem überwachungspflichtigen AAKD gehört, oder allenfalls zu einem nicht überwachungspflichtigen Dienst? Muss er einfach den ganzen Verkehr aufzeichnen? Wie weit zurück gehen die «zugriffsrelevanten» Aktivitäten? Müssen alle Daten für sechs Monate aufbewahrt werden? - Abgesehen davon: Wo wäre die gesetzliche Grundlage im BüPF für die vorgesehene inhaltliche Überwachung des Internetverkehrs? Das BüPF selber regelt bisher ausschliesslich die Überwachung der Randdaten, nicht aber von Inhaltsdaten, und spätestens dann, wenn Randdaten einen passant auch Auskunft über die vom Kunden abgerufenen Inhalte geben, handelt es sich dabei um Inhaltsdaten, deren Sammlung erst recht gesetzes- und verfassungswidrig wäre, nachdem schon das Sammeln reiner Randdaten als menschenrechtswidrig taxiert wurde.
17.	50a	Artikel streichen	<p>Art. 50a sieht neu vor, dass Anbieter verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Diese Pflicht gilt nicht mehr nur für FDA (Art. 26 BüPF) oder ausnahmsweise für ausgewählte AAKD von hoher wirtschaftlicher Bedeutung (Art. 27 BüPF), sondern soll nun vorgabemässig und ohne Differenzierung auf sämtliche Anbieter mit mehr als 5'000 Teilnehmern angewendet werden, womit wohl fast die gesamte Schweizer AAKD-Branche betroffen ist (kaum ein Produkt ist lebensfähig mit weniger als 5000 Teilnehmern).</p> <p>Dies stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar.</p> <p>Diese Ausweitung ist nicht nur unverhältnismässig, sondern gefährdet aktiv nahezu die gesamte Schweizer IT-Branche: Indem de facto alle Anbieter vorgabemässig gezwungen werden, ihre Verschlüsselungssysteme für Behörden jederzeit entschlüsselbar zu gestalten, entstehen enorme Sicherheitsrisiken, denn Verschlüsselung ist wie eine Eierschale: Unversehrt ist sie stark, aber der kleinste Riss führt zu einer er-</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>heblichen Schwächung. Die betroffenen Systeme werden durch den vom Verordnungsgeber nun verpflichtend vorgesehenen Einbau von Hintertüren anfälliger für Hackerangriffe, Datenmissbrauch und Spionage. Dies widerspricht Art. 13 BV und dem diesen konkretisierenden Datenschutzgesetz, das den Schutz personenbezogener Daten ausdrücklich durch wirksame technische Massnahmen – insbesondere Verschlüsselung – vorschreibt. Eine durch den Anbieter aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung in jedem Fall.</p> <p>Genau eine solche Schwächung der Verschlüsselung wurde kürzlich vom Europäischen Gerichtshof für Menschenrechte im Fall PODCHASOV gegen Russland (33696/19) als Verstoss gegen Grundrechte gewertet. Art. 50a verstösst somit auch gegen geltendes Völkerrecht.</p> <p>Nebst diesem Verstoss gegen das Völkerrecht wird aber auch das Gebot der Verhältnismässigkeit aus Art. 36 BV nicht eingehalten, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Wie bereits bei Art. 16e, Art. 16f und Art. 16g erwähnt, müssen zuerst die einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.</p> <p>Zusätzlich, und wie bereits bei Art. 16d erwähnt, verhindert Art. 50a die effektive Erbringung von VPN-Diensten. Bei solch einem VPN kontrolliert der Betreiber sowohl den Eingangs- als auch den Endpunkt. Da die Kommunikation vom Endpunkt zu einer Webseite aufgrund der vorherrschenden Struktur im allgemeinen Internet nicht End-zu-End-Verschlüsselt erfolgen kann, werden schon kleine VPNs (mit 5000 Nutzern) dazu gezwungen ihre eigene Verschlüsselung zu entfernen und ihre Kunden zu überwachen. Da der Schutz der Privatsphäre der Nutzer*innen von VPNs just den Kernpunkt oder USP der Dienstleistung darstellt, werden Schweizer VPN-Anbieterinnen hierdurch am internationalen Markt übermässig benachteiligt, ja ihres eigentlichen Daseinszwecks beraubt.</p> <p>Wesentlich ist zudem, dass Anbieter von Mail- oder Messaging-Apps zwangsläufig die Nachricht in der App in einer menschenlesbaren Version anzeigen muss, und dass an dieser Stelle die End-zu-End-Verschlüsselung notwendigerweise bereits entfernt ist. Der Wortlaut von Art. 50a lässt entgegen sämtlichen Beteuerungen des Dienstes ÜPF bereits anlässlich der letzten Revision der VÜPF weiterhin offen, ob eine Entfernung der Verschlüsselung auch an dieser Stelle gefordert werden können soll. Angesichts der seit</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			Jahren erkennbaren Tendenz der Schweizer Überwachungsbehörden, die Anwendbarkeit des Überwachungsrechts laufend weiter auszudehnen und sich dabei nur durch Gerichte bremsen zu lassen, ist bei dieser Gelegenheit erneut die Klarstellung zu fordern, wonach die Entfernung von Verschlüsselungen, die erst in der Sphäre des Benutzers angebracht werden (wenngleich auch durch Software der Anbieterin) nicht verlangt werden darf. Dies ist zumindest im erläuternden Bericht zu erwähnen. Der erneute Verzicht wäre nichts anderes als eine Einladung an die Überwachungsbehörden, die Einführung einer offensichtlich illegalen und vom BÜPF keineswegs vorgesehenen «Chatkontrolle» auf dem «Auslegungsweg» vorzunehmen.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Artikel	Antrag	Begründung / Bemerkung
VD-ÜPF / OME-SCPT / OE-SCPT		
Art. 14 Abs. 3 VD-ÜPF	Streichung	Wie bereits bei Art. 16e bis 16f Rev. VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit 5000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Absatz ist daher ersatzlos zu streichen.
Art. 14 Abs. 4 VD-ÜPF	Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten.	Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der Unterworfenen AAKD massiv. Dies ist wie beschrieben weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.
Art. 20 Abs. 1 VD-ÜPF	Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f Rev. VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.

*Vernehmlassungsantwort zu den Teilrevisionen der VÜPF und der VD-ÜPF
gemäss Schreiben des EJPD vom 29. Januar 2025*

Datum	2. Mai 2025
Verfasser (Unternehmen)	iWay AG, Badenerstrasse 569, 8048 Zürich
Kontaktperson bei Fragen (Name/Tel./E-Mail)	Henry Salzmann, 043 500 11 52, henry.salzmann@iway.ch

Dieses Dokument geht an:

Eidgenössisches Justiz- und Polizeidepartement EJPD, ptss-aemterkonsultationen@isc-eipd.admin.ch

Sehr geehrter Herr Bundesrat Jans, sehr geehrte Damen und Herren

Wir beziehen uns auf das am 29. Januar 2025 eröffnete Vernehmlassungsverfahren zu Teilrevisionen von VÜPF und VD-ÜPF und bedanken uns für die Möglichkeit einer Stellungnahme.

Wir lehnen die geplante Teilrevisionen der VÜPF und der VD-ÜPF in aller Deutlichkeit und vollumfänglich ab.

Im Bericht des Bundesrates zur aktuellen Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF und der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) ist zu lesen, dass die Revision im Wesentlichen auf die Anpassung der Verordnungen an die KMU-Freundlichkeit abziele. Ein grosser Teil der vorgeschlagenen Änderungen *verfolgt aber gerade das Gegenteil*.

Die Geschäftsgrundlagen von Schweizer Unternehmen wie Threema, Proton und anderer KMU, die weltweit einen hervorragenden Ruf als Anbieterinnen sicherer Kommunikationsdienste im Internet geniessen, drohen durch die Vorlage zerstört zu werden. Die Sicherheit des Internets in der Schweiz soll mit der Revision der Überwachung jeglichen Internetverkehrs regelrecht untergeordnet werden: «**Sicherheit vor Freiheit» ist das neue Paradigma**. Dieses zieht sich wie ein roter Faden quer durch diese völlig verunglückte Reform. KMU, die aus der Schweiz heraus Internet-Dienste anbieten («abgeleitete Kommunikationsdienste» in der Terminologie des Gesetzes), soll die Schweiz als Standort geradezu vergällt werden. Dies scheint denn auch zu gelingen: **Erste der betroffenen Unternehmen haben bereits angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen** (siehe Tages-Anzeiger vom 1. April 2025).

Ein derartiger Paradigmenwechsel, weg von KMU-Schutz und Überwachung mit Augenmass, hin zu knallharter Überwachung, die alle anderen Interessen unterordnet, wird durch das geltende Gesetz (BÜPF) keineswegs gestützt. Der Paradigmenwechsel widerspricht vielmehr geradezu dem Geist des ursprünglichen BÜPF, das Internetdienste, die in der Schweiz meist von KMU betrieben werden, gerade von der Implementierung teurer Überwachungsmassnahmen schützen wollte, und das eine austarierte Interessenabwägung vorsah zwischen Privatsphäre und Freiheit auf der einen Seite und staatlicher Überwachung auf der anderen Seite.

Entgegen dem im Begleitbericht zum vorgelegten Entwurf erklärten Ziel, die «finanzielle Belastung der KMU gering zu halten», stuft die Vorlage eine grosse Mehrheit der Schweizer Anbieterinnen von Internetdiensten in eine höhere Stufe auf, und zwingt sie neu auch in jenen Bereichen zu einer kostspieligen aktiven Überwachungstätigkeit, wo bisher nur eine KMU-freundliche Duldungspflicht bestand. Dies verschiebt das bisherige Gleichgewicht der Interessen zwischen Strafverfolgung und betroffenen Anbieterinnen in drastischer Weise zulasten der betroffenen Anbieterinnen.

Die vorgeschlagenen Anpassungen bringen ganz erhebliche Risiken für den Innovations- und Wirtschaftsstandort Schweiz mit sich und erfüllen die Kernziele der Revision, die Entlastung von KMU, gerade nicht. Der Ruf der Schweiz als sicherer Hafen für vertrauenswürdige IT-Anbieter droht durch die Revision nachhaltig beschädigt zu werden. Deshalb lehnen wir die Revision vollumfänglich ab.

Auch **die Schweizer Armee** nutzt solche Dienste, wie beispielsweise Threema, und zwar gerade aufgrund des hohen gebotenen Sicherheitsstandards. Die Annahme dieser Revision, welche dieses Sicherheitsniveau gezielt untergraben will, verletzt damit indirekt auch das direkte Interesse der Schweiz an lokal betriebenen Hochsicherheitsanwendungen. Gerade in der heutigen Zeit, in der die Zuverlässigkeit der grossen US-Anbieter in ihrer Abhängigkeit von einer zunehmend erratisch agierenden US-Regierung mehr und mehr in Frage steht, erscheint dies als **inakzeptable Hochrisikostrategie**.

Nicht zuletzt ist mit Nachdruck darauf hinzuweisen, dass die Revision die Überwachung ganz allgemein stark ausweitet. Dies ist mit der durch den Gesetzgeber im BÜPF festgelegten, fein austarierten Interessenabwägung zwischen Freiheit und Privatsphäre der Einwohner der Schweiz einerseits und Sicherheit durch Überwachungsmassnahmen andererseits absolut nicht vereinbar. Die Revision entpuppt sich geradezu als eine Art Wunschkonzert für Überwachungsbehörden. Insbesondere ist künftig auch **eine komplette inhaltliche Überwachung des gesamten Internetverkehrs** der Schweiz vorgesehen. Dies ohne dass eine solche inhaltliche Überwachung durch die gesetzlichen Grundlagen des BÜPF in irgend einer Weise gedeckt wäre: Zulässig ist gemäss BÜPF einzig und allein die Überwachung von Randdaten des Fernmeldeverkehrs, und selbst die Zulässigkeit der in diesem Kontext angewendeten anlasslosen Vorratsdatenspeicherung von Randdaten ist bis heute umstritten und Gegenstand von Gerichtsverfahren, ja in der EU bereits höchstrichterlich als menschenrechtswidrig erkannt. Die durch die Verordnungsrevision eingeführte *Inhaltsüberwachung* ist in der Schweiz damit erst recht **offensichtlich illegal und verfassungswidrig**.

Abschliessend sei noch der Hinweis angebracht, dass wir die Gesetzgebungstechnik des Entwurfs für überaus schlecht halten. **Sowohl der Verordnungstext als auch der zugehörige erläuternde Bericht sind über weite Strecken höchst verwirrend und unverständlich formuliert**, unter anderem mit einer Vielzahl von Querverweisen, technischen Fehlern und unklarer Begrifflichkeit (für ein Beispiel hierfür siehe unten, Bemerkungen zu Art. 43a). Die Texte sind in dieser Form selbst für Fachleute über weite Strecken nicht zu verstehen, geschweige denn als Ganzes zu überblicken. Für KMU, die durch die Revision neu mit erheblich strengerem Pflichten konfrontiert werden, ist eine rechtskonforme Umsetzung dieser Vorlage daher ein schlicht aussichtsloses Unterfangen.

Das Legalitätsprinzip gemäss Art. 5 Bundesverfassung fordert vom Gesetzgeber, dass Gesetzestexte für die Adressaten verständlich formuliert sind. Die Texte der Verordnungsrevision genügen dieser Anforderung offensichtlich in keiner Weise. Nur schon aufgrund der völlig fehlenden Verständlichkeit ist die Verfassungsmässigkeit der Revision insgesamt *höchst zweifelhaft*. Wir fordern nur schon deshalb einen Rückzug der vorgelegten Texte, eine komplette Überarbeitung zur Verbesserung der Verständlichkeit und eine erneute Auflage zur Vernehmlassung.

Mit freundlichen Grüßen

iWay AG



Henry Salzmann

Bemerkungen zu einzelnen Artikeln der VÜPF

Nr.	Artikel	Antrag	Begründung / Bemerkung
VÜPF / OSCPT / OSCPT			
0.	Alle Artikel	Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.	<p>Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kunden auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.</p> <p>Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.dgl. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.</p>
1.	16b, Abs. 1	Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.»	Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile, wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Anforderungen in Kauf nehmen.
2.	16c, Abs. 3	Streichung von lit. a «automatisierte Erteilung der Auskünfte (Art. 18 Abs. 2);»	Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Dies untergräbt rechtsstaatliche Prinzipien doppelt: Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>«natürliche» Schutzmechanismen gegen eine überschiessende, missbräuchliche oder zumindest unverhältnismässige Nutzung solcher Massnahmen durch die Untersuchungsbehörden.</p> <p>Der vorgesehene Umsetzungszeitraum von 12 Monaten für die rechtssichere Implementierung eines derart komplexen Systems völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.</p>
3.	Art. 16d	<p>Streichung von Online-speicherdiensten und VPN-Anbietern in der Auslegung</p>	<p>Eine klarere Definition des Begriffs AAKD ist begrüssenswert, doch die neue Auslegung gemäss erläuterndem Bericht geht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdiensten wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter, etc.) genutzt werden.</p> <p>Art. 2 lit. c BüPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug den gesetzlichen Rahmen sprengt. Onlinespeicherdiene sind deshalb aus Art. 16d zu streichen.</p> <p>Zudem anerkennt der erläuternde Bericht, dass VPNs zur Anonymisierung der Nutzer*innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Anbieter von VPNs sind daher ebenfalls aus dem Geltungsbereich von Art. 16d auszunehmen.</p>
4.	Art. 16e, Art. 16f und Art. 16g	<p>Streichung der Artikel und Beibehaltung der bestehenden Kriterien</p> <p>Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).</p>	<p>Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch diametral entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung. Dies daher, weil neu KMU bereits mit mehr als 5'000 Nutzern erfasst werden.</p> <p>Die Einführung von 5000 Nutzern als gesondert zu beurteilende Untergrenze verletzt aus unserer Sicht bereits Art. 27 Abs. 3 BüPF, denn 5000 Personen keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strenger Überwachungsmassnahmen, gerechtfertigt wären. 5000 Nutzer werden in der digitalen Welt vielmehr sehr rasch erreicht.</p> <p>Zusätzlich führt das Einführen eines «Konzerntatbestandes» in Art. 16f Abs. 3 zu massiven Problemen, da die Produkte nun nicht mehr für sich alleine eine bestimmte Grösse erreichen müssen, sondern die rele-</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>vanten Zahlen anhand des Umsatzes des Unternehmens, bzw. in Konzernverhältnissen sogar des Konzerns bestimmt werden. Vor allem bei Unternehmen mit Beteiligungsfirmen im Hintergrund fallen nun neu alle Dienstleistungen und Produkte automatisch unter die härteste Stufe, egal ob sie sich erst in einem frühen Entwicklungsstadium befinden. Dies behindert Innovation, da jedes Projekt bereits mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden müsste. Durch diese extreme Einstieghürde wird der Innovationsstandort Schweiz nachhaltig geschädigt.</p> <p>Gleichzeitig wird auch der Wirkungsbereich der VÜPF stark erweitert. Während heute ein Unternehmen einen grossen Teil seiner Geschäftstätigkeit durch abgeleitete Kommunikationsdienste erbringen muss (Art. 22 Abs. 1 lit. b und Art. 52 Abs. 1 lit. b VÜPF), fällt dieses Kriterium neu weg. Dadurch können künftig auch Unternehmen, deren Geschäftstätigkeit nur am Rande auf abgeleiteten Kommunikationsdiensten basiert, wie Onlineshops, Marktplätze, Auktionsplattformen, Zeitungen, Computerspielhersteller und zahlreiche weitere Unternehmen, unter die VÜPF fallen – allein deshalb, weil ihre Produkte irgendeine Form privater Kommunikation zwischen Nutzer*innen und/oder Drittanbietern ermöglichen.</p> <p>Die vorgeschlagene Regelung stünde sodann im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali, das die zu weite Betroffenheit und die seltene Anwendung von Downgrades kritisierte: «Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»</p> <p>Statt KMU zu entlasten, führt die Revision neu sogar zu einer «automatischen Hochstufung per Verordnung ohne konkretisierende Verfügung (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.</p> <p>Die neue Regelung steht zudem in offensichtlichem Widerspruch zur bisherigen Praxis, denn bis heute wurde gemäss Angaben des Dienst-ÜPF keine einzige AAKD hochgestuft. Auch der Bundesrat stützte sich ausdrücklich auf die geltende Kombination von drei Schranken – einem Unternehmensfokus auf Kommunikationsdienste, einer Umsatzgrenze von 100 Millionen Franken sowie einer grossen Nutzerzahl – als er noch 2023 begründete, die Umsetzung des BÜPF sei gerade wegen der genannten Schranken als KMU-freundlich zu verstehen. Die vorliegende Revision hebt jedoch genau diese Kombination kumulativer Kriterien auf und will die einzelnen Kriterien künftig alternativ anwenden bzw. streicht sie sogar vollständig. Dadurch verlieren die bisherigen Schutzmechanismen ihre Wirkung, und das BÜPF soll neu auf viele KMU Anwendung finden, die früher nicht unter Gesetz und Verordnung fielen.</p> <p>Die Analyse der offiziellen Statistik des Dienstes ÜPF macht die offensichtliche Unverhältnismässigkeit dieses Ansinnens deutlich. Im Jahr 2023 betrafen 98,95 % der total 9'430 Überwachungen allein</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,05 % für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,73 % wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100 % des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.</p> <p>Wesentlich ist insbesondere eine neue Pflicht zur Identifikation der Nutzer: Hiervon betroffen sind nicht nur alle AAKD mit reduzierten oder vollen Pflichten (und damit de facto fast alle AAKD der Schweiz), sondern auch all deren Wiederverkäufer. Im Ergebnis führt die neue Verordnung aus unserer Sicht dazu, dass man sich bei keinem marktrelevanten Dienst mehr anmelden kann, ohne den Pass, Führerschein oder ID zu hinterlegen oder zumindest Daten wie eine Telefonnummer anzugeben, die man ohne Pass oder ID nicht erhalten kann.</p> <p>Die automatische Hochstufung an sich führt bereits zu erheblicher Rechtsunsicherheit bei den betroffenen Unternehmen. Unter dem bestehenden System werden die generell-abstrakten Normen der VÜPF mittels Verfügung auf einen konkreten Einzelfall angewendet. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes ist aber im Zweifelsfall möglicherweise nur schwer zu beantworten. Zweifelsohne besteht hier ein schutzwürdiges Interesse seitens der AAKD daran, zu wissen, ob sie die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Nur das bisherige System entspricht den allgemeinen Grundsätzen des Verwaltungsverfahrens, welches für die Anwendung einer generell-abstrakten Norm eine Konkretisierung durch die Verwaltung voraussetzt. Von einer automatischen Hochstufung von AAKD ist daher aus Gründen der Rechtssicherheit abzusehen. Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.</p> <p>Gegenüber der alten VÜPF erweitert die Revision die Pflichten zur Automatisierung sodann noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragen wie z.B. IR_59 und IR_60, welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen. Genau diese Möglichkeit einer manuellen Intervention ist aber für die Provider kritisch, um Missbräuche zu verhindern, die wiederum die Verträge mit ihren Kunden und das Fernmeldegeheimnis verletzen könnten. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente damit erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 Bst. b der alten VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grossen[n] Teil ihrer Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. Damit fallen insbesondere bereits Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz. Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Dies setzt der Innovation in der Schweiz neue riesige Hürden entgegen.</p> <p>Auch Non-Profit-Organisationen wie die Signal Foundation, die kaum Umsätze erwirtschaften, geraten unter diese verschärften Vorgaben. Während sie bisher unter Duldungspflichten verbleiben konnten, solange sie Art. 22 Abs. 1 VÜPF nicht erfüllten, wird neu allein auf die Anzahl der Nutzer*innen abgestellt, womit z.B. Signal neu als AAKD mit vollen Pflichten erfasst würde. Dies würde dazu führen, dass Signal in der Schweiz entweder zu einem Rückzug aus dem Markt gezwungen wird oder erhebliche rechtliche Konsequenzen riskiert, da Signal keine IP-Adressen speichert und somit gegen Art. 19 RevVÜPF verstößt.</p> <p>Die Regelung ignoriert zudem wirtschaftliche Realitäten: Ein hoher Nutzerkreis bedeutet bei Non-Profits keine finanzielle Tragfähigkeit für umfangreiche Überwachungsmassnahmen. Damit werden Open-Source- und Non-Profit-Lösungen gezielt aus dem Markt gedrängt, während bestehende Monopole wie WhatsApp (96 % Marktanteil in der Schweiz) gestärkt werden. Die neue Regelung ist daher aus ökonomischer Sicht zu verwerfen. Das Kriterium der reinen Nutzerzahl ist ungeeignet und muss gestrichen werden.</p> <p>Nicht zuletzt schwächt die Regelung auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger*innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, Ende-zu-Ende-verschlüsselter Kommunikation ist heute wichtiger denn je.</p> <p>Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade als rechtswidrig gilt (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer*innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, sondern allein diese Anhäufung an Daten malt eine Zielscheibe auf den Rücken von Schweizer Unternehmen und Dienstleistungen für Hackerangriffe aus der ganzen Welt.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Weiters ist zu erwähnen, dass es gar nicht erwiesen ist, dass die Speicherung der fraglichen Daten eine merklich höhere Quote erfolgreicher Ermittlungen durch die Strafverfolgungsbehörden mit sich bringen würde. Im Gegenteil müssen die bereits existierenden Sekundärdaten, die allein durch die Bereitstellung eines Dienstes für den Nutzer entstehen, besser genutzt werden. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisbrauch via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfügt, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden. Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren.</p> <p>Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Souveränität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.</p> <p>Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das Datenschutzgesetz. Der Entwurf bringt nicht, wie der Begleitbericht dem Leser in geradezu in Orwell'scher Manier weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit und steht in direktem Gegensatz zum besagten Postulat 19.4031.</p> <p>Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen, und das bestehende System muss beibehalten werden.</p>
5.	Art. 16h Abs. 2	Streichung der Ausführung im erläuternden Bericht und ein Abstellen der Formulierung auf die gleichzeitige Anzahl Nutzer.	Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Nutzer*innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 Rev.VÜPF, gemäss dem die das WLAN erschliessenden FDA die Verantwortung für die Identifikation der Nutzer der WLANs tragen.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer*innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24) oder die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22). Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDAs unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden. Unter der bestehenden Regelung konnte eine FDA anhand der Lokation (z.B. Bibliothek, Flughafen) eine Einschätzung treffen. Die neue Definition hingegen würde von ihr verlangen, Zugriff auf jedes private Netzwerk zu erhalten, um Hardware und Einstellungen zu prüfen – ein offensichtlich verfassungswidriges und auch praktisch unmögliches Unterfangen. Diese vage Formulierung führt zu anhaltender Rechtsunsicherheit für FDA.</p> <p>Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten.</p> <p>Zudem könnte Art. 16h dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist*innen, Whistleblower*innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer*innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen. Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt.</p>
	Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2	Streichung des «Konzernatbestand» und Beibehaltung der bestehenden Regelung	<p>Die Verordnung nimmt neu nicht mehr die Umsatz- und Nutzerzahlen der betroffenen Unternehmen, sondern die Zahlen des jeweiligen Konzerns als Basis für Up- und Downgrades. Die Begründung zur Einführung dieses «Konzernatbestands», wonach die neue Regelung für die betroffenen Unternehmen zu einer Vereinfachung führe, ist kontraintuitiv, ja offensichtlich falsch und irreführend. In der Praxis sind die betroffenen Unternehmen nämlich schon heute verpflichtet, ihre Buchhaltung nach Produkten aufzugliedern. Somit können die Kennzahlen bereits heute sehr einfach festgestellt werden. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.</p>
6.	Art. 19 Abs. 1	Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation	<p>Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vor sieht.</p> <p>Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des Schweizer Datenschutzgesetzes, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch der Schutz der Schweizer Kundschaft massiv</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
		von Teilnehmenden.	<p>beeinträchtigt wird. Datenschutzfreundliche Unternehmen werden bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.</p> <p>Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Dies wahrt nicht nur den Datenschutz, sondern schützt auch die Wettbewerbsfähigkeit von KMU, stärkt den Innovationsstandort Schweiz und die digitale Souveränität unseres Landes.</p>
7.	Art. 18	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.
8.	Art. 19 Abs. 2	Ersatzlose Streichung zugunsten bestehender Regelung	Eine Überwachung von Kunden durch FDA, ob diese die neuen Vorgaben der VÜPF zu WLANs einhalten (Art. 19 Abs. 2 Rev. VÜPF), und erst recht die dazu gelieferte Erklärung im erläuternden Bericht, wonach die FDA die Identifikation der WLAN-Nutzer vorzunehmen hätten, ist weder gesetzeskonform noch zumutbar (siehe vorstehend). Art. 19 Abs. 2 ist ersatzlos zu streichen.
9.	Art. 21 Abs. 1 lit. a	Streichung	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.
10.	Art. 22	beibehalten	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.
11.	Art. 11 Abs. 4	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.
12.	Art. 16b	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.
13.	Art. 31 Abs. 1	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.
14.	Art. 51 und 52	beibehalten	Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.
15.	Art. 60a	Streichung des Artikels	Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Art. 60a VÜPF (Erläuterung Bundesrat: «...lediglich redaktionelle Änderungen....») sieht vor, dass Fernmelddenstanbieterinnen über einen rückwirkenden Zeitraum von 6 Monaten alle Ziel-IP-Adressen liefern müssen, welche ihre Kunden besucht haben. Damit wird einerseits das Surfverhalten der gesamten schweizerischen Bevölkerung anlasslos und völlig unverhältnismässig ausspioniert. Andererseits wird die klare Vorgabe des BÜPF umgangen, das nur die Speicherung von Randdaten, aber nicht die Speicherung von Inhaltsdaten vorsieht.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Die geplante Überwachung des Internetverkehrs führt zu einer Überwachung, wer im Internet welche Adressen besucht hat. Dies geht zweifellos über die Schranken der gesetzlichen Regelung hinaus, dies insbesondere nachdem bereits die Aufzeichnung reiner Randdaten höchst umstritten und Gegenstand laufender Gerichtsverfahren ist. Hinzu kommt folgendes: Während bislang die Überwachung einer IP-Adresse nur im Rahmen einer sog. Echtzeit-Überwachung zulässig war, welche entsprechende Bewilligungen durch ein Gericht erforderte, muss neu nur noch ein einfaches Auskunftsbegehren durch die zuständige Behörde genehmigt werden. Die Abfragen erfolgen automatisiert.</p> <p>Art. 60a sieht weiter vor, dass bei nicht exakt zuordenbaren IP-Adressen die kompletten Listen aller Nutzerinnen und Nutzer zu liefern ist. IP-Adressen sind ein rares Gut. Alle FDA teilen diese den Nutzenden im Millisekunden-Takt zu. Da die Zeitstempel der Systemanbieter nicht immer übereinstimmen, sind diese IP-Adressen nicht immer eindeutig einem Nutzenden zuzuordnen. Neu müssen Provider nun komplettene Listen aller Nutzenden liefern. Dies bringt Zehntausende in den Fokus von Überwachungsbehörden, was auf eine Art Rasterfahndung nach Delikten über grosse Teile der Bevölkerung hinausläuft. Entdecken Strafverfolger dabei zufälligerweise etwas, können sie umgehend Strafverfahren einleiten.</p> <p>Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde sodann gemäss Bericht gezielt auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten.</p> <p>Art. 60a ist zu streichen.</p>
16.	Art. 42a und Art. 43a	Streichung des Artikels	<p>Sowohl Art. 42a als auch Art. 43a fordern die Abrufbarkeit des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Nicht nur gilt auch hier wieder die Limite von 5'000 Nutzern, was somit fast die gesamte AAKD-Landschaft der Schweiz flächendeckend umfasst, sondern solche Abfragen sollen nun auch durch eine einfach «IR_» Abfrage gemacht werden können, welche im Gegensatz zu den «HD_»-Abfragen und den «RT_»-Überwachungen ohne weitere juristische Aufsicht automatisiert abgerufen werden können, obwohl es sich auch hier um das Abrufen einer IP-Adresse in der Vergangenheit handelt, genau wie bei den «HD_» abfragen, welche deutlich strenger reglementiert sind. Es ist nicht nachvollziehbar und verletzt aus unserer Sicht die gesetzliche Grundlage des BÜPF, dass Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber.</p> <p>Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser Automatisierten Auskünfte ergibt. Durch das Fehlen solcher Limiten könnte daher z.B. alle 5 Minuten eine solche Anfrage automatisiert gestellt werden. Zunächst können sich dadurch lärmende Kosten für die betroffenen AAKD ergeben. Sodann können die Anfragen an ein automatisiertes Auskunftssystem gestellt werden, und es können auf diese Weise viele der Informationen welche ursprünglich über die juristisch</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>sichereren HD_ und RT_ Auskunfts-/Überwachungstypen liefern, neu über den rechtlich unsicheren IR_- Typ eingeholt werden. IR_59 und IR_60 ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne dass sie den benötigten Kontrollen dieser invasiven Überwachungsarten unterliegen würden.</p> <p>Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind, wie dies das BÜPF vorsieht.</p> <p>Die beiden Artikel sind daher vollumfänglich zu streichen.</p> <p>Diese neue Regelung und der zugehörige erläuternde Bericht sind im Übrigen eklatante Beispiele für die eingangs bemängelte überaus verwirrende und unverständliche Darstellung von Verordnungstext und erläuterndem Bericht.</p> <p>Im erläuternden Bericht steht auf S. 39 wörtlich:</p> <p><i>«In Absatz 1 sind die zu liefernden Angaben geregelt. Gemäss Buchstabe a ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin der oder dem Teilnehmenden einen solchen zugeteilt hat. Der «eindeutige Dienstidentifikator» gemäss Buchstabe b bezeichnet den Fernmelde- oder abgeleiteten Kommunikationsdienst, auf den sich die Antwort bezieht, eindeutig im Bereich der Anbieterin. In Buchstabe c werden die zu liefernden Angaben über den Ursprung der Verbindung bei der letzten zugriffsrelevanten Aktivität aufgezählt. Diese Angaben können für die Identifikation der Benutzerinnen und Benutzer nützlich sein.»</i></p> <p>Der Leser bzw. die Leserin urteile selber über die Verständlichkeit.</p> <p>Folgende Begriffe sind auch für den fachkundigen Leser nicht nachvollziehbar, bzw. es stellen sich folgende Verständnisfragen:</p> <ul style="list-style-type: none"> - Eindeutiger Identifikator: Was ist gemeint? Ist die Kundennummer des Internetproviders gemeint? Oder jene des genutzten dritten Fernmeldedienstes oder abgeleiteten Kommunikationsdienstes? Wie soll der Internetprovider überhaupt an diese Daten herankommen? - Eindeutiger Dienstidentifikator: Muss der Internetprovider eine Liste aller möglichen durch seine Kunden im Internet genutzten Kommunikationsdienste führen und aufzeichnen, muss er zudem aufzeichnen welcher Kunde welchen Dienst wann genau genutzt hat? Woher hat er diese Liste? Wie kann er herausfinden, ob ein Kunde gerade einen bestimmten Dienst nutzt? Gilt dies auch für ausländische Dienste? Nur für AAKD, für ausländische Fernmeldedienste, oder für alle Internetangebote weltweit? Der erläuternde Bericht bleibt hier völlig unklar.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<ul style="list-style-type: none"> - Was ist mit «Antwort» gemeint? Die Antwort des Servers des abgeleiteten Kommunikationsdienstes, den der Kunde besucht hat, oder die Antwort des Kundengeräts auf eine Nachricht von diesem Kommunikationsdienst? - Was ist mit «eindeutig im Bereich der Anbieterin» gemeint? Die Formulierung ist auch hier unverständlich. - Wie soll man sich eine «Antwort von einem anderen Fernmeldedienst» vorstellen? Muss ein Internetprovider die Herkunft sämtlicher auf seinem Netz eintreffenden Datenpakete aufzeichnen und dem Dienst ÜPF auf Anfrage diese Aufzeichnungen herausgeben? Wie soll die gigantische Masse an Daten, die durch ein solches Logging anfällt, durch die Internetprovider gemanaged werden? - Was ist mit «letzter zugriffsrelevanter Aktivitäten» gemeint? Geht es hier um die durch Kunden des Internetproviders aufgerufenen AAKD und andere Internetangebote? Wie soll der Internetprovider wissen, ob eine durch den Kunden aufgerufene IP-Adresse zu einem überwachungspflichtigen AAKD gehört, oder allenfalls zu einem nicht überwachungspflichtigen Dienst? Muss er einfach den ganzen Verkehr aufzeichnen? Wie weit zurück gehen die «zugriffsrelevanten» Aktivitäten? Müssen alle Daten für sechs Monate aufbewahrt werden? - Abgesehen davon: Wo wäre die gesetzliche Grundlage im BüPF für die vorgesehene inhaltliche Überwachung des Internetverkehrs? Das BüPF selber regelt bisher ausschliesslich die Überwachung der Randdaten, nicht aber von Inhaltsdaten, und spätestens dann, wenn Randdaten einen passant auch Auskunft über die vom Kunden abgerufenen Inhalte geben, handelt es sich dabei um Inhaltsdaten, deren Sammlung erst recht gesetzes- und verfassungswidrig wäre, nachdem schon das Sammeln reiner Randdaten als menschenrechtswidrig taxiert wurde.
17.	50a	Artikel streichen	<p>Art. 50a sieht neu vor, dass Anbieter verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Diese Pflicht gilt nicht mehr nur für FDA (Art. 26 BüPF) oder ausnahmsweise für ausgewählte AAKD von hoher wirtschaftlicher Bedeutung (Art. 27 BüPF), sondern soll nun vorgabemässig und ohne Differenzierung auf sämtliche Anbieter mit mehr als 5'000 Teilnehmern angewendet werden, womit wohl fast die gesamte Schweizer AAKD-Branche betroffen ist (kaum ein Produkt ist lebensfähig mit weniger als 5000 Teilnehmern).</p> <p>Dies stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar.</p> <p>Diese Ausweitung ist nicht nur unverhältnismässig, sondern gefährdet aktiv nahezu die gesamte Schweizer IT-Branche: Indem de facto alle Anbieter vorgabemässig gezwungen werden, ihre Verschlüsselungssysteme für Behörden jederzeit entschlüsselbar zu gestalten, entstehen enorme Sicherheitsrisiken, denn</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Verschlüsselung ist wie eine Eierschale: Unversehrt ist sie stark, aber der kleinste Riss führt zu einer erheblichen Schwächung. Die betroffenen Systeme werden durch den vom Verordnungsgeber nun verpflichtend vorgesehenen Einbau von Hintertüren anfälliger für Hackerangriffe, Datenmissbrauch und Spionage. Dies widerspricht Art. 13 BV und dem diesen konkretisierenden Datenschutzgesetz, das den Schutz personenbezogener Daten ausdrücklich durch wirksame technische Massnahmen – insbesondere Verschlüsselung – vorschreibt. Eine durch den Anbieter aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung in jedem Fall.</p> <p>Genau eine solche Schwächung der Verschlüsselung wurde kürzlich vom Europäischen Gerichtshof für Menschenrechte im Fall PODCHASOV gegen Russland (33696/19) als Verstoss gegen Grundrechte gewertet. Art. 50a verstösst somit auch gegen geltendes Völkerrecht.</p> <p>Nebst diesem Verstoss gegen das Völkerrecht wird aber auch das Gebot der Verhältnismässigkeit aus Art. 36 BV nicht eingehalten, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördararbeit steht. Wie bereits bei Art. 16e, Art. 16f und Art. 16g erwähnt, müssen zuerst die einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.</p> <p>Zusätzlich, und wie bereits bei Art. 16d erwähnt, verhindert Art. 50a die effektive Erbringung von VPN-Diensten. Bei solch einem VPN kontrolliert der Betreiber sowohl den Eingangs- als auch den Endpunkt. Da die Kommunikation vom Endpunkt zu einer Webseite aufgrund der vorherrschenden Struktur im allgemeinen Internet nicht End-zu-End-Verschlüsselt erfolgen kann, werden schon kleine VPNs (mit 5000 Nutzern) dazu gezwungen ihre eigene Verschlüsselung zu entfernen und ihre Kunden zu überwachen. Da der Schutz der Privatsphäre der Nutzer*innen von VPNs just den Kernpunkt oder USP der Dienstleistung darstellt, werden Schweizer VPN-Anbieterinnen hierdurch am internationalen Markt übermässig benachteiligt, ja ihres eigentlichen Daseinszwecks beraubt.</p> <p>Wesentlich ist zudem, dass Anbieter von Mail- oder Messaging-Apps zwangsläufig die Nachricht in der App in einer menschenlesbaren Version anzeigen muss, und dass an dieser Stelle die End-zu-End-Verschlüsselung notwendigerweise bereits entfernt ist. Der Wortlaut von Art. 50a lässt entgegen sämtlichen Beteuerungen des Dienstes ÜPF bereits anlässlich der letzten Revision der VÜPF weiterhin offen, ob eine Entfernung der Verschlüsselung auch an dieser Stelle gefordert werden können soll. Angesichts der seit</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			Jahren erkennbaren Tendenz der Schweizer Überwachungsbehörden, die Anwendbarkeit des Überwachungsrechts laufend weiter auszudehnen und sich dabei nur durch Gerichte bremsen zu lassen, ist bei dieser Gelegenheit erneut die Klarstellung zu fordern, wonach die Entfernung von Verschlüsselungen, die erst in der Sphäre des Benutzers angebracht werden (wenngleich auch durch Software der Anbieterin) nicht verlangt werden darf. Dies ist zumindest im erläuternden Bericht zu erwähnen. Der erneute Verzicht wäre nichts anderes als eine Einladung an die Überwachungsbehörden, die Einführung einer offensichtlich illegalen und vom BÜPF keineswegs vorgesehenen «Chatkontrolle» auf dem «Auslegungsweg» vorzunehmen.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Artikel	Antrag	Begründung / Bemerkung	
VD-ÜPF / OME-SCPT / OE-SCPT			
Art. 14 Abs. 3 VD-ÜPF	Streichung	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit 5000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Absatz ist daher ersatzlos zu streichen.	
Art. 14 Abs. 4 VD-ÜPF	Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten.	Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der unterworfenen AAKD massiv. Dies ist wie beschrieben weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.	
Art. 20 Abs. 1 VD-ÜPF	Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.	

*Vernehmlassungsantwort zu den Teilrevisionen der VÜPF und der VD-ÜPF
gemäss Schreiben des EJPD vom 29. Januar 2025*

Datum	05.05.2025
Verfasser (Unternehmen)	NYM Technologies SA
Kontaktperson bei Fragen (Name/Tel./E-Mail)	Alexis Roussel / alexis@nym.com

Dieses Dokument geht an:

Eidgenössisches Justiz- und Polizeidepartement EJPD, ptss-aemterkonsultationen@isc-ejpd.admin.ch

Sehr geehrter Herr Bundesrat Jans, sehr geehrte Damen und Herren

Wir beziehen uns auf das am 29. Januar 2025 eröffnete Vernehmlassungsverfahren zu Teilrevisionen von VÜPF und VD-ÜPF und bedanken uns für die Möglichkeit einer Stellungnahme.

Wir lehnen die geplante Teilrevisionen der VÜPF und der VD-ÜPF in aller Deutlichkeit und vollumfänglich ab.

Im Bericht des Bundesrates zur aktuellen Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF und der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) ist zu lesen, dass die Revision im Wesentlichen auf die Anpassung der Verordnungen an die KMU-Freundlichkeit abziele. Ein grosser Teil der vorgeschlagenen Änderungen verfolgt aber gerade das Gegenteil.

Die Geschäftsgrundlagen von Schweizer Unternehmen wie Threema, Proton und anderer KMU, die weltweit einen hervorragenden Ruf als Anbieterinnen sicherer Kommunikationsdienste im Internet geniessen, drohen durch die Vorlage zerstört zu werden. Die Sicherheit des Internets in der Schweiz soll mit der Revision der Überwachung jeglichen Internetverkehrs regelrecht untergeordnet werden: **«Sicherheit vor Freiheit» ist das neue Paradigma.** Dieses zieht sich wie ein roter Faden quer durch diese völlig verunglückte Reform. KMU, die aus der Schweiz heraus Internet-Dienste anbieten («abgeleitete Kommunikationsdienste» in der Terminologie des Gesetzes), soll die Schweiz als Standort geradezu vergällt werden. Dies scheint denn auch zu gelingen: **Erste der betroffenen Unternehmen haben bereits angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen** (siehe Tages-Anzeiger vom 1. April 2025). **Auch unser Unternehmen wird ins Ausland abwandern müssen,** was für unseren Kanton einen Nettoverlust bedeuten würde.

Ein derartiger Paradigmenwechsel, weg von KMU-Schutz und Überwachung mit Augenmass, hin zu knallharter Überwachung, die alle anderen Interessen unterordnet, wird durch das geltende Gesetz (BÜPF) keineswegs gestützt. Der Paradigmenwechsel widerspricht vielmehr geradezu dem Geist des ursprünglichen BÜPF, das Internetdienste, die in der Schweiz meist von KMU betrieben werden, gerade von der Implementierung teurer Überwachungsmassnahmen schützen wollte, und das eine austarierte Interessenabwägung vorsah zwischen Privatsphäre und Freiheit auf der einen Seite und staatlicher Überwachung auf der anderen Seite.

Entgegen dem im Begleitbericht zum vorgelegten Entwurf erklärten Ziel, die «finanzielle Belastung der KMU gering zu halten», stuft die Vorlage eine grosse Mehrheit der Schweizer Anbieterinnen von Internetdiensten in eine höhere Stufe auf, und zwingt sie neu auch in jenen Bereichen zu einer kostspieligen aktiven Überwachungstätigkeit, wo bisher nur eine KMU-freundliche Duldungspflicht bestand. Dies verschiebt das bisherige Gleichgewicht der Interessen zwischen Strafverfolgung und betroffenen Anbieterinnen in drastischer Weise zugunsten der betroffenen Anbieterinnen.

Die vorgeschlagenen Anpassungen bringen ganz erhebliche Risiken für den Innovations- und Wirtschaftsstandort Schweiz mit sich und erfüllen die Kernziele der Revision, die Entlastung von KMU, gerade nicht. Der Ruf der Schweiz als sicherer Hafen für vertrauenswürdige IT-Anbieter droht durch die Revision nachhaltig beschädigt zu werden. Deshalb lehnen wir die Revision vollumfänglich ab.

Auch **die Schweizer Armee** nutzt solche Dienste, wie beispielsweise Threema, und zwar gerade aufgrund des hohen gebotenen Sicherheitsstandards. Die Annahme dieser Revision, welche dieses Sicherheitsniveau gezielt untergraben will, verletzt damit indirekt auch das direkte Interesse der Schweiz an lokal betriebenen Hochsicherheitsanwendungen. Gerade in der heutigen Zeit, in der die Zuverlässigkeit der grossen US-Anbieter in ihrer Abhängigkeit von einer zunehmend erratisch agierenden US-Regierung mehr und mehr in Frage steht, erscheint dies als **inakzeptable Hochrisikostrategie**.

Nicht zuletzt ist mit Nachdruck darauf hinzuweisen, dass die Revision die Überwachung ganz allgemein stark ausweitet. Dies ist mit der durch den Gesetzgeber im BÜPF festgelegten, fein austarierten Interessenabwägung zwischen Freiheit und Privatsphäre der Einwohner der Schweiz einerseits und Sicherheit durch Überwachungsmassnahmen andererseits absolut nicht vereinbar. Die Revision entpuppt sich geradezu als eine Art Wunschkonzert für Überwachungsbehörden. Insbesondere ist künftig auch **eine komplette inhaltliche Überwachung des gesamten Internetverkehrs** der Schweiz vorgesehen. Dies ohne dass eine solche inhaltliche Überwachung durch die gesetzlichen Grundlagen des BÜPF in irgend einer Weise gedeckt wäre: Zulässig ist gemäss BÜPF einzig und allein die Überwachung von Randdaten des Fernmeldeverkehrs, und selbst die Zulässigkeit der in diesem Kontext angewendeten anlasslosen Vorratsdatenspeicherung von Randdaten ist bis heute umstritten und Gegenstand von Gerichtsverfahren, ja in der EU bereits höchstrichterlich als menschenrechtswidrig erkannt. Die durch die Verordnungsrevision eingeführte *Inhaltsüberwachung* ist in der Schweiz damit erst recht **offensichtlich illegal und verfassungswidrig**.

Abschliessend sei noch der Hinweis angebracht, dass wir die Gesetzgebungstechnik des Entwurfs für überaus schlecht halten. **Sowohl der Verordnungstext als auch der zugehörige erläuternde Bericht sind über weite Strecken höchst verwirrend und unverständlich formuliert**, unter anderem mit einer Vielzahl von Querverweisen, technischen Fehlern und unklarer Begrifflichkeiten (für ein Beispiel hierfür siehe unten, Bemerkungen zu Art. 43a). Die Texte sind in dieser Form selbst für Fachleute über weite Strecken nicht zu verstehen, geschweige denn als Ganzes zu überblicken. Für KMU, die durch die Revision neu mit erheblich strengerem Pflichten konfrontiert werden, ist eine rechtskonforme Umsetzung dieser Vorlage daher ein schlicht aussichtsloses Unterfangen.

Das Legalitätsprinzip gemäss Art. 5 Bundesverfassung fordert vom Gesetzgeber, dass Gesetzestexte für die Adressaten verständlich formuliert sind. Die Texte der Verordnungsrevision genügen dieser Anforderung offensichtlich in keiner Weise. Nur schon aufgrund der völlig fehlenden Verständlichkeit ist die Verfassungsmässigkeit der Revision insgesamt *höchst zweifelhaft*. Wir fordern nur schon deshalb einen Rückzug der vorgelegten Texte, eine komplette Überarbeitung zur Verbesserung der Verständlichkeit und eine erneute Auflage zur Vernehmlassung.

Mit freundlichen Grüßen

NYM Technologies SA, Alexis Roussel

Bemerkungen zu einzelnen Artikeln der VÜPF

Nr.	Artikel	Antrag	Begründung / Bemerkung
VÜPF / OSCPT / OSCPT			
0.	Alle Artikel	Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.	<p>Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kunden auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.</p> <p>Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.dgl. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.</p>
1.	16b, Abs. 1	Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.»	Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile, wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Anforderungen in Kauf nehmen.
2.	16c, Abs. 3	Streichung von lit. a «automatisierte Erteilung der Auskünfte (Art. 18 Abs. 2);»	Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Dies untergräbt rechtsstaatliche Prinzipien doppelt: Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>dienen als «natürliche» Schutzmechanismen gegen eine überschiessende, missbräuchliche oder zumindest unverhältnismässige Nutzung solcher Massnahmen durch die Untersuchungsbehörden.</p> <p>Der vorgesehene Umsetzungszeitraum von 12 Monaten für die rechtssichere Implementierung eines derart komplexen Systems völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.</p>
3.	Art. 16d	Streichung von Onlinespeicherdielen und VPN-Anbietern in der Auslegung	<p>Eine klarere Definition des Begriffs AAKD ist begrüssenswert, doch die neue Auslegung gemäss erläuterndem Bericht geht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdielen wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter, etc.) genutzt werden.</p> <p>Art. 2 lit. c BüPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug den gesetzlichen Rahmen sprengt. Onlinespeicherdielen sind deshalb aus Art. 16d zu streichen.</p> <p>Zudem anerkennt der erläuternde Bericht, dass VPNs zur Anonymisierung der Nutzer*innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Anbieter von VPNs sind daher ebenfalls aus dem Geltungsbereich von Art. 16d auszunehmen.</p>
4.	Art. 16e, Art. 16f und Art. 16g	<p>Streichung der Artikel und Beibehaltung der bestehenden Kriterien</p> <p>Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).</p>	<p>Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch diametral entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung. Dies daher, weil neu KMU bereits mit mehr als 5'000 Nutzern erfasst werden.</p> <p>Die Einführung von 5000 Nutzern als gesondert zu beurteilende Untergrenze verletzt aus unserer Sicht bereits Art. 27 Abs. 3 BüPF, denn 5000 Personen keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strenger Überwachungsmassnahmen, gerechtfertigt wären. 5000 Nutzer werden in der digitalen Welt vielmehr sehr rasch erreicht.</p> <p>Zusätzlich führt das Einführen eines «Konzernatbestandes» in Art. 16f Abs. 3 zu massiven Problemen, da</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>die Produkte nun nicht mehr für sich alleine eine bestimmte Grösse erreichen müssen, sondern die relevanten Zahlen anhand des Umsatzes des Unternehmens, bzw. in Konzernverhältnissen sogar des Konzerns bestimmt werden. Vor allem bei Unternehmen mit Beteiligungsfirmen im Hintergrund fallen nun neu alle Dienstleistungen und Produkte automatisch unter die härteste Stufe, egal ob sie sich erst in einem frühen Entwicklungsstadium befinden. Dies behindert Innovation, da jedes Projekt bereits mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden müsste. Durch diese extreme Einstiegshürde wird der Innovationsstandort Schweiz nachhaltig geschädigt.</p> <p>Gleichzeitig wird auch der Wirkungsbereich der VÜPF stark erweitert. Während heute ein Unternehmen einen grossen Teil seiner Geschäftstätigkeit durch abgeleitete Kommunikationsdienste erbringen muss (Art. 22 Abs. 1 lit. b und Art. 52 Abs. 1 lit. b VÜPF), fällt dieses Kriterium neu weg. Dadurch können künftig auch Unternehmen, deren Geschäftstätigkeit nur am Rande auf abgeleiteten Kommunikationsdiensten basiert, wie Onlineshops, Marktplätze, Auktionsplattformen, Zeitungen, Computerspielhersteller und zahlreiche weitere Unternehmen, unter die VÜPF fallen – allein deshalb, weil ihre Produkte irgendeine Form privater Kommunikation zwischen Nutzer*innen und/oder Drittanbietern ermöglichen.</p> <p>Die vorgeschlagene Regelung stünde sodann im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali, das die zu weite Betroffenheit und die seltene Anwendung von Downgrades kritisierte: «Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»</p> <p>Statt KMU zu entlasten, führt die Revision neu sogar zu einer «automatischen Hochstufung per Verordnung ohne konkretisierende Verfügung (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.</p> <p>Die neue Regelung steht zudem in offensichtlichem Widerspruch zur bisherigen Praxis, denn bis heute wurde gemäss Angaben des Dienst-ÜPF keine einzige AAKD hochgestuft. Auch der Bundesrat stützte sich ausdrücklich auf die geltende Kombination von drei Schranken – einem Unternehmensfokus auf Kommunikationsdienste, einer Umsatzgrenze von 100 Millionen Franken sowie einer grossen Nutzerzahl – als er noch 2023 begründete, die Umsetzung des BÜPF sei gerade wegen der genannten Schranken als KMU-freundlich zu verstehen. Die vorliegende Revision hebt jedoch genau diese Kombination kumulativer Kriterien auf und will die einzelnen Kriterien künftig alternativ anwenden bzw. streicht sie sogar vollständig. Dadurch verlieren die bisherigen Schutzmechanismen ihre Wirkung, und das BÜPF soll neu auf viele KMU Anwendung finden, die früher nicht unter Gesetz und Verordnung fielen.</p> <p>Die Analyse der offiziellen Statistik des Dienstes ÜPF macht die offensichtliche Unverhältnismässigkeit</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>dieses Ansinnens deutlich. Im Jahr 2023 betrafen 98,95 % der total 9'430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,05 % für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,73 % wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100 % des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.</p> <p>Wesentlich ist insbesondere eine neue Pflicht zur Identifikation der Nutzer: Hiervon betroffen sind nicht nur alle AAKD mit reduzierten oder vollen Pflichten (und damit de facto fast alle AAKD der Schweiz), sondern auch all deren Wiederverkäufer. Im Ergebnis führt die neue Verordnung aus unserer Sicht dazu, dass man sich bei keinem marktrelevanten Dienst mehr anmelden kann, ohne den Pass, Führerschein oder ID zu hinterlegen oder zumindest Daten wie eine Telefonnummer anzugeben, die man ohne Pass oder ID nicht erhalten kann.</p> <p>Die automatische Hochstufung an sich führt bereits zu erheblicher Rechtsunsicherheit bei den betroffenen Unternehmen. Unter dem bestehenden System werden die generell-abstrakten Normen der VÜPF mittels Verfügung auf einen konkreten Einzelfall angewendet. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes ist aber im Zweifelsfall möglicherweise nur schwer zu beantworten. Zweifelsohne besteht hier ein schutzwürdiges Interesse seitens der AAKD daran, zu wissen, ob sie die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Nur das bisherige System entspricht den allgemeinen Grundsätzen des Verwaltungsverfahrens, welches für die Anwendung einer generell-abstrakten Norm eine Konkretisierung durch die Verwaltung voraussetzt. Von einer automatischen Hochstufung von AAKD ist daher aus Gründen der Rechtssicherheit abzusehen. Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.</p> <p>Gegenüber der alten VÜPF erweitert die Revision die Pflichten zur Automatisierung sodann noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragen wie z.B. IR_59 und IR_60, welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen. Genau diese Möglichkeit einer manuellen Intervention ist aber für die Provider kritisch, um Missbräuche zu verhindern, die wiederum die Verträge mit ihren Kunden und das Fernmeldegeheimnis verletzen könnten. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente damit erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>ersatzlos gestrichen werden.</p> <p>Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 Bst. b der alten VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grossen[n] Teil ihrer Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. Damit fallen insbesondere bereits Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz. Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Dies setzt der Innovation in der Schweiz neue riesige Hürden entgegen.</p> <p>Auch Non-Profit-Organisationen wie die Signal Foundation, die kaum Umsätze erwirtschaften, geraten unter diese verschärften Vorgaben. Während sie bisher unter Duldungspflichten verbleiben konnten, solange sie Art. 22 Abs. 1 VÜPF nicht erfüllten, wird neu allein auf die Anzahl der Nutzer*innen abgestellt, womit z.B. Signal neu als AAKD mit vollen Pflichten erfasst würde. Dies würde dazu führen, dass Signal in der Schweiz entweder zu einem Rückzug aus dem Markt gezwungen wird oder erhebliche rechtliche Konsequenzen riskiert, da Signal keine IP-Adressen speichert und somit gegen Art. 19 RevVÜPF verstößt.</p> <p>Die Regelung ignoriert zudem wirtschaftliche Realitäten: Ein hoher Nutzerkreis bedeutet bei Non-Profits keine finanzielle Tragfähigkeit für umfangreiche Überwachungsmassnahmen. Damit werden Open-Source- und Non-Profit-Lösungen gezielt aus dem Markt gedrängt, während bestehende Monopole wie WhatsApp (96 % Marktanteil in der Schweiz) gestärkt werden. Die neue Regelung ist daher aus ökonomischer Sicht zu verwerfen. Das Kriterium der reinen Nutzerzahl ist ungeeignet und muss gestrichen werden.</p> <p>Nicht zuletzt schwächt die Regelung auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger*innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, Ende-zu-Ende-verschlüsselter Kommunikation ist heute wichtiger denn je.</p> <p>Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade als rechtswidrig gilt (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer*innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, sondern allein diese</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Anhäufung an Daten malt eine Zielscheibe auf den Rücken von Schweizer Unternehmen und Dienstleistungen für Hackerangriffe aus der ganzen Welt.</p> <p>Weiters ist zu erwähnen, dass es gar nicht erwiesen ist, dass die Speicherung der fraglichen Daten eine merklich höhere Quote erfolgreicher Ermittlungen durch die Strafverfolgungsbehörden mit sich bringen würde. Im Gegenteil müssen die bereits existierenden Sekundärdaten, die allein durch die Bereitstellung eines Dienstes für den Nutzer entstehen, besser genutzt werden. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisshandlung via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfügt, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden. Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren.</p> <p>Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Souveränität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.</p> <p>Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das Datenschutzgesetz. Der Entwurf bringt nicht, wie der Begleitbericht dem Leser in geradezu in Orwell'scher Manier weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit und steht in direktem Gegensatz zum besagten Postulat 19.4031.</p> <p>Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen, und das bestehende System muss beibehalten werden.</p>
5.	Art. 16h Abs. 2	Streichung der Ausführung im erläuternden Bericht und	Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Nutzer*innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die

Nr.	Artikel	Antrag	Begründung / Bemerkung
		ein Abstellen der Formulierung auf die gleichzeitige Anzahl Nutzer.	<p>praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 Rev.VÜPF, gemäss dem die das WLAN erschliessenden FDA die Verantwortung für die Identifikation der Nutzer der WLANs tragen.</p> <p>Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer*innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24) oder die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22). Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDAs unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden. Unter der bestehenden Regelung konnte eine FDA anhand der Lokation (z.B. Bibliothek, Flughafen) eine Einschätzung treffen. Die neue Definition hingegen würde von ihr verlangen, Zugriff auf jedes private Netzwerk zu erhalten, um Hardware und Einstellungen zu prüfen – ein offensichtlich verfassungswidriges und auch praktisch unmögliches Unterfangen. Diese vage Formulierung führt zu anhaltender Rechtsunsicherheit für FDA.</p> <p>Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten.</p> <p>Zudem könnte Art. 16h dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist*innen, Whistleblower*innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer*innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen. Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt.</p>
	Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2	Streichung des «Konzerntatbestand» und Beibehaltung der bestehenden Regelung	Die Verordnung nimmt neu nicht mehr die Umsatz- und Nutzerzahlen der betroffenen Unternehmen, sondern die Zahlen des jeweiligen Konzerns als Basis für Up- und Downgrades. Die Begründung zur Einführung dieses «Konzerntatbestands», wonach die neue Regelung für die betroffenen Unternehmen zu einer Vereinfachung führe, ist kontraintuitiv, ja offensichtlich falsch und irreführend. In der Praxis sind die betroffenen Unternehmen nämlich schon heute verpflichtet, ihre Buchhaltung nach Produkten aufzugliedern. Somit können die Kennzahlen bereits heute sehr einfach festgestellt werden. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.
6.	Art. 19 Abs. 1	Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller	Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht.

Nr.	Artikel	Antrag	Begründung / Bemerkung
		erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation von Teilnehmenden.	<p>Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des Schweizer Datenschutzgesetzes, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch der Schutz der Schweizer Kundschaft massiv beeinträchtigt wird. Datenschutzfreundliche Unternehmen werden bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.</p> <p>Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Dies wahrt nicht nur den Datenschutz, sondern schützt auch die Wettbewerbsfähigkeit von KMU, stärkt den Innovationsstandort Schweiz und die digitale Souveränität unseres Landes.</p>
7.	Art. 18	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.
8.	Art. 19 Abs. 2	Ersatzlose Streichung zugunsten bestehender Regelung	Eine Überwachung von Kunden durch FDA, ob diese die neuen Vorgaben der VÜPF zu WLANs einhalten (Art. 19 Abs. 2 Rev.VÜPF), und erst recht die dazu gelieferte Erklärung im erläuternden Bericht, wonach die FDA die Identifikation der WLAN-Nutzer vorzunehmen hätten, ist weder gesetzeskonform noch zumutbar (siehe vorstehend). Art. 19 Abs. 2 ist ersatzlos zu streichen.
9.	Art. 21 Abs. 1 lit. a	Streichung	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.
10.	Art. 22	beibehalten	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.
11.	Art. 11 Abs. 4	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.
12.	Art. 16b	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.
13.	Art. 31 Abs. 1	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.
14.	Art. 51 und 52	beibehalten	Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.
15.	Art. 60a	Streichung des Artikels	<p>Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen.</p> <p>Art. 60a VÜPF (Erläuterung Bundesrat: «...lediglich redaktionelle Änderungen....») sieht vor, dass Fernmeldedienstanbieterinnen über einen rückwirkenden Zeitraum von 6 Monaten alle Ziel-IP-Adressen liefern müssen, welche ihre Kunden besucht haben. Damit wird einerseits das Surfverhalten der gesamten schweizerischen Bevölkerung anlasslos und völlig unverhältnismässig ausspioniert. Andererseits wird die klare Vorgabe des BÜPF umgangen, das nur die Speicherung von Randdaten, aber nicht die Speicherung</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>von Inhaltsdaten vorsieht.</p> <p>Die geplante Überwachung des Internetverkehrs führt zu einer Überwachung, wer im Internet welche Adressen besucht hat. Dies geht zweifellos über die Schranken der gesetzlichen Regelung hinaus, dies insbesondere nachdem bereits die Aufzeichnung reiner Randdaten höchst umstritten und Gegenstand laufender Gerichtsverfahren ist. Hinzu kommt folgendes: Während bislang die Überwachung einer IP-Adresse nur im Rahmen einer sog. Echtzeit-Überwachung zulässig war, welche entsprechende Bewilligungen durch ein Gericht erforderte, muss neu nur noch ein einfaches Auskunftsbegehrten durch die zuständige Behörde genehmigt werden. Die Abfragen erfolgen automatisiert.</p> <p>Art. 60a sieht weiter vor, dass bei nicht exakt zuordenbaren IP-Adressen die kompletten Listen aller Nutzerinnen und Nutzer zu liefern ist. IP-Adressen sind ein rares Gut. Alle FDA teilen diese den Nutzenden im Millisekunden-Takt zu. Da die Zeitstempel der Systemanbieter nicht immer übereinstimmen, sind diese IP-Adressen nicht immer eindeutig einem Nutzenden zuzuordnen. Neu müssen Provider nun komplettte Listen aller Nutzenden liefern. Dies bringt Zehntausende in den Fokus von Überwachungsbehörden, was auf eine Art Rasterfahndung nach Delikten über grosse Teile der Bevölkerung hinausläuft. Entdecken Strafverfolger dabei zufälligerweise etwas, können sie umgehend Strafverfahren einleiten.</p> <p>Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde sodann gemäss Bericht gezielt auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten.</p> <p>Art. 60a ist zu streichen.</p>
16.	Art. 42a und Art. 43a	Streichung des Artikels	<p>Sowohl Art. 42a als auch Art. 43a fordern die Abrufbarkeit des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Nicht nur gilt auch hier wieder die Limite von 5'000 Nutzern, was somit fast die gesamte AAKD-Landschaft der Schweiz flächendeckend umfasst, sondern solche Abfragen sollen nun auch durch eine einfach «IR_» Abfrage gemacht werden können, welche im Gegensatz zu den «HD_»-Abfragen und den «RT_»-Überwachungen ohne weitere juristische Aufsicht automatisiert abgerufen werden können, obwohl es sich auch hier um das Abrufen einer IP-Adresse in der Vergangenheit handelt, genau wie bei den «HD_» abfragen, welche deutlich strenger reglementiert sind. Es ist nicht nachvollziehbar und verletzt aus unserer Sicht die gesetzliche Grundlage des BÜPF, dass Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber.</p> <p>Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser Automatisierten Auskünfte ergibt. Durch das Fehlen solcher Limiten könnte daher z.B. alle 5 Minuten eine</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>solche Anfrage automatisiert gestellt werden. Zunächst können sich dadurch lähmende Kosten für die betroffenen AAKD ergeben. Sodann können die Anfragen an ein automatisiertes Auskunftssystem gestellt werden, und es können auf diese Weise viele der Informationen welche ursprünglich über die juristisch sichereren HD_ und RT_Auskunfts-/Überwachungstypen liefern, neu über den rechtlich unsicheren IR_- Typ eingeholt werden. IR_59 und IR_60 ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne dass sie den benötigten Kontrollen dieser invasiven Überwachungsarten unterliegen würden.</p> <p>Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind, wie dies das BÜPF vorsieht.</p> <p>Die beiden Artikel sind daher vollumfänglich zu streichen.</p> <p>Diese neue Regelung und der zugehörige erläuternde Bericht sind im Übrigen eklatante Beispiele für die eingangs bemängelte überaus verwirrende und unverständliche Darstellung von Verordnungstext und erläuterndem Bericht.</p> <p>Im erläuternden Bericht steht auf S. 39 wörtlich:</p> <p><i>«In Absatz 1 sind die zu liefernden Angaben geregelt. Gemäss Buchstabe a ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin der oder dem Teilnehmenden einen solchen zugeteilt hat. Der «eindeutige Dienstidentifikator» gemäss Buchstabe b bezeichnet den Fernmelde- oder abgeleiteten Kommunikationsdienst, auf den sich die Antwort bezieht, eindeutig im Bereich der Anbieterin. In Buchstabe c werden die zu liefernden Angaben über den Ursprung der Verbindung bei der letzten zugriffsrelevanten Aktivität aufgezählt. Diese Angaben können für die Identifikation der Benutzerinnen und Benutzer nützlich sein.»</i></p> <p>Der Leser bzw. die Leserin urteile selber über die Verständlichkeit.</p> <p>Folgende Begriffe sind auch für den fachkundigen Leser nicht nachvollziehbar, bzw. es stellen sich folgende Verständnisfragen:</p> <ul style="list-style-type: none"> - Eindeutiger Identifikator: Was ist gemeint? Ist die Kundennummer des Internetproviders gemeint? Oder jene des genutzten dritten Fernmeldedienstes oder abgeleiteten Kommunikationsdienstes? Wie soll der Internetprovider überhaupt an diese Daten herankommen? - Eindeutiger Dienstidentifikator: Muss der Internetprovider eine Liste aller möglichen durch seine Kunden im Internet genutzten Kommunikationsdienste führen und aufzeichnen, muss er zudem aufzeichnen welcher Kunde welchen Dienst wann genau genutzt hat? Woher hat er diese Liste?

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Wie kann er herausfinden, ob ein Kunde gerade einen bestimmten Dienst nutzt? Gilt dies auch für ausländische Dienste? Nur für AAKD, für ausländische Fernmeldedienste, oder für alle Internetangebote weltweit? Der erläuternde Bericht bleibt hier völlig unklar.</p> <ul style="list-style-type: none"> - Was ist mit «Antwort» gemeint? Die Antwort des Servers des abgeleiteten Kommunikationsdienstes, den der Kunde besucht hat, oder die Antwort des Kundengeräts auf eine Nachricht von diesem Kommunikationsdienst? - Was ist mit «eindeutig im Bereich der Anbieterin» gemeint? Die Formulierung ist auch hier unverständlich. - Wie soll man sich eine «Antwort von einem anderen Fernmeldedienst» vorstellen? Muss ein Internetprovider die Herkunft sämtlicher auf seinem Netz eintreffenden Datenpakete aufzeichnen und dem Dienst ÜPF auf Anfrage diese Aufzeichnungen herausgeben? Wie soll die gigantische Masse an Daten, die durch ein solches Logging anfällt, durch die Internetprovider gemanaged werden? - Was ist mit «letzter zugriffsrelevanter Aktivitäten» gemeint? Geht es hier um die durch Kunden des Internetproviders aufgerufenen AAKD und andere Internetangebote? Wie soll der Internetprovider wissen, ob eine durch den Kunden aufgerufene IP-Adresse zu einem überwachungspflichtigen AAKD gehört, oder allenfalls zu einem nicht überwachungspflichtigen Dienst? Muss er einfach den ganzen Verkehr aufzeichnen? Wie weit zurück gehen die «zugriffsrelevanten» Aktivitäten? Müssen alle Daten für sechs Monate aufbewahrt werden? - Abgesehen davon: Wo wäre die gesetzliche Grundlage im BüPF für die vorgesehene inhaltliche Überwachung des Internetverkehrs? Das BüPF selber regelt bisher ausschliesslich die Überwachung der Randdaten, nicht aber von Inhaltsdaten, und spätestens dann, wenn Randdaten en passant auch Auskunft über die vom Kunden abgerufenen Inhalte geben, handelt es sich dabei um Inhaltsdaten, deren Sammlung erst recht gesetzes- und verfassungswidrig wäre, nachdem schon das Sammeln reiner Randdaten als menschenrechtswidrig taxiert wurde.
17.	50a	Artikel streichen	<p>Art. 50a sieht neu vor, dass Anbieter verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Diese Pflicht gilt nicht mehr nur für FDA (Art. 26 BüPF) oder ausnahmsweise für ausgewählte AAKD von hoher wirtschaftlicher Bedeutung (Art. 27 BüPF), sondern soll nun vorgabemässig und ohne Differenzierung auf sämtliche Anbieter mit mehr als 5'000 Teilnehmern angewendet werden, womit wohl fast die gesamte Schweizer AAKD-Branche betroffen ist (kaum ein Produkt ist lebensfähig mit weniger als 5000 Teilnehmern).</p> <p>Dies stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar.</p> <p>Diese Ausweitung ist nicht nur unverhältnismässig, sondern gefährdet aktiv nahezu die gesamte Schweizer IT-Branche: Indem de facto alle Anbieter vorgabemässig gezwungen werden, ihre</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Verschlüsselungssysteme für Behörden jederzeit entschlüsselbar zu gestalten, entstehen enorme Sicherheitsrisiken, denn Verschlüsselung ist wie eine Eierschale: Unversehrt ist sie stark, aber der kleinste Riss führt zu einer erheblichen Schwächung. Die betroffenen Systeme werden durch den vom Verordnungsgeber nun verpflichtend vorgesehenen Einbau von Hintertüren anfälliger für Hackerangriffe, Datenmissbrauch und Spionage. Dies widerspricht Art. 13 BV und dem diesen konkretisierenden Datenschutzgesetz, das den Schutz personenbezogener Daten ausdrücklich durch wirksame technische Massnahmen – insbesondere Verschlüsselung – vorschreibt. Eine durch den Anbieter aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung in jedem Fall.</p> <p>Genau eine solche Schwächung der Verschlüsselung wurde kürzlich vom Europäischen Gerichtshof für Menschenrechte im Fall PODCHASOV gegen Russland (33696/19) als Verstoss gegen Grundrechte gewertet. Art. 50a verstösst somit auch gegen geltendes Völkerrecht.</p> <p>Nebst diesem Verstoss gegen das Völkerrecht wird aber auch das Gebot der Verhältnismässigkeit aus Art. 36 BV nicht eingehalten, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördararbeit steht. Wie bereits bei Art. 16e, Art. 16f und Art. 16g erwähnt, müssen zuerst die einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.</p> <p>Zusätzlich, und wie bereits bei Art. 16d erwähnt, verhindert Art. 50a die effektive Erbringung von VPN-Diensten. Bei solch einem VPN kontrolliert der Betreiber sowohl den Eingangs- als auch den Endpunkt. Da die Kommunikation vom Endpunkt zu einer Webseite aufgrund der vorherrschenden Struktur im allgemeinen Internet nicht End-zu-End-Verschlüsselt erfolgen kann, werden schon kleine VPNs (mit 5000 Nutzern) dazu gezwungen ihre eigene Verschlüsselung zu entfernen und ihre Kunden zu überwachen. Da der Schutz der Privatsphäre der Nutzer*innen von VPNs just den Kernpunkt oder USP der Dienstleistung darstellt, werden Schweizer VPN-Anbieterinnen hierdurch am internationalen Markt übermässig benachteiligt, ja ihres eigentlichen Daseinszwecks beraubt.</p> <p>Wesentlich ist zudem, dass Anbieter von Mail- oder Messaging-Apps zwangsläufig die Nachricht in der App in einer menschenlesbaren Version anzeigen muss, und dass an dieser Stelle die End-zu-End-Verschlüsselung notwendigerweise bereits entfernt ist. Der Wortlaut von Art. 50a lässt entgegen sämtlichen Beteuerungen des Dienstes ÜPF bereits anlässlich der letzten Revision der VÜPF weiterhin</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>offen, ob eine Entfernung der Verschlüsselung auch an dieser Stelle gefordert werden können soll. Angesichts der seit Jahren erkennbaren Tendenz der Schweizer Überwachungsbehörden, die Anwendbarkeit des Überwachungsrechts laufend weiter auszudehnen und sich dabei nur durch Gerichte bremsen zu lassen, ist bei dieser Gelegenheit erneut die Klarstellung zu fordern, wonach die Entfernung von Verschlüsselungen, die erst in der Sphäre des Benutzers angebracht werden (wenngleich auch durch Software der Anbieterin) nicht verlangt werden darf. Dies ist zumindest im erläuternden Bericht zu erwähnen. Der erneute Verzicht wäre nichts anderes als eine Einladung an die Überwachungsbehörden, die Einführung einer offensichtlich illegalen und vom BÜPF keineswegs vorgesehenen «Chatkontrolle» auf dem «Auslegungsweg» vorzunehmen.</p>

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Artikel	Antrag	Begründung / Bemerkung	
VD-ÜPF / OME-SCPT / OE-SCPT			
Art. 14 Abs. 3 VD-ÜPF	Streichung	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit 5000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Absatz ist daher ersatzlos zu streichen.	
Art. 14 Abs. 4 VD-ÜPF	Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten.	Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der Unterworfenen AAKD massiv. Dies ist wie beschrieben weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.	
Art. 20 Abs. 1 VD-ÜPF	Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.	

Consultation on the partial revisions of the SPTO and OME-PTSS

Date	May 5, 2025
Office	Wire Swiss GmbH Untermüli 9 Zug, Zug 6300, CH
Contact person for questions (Name/phone/e-mail)	Florian Frese +49 162 2605492 florian.frese@wire.com

Position Paper on the Revision of the Ordinance on the Surveillance of Correspondence by Post and Telecommunication (OSCPT) and Its Impact on Derived Communication Service Providers (DSPs)

May 2, 2025, Wire

Executive Summary

The proposed revisions to the Swiss Ordinance on the Surveillance of Correspondence by Post and Telecommunication (OSCPT) would impose disproportionate surveillance and data retention obligations on Derived Communication Service Providers (FSCDs). These changes—particularly the creation of new provider categories based on lower thresholds for user numbers or revenue—threaten to undermine Switzerland’s position as a hub for digital innovation, infringe on international norms for privacy and human rights, and create technical and economic burdens without demonstrable benefits in fighting crime.

This paper outlines Wire’s position on why these revisions should be reconsidered, focusing on four core arguments:

- 1. Technical and Economic Burden on DSPs**
 - 2. Lack of Proportionality and Efficacy in Crime Prevention**
 - 3. Incompatibility with European and International Legal Norms**
 - 4. Risk of Flight of Swiss Digital and Technology Businesses**
-

1. Technical and Economic Burden on DSPs

The new classification system, which subjects DSPs with more than 1 million users or CHF 100 million in revenue to heightened obligations, fails to recognize the fundamental differences between traditional telecom operators and modern DSPs. Derived services, such as Wire, ProtonMail, and Threema, are often end-to-end encrypted and decentralized, making it technically infeasible—or at least cost-prohibitive—for them to comply with such obligations without redesigning core systems. In the case of Wire, our technical assessment is that our systems architecture, because it is expressly designed to minimize metadata collection for security and privacy purposes, is highly incompatible with long-term collection and retention of

extensive per-user metadata for the over 12 million users on our platform, many of whom utilize Wire on multiple devices.

Implications:

- **Engineering Costs:** For many DSPs, compliance would require extensive architectural changes, undermining the integrity of privacy-preserving designs. The costs and implementation uncertainties are extensive enough that they are impractical for many DSPs, including Wire.
- **Operational Disruption:** Smaller or medium-sized DSPs nearing the user or revenue thresholds may face abrupt changes in their compliance obligations, creating legal uncertainty and operational instability.
- **Competitive Disadvantage:** Foreign competitors not subject to such rules would gain a market advantage, threatening the viability of Swiss-headquartered DSPs.

2. Lack of Proportionality and Efficacy in Crime Prevention

There is little evidence that the surveillance requirements proposed will materially aid in crime reduction or intelligence gathering. The attempt to make DSPs responsible for retaining extensive metadata (referred to as “marginal data”) in hopes of being able to find criminals is based on a misunderstanding of the utility of the metadata from DSPs as compared to metadata collected by traditional, facilities-based telecom providers.

Internet-Based Communications vs. Facilities-Based Providers:

It is important to note that there is often confusion about what is feasible in terms of tracing vital information about users, depending on the nature of the service provided. Users of Internet-based communication services are not traceable in the same way as users of traditional telecom networks, where physical infrastructure and subscription data are tightly linked. The connectivity between DSPs and their users is highly virtualized from physical infrastructure. DSPs operate on shared, global Internet infrastructure, which includes many thousands of different Internet Service Provider links that are shared by literally billions of different Internet users, cloud platforms and Content Distribution Networks (CDNs). The very nature of Internet addresses allows them to be used without being fixed to particular physical location. Users can connect from virtually anywhere via public Wi-Fi, Internet Cafes, and can easily disguise their IP addresses in multiple ways, for example by utilizing VPNs or by connecting via ISPs that are permissive in allowing communications from unknown IP addresses.

This is fundamentally and critically different from the interconnected relationship of users and facilities-based telecom providers, where users are directly and provably connected to

equipment owned and operated by the provider, and traffic to and from user devices can be traced across multiple pieces of equipment in that provider's network.

Criminals are Highly Adept at Exploiting the Anonymity Afforded by the Internet

Any serious criminal or nation-state organization that intends to evade detection can easily do so on the Internet. These individuals and organizations are technically versed on the many ways the greater Internet allows them to obscure or disguise their location and identity. For example, a criminal organization can take over idle IP address blocks using BGP route hijacking, utilize burner phones with hacked eSIMs, route traffic over the [TOR network](#), or connect via VPNs to easily make any IP address and supposed geolocation data that presents to a DSP completely useless for crime-fighting purposes.

What this means is that the heavy burden of carrying months of extensive metadata does not materially improve law enforcement efforts. And in cases where individuals under investigation have not taken such evasive measures, the basic operational metadata that DSPs maintain to run their services is sufficient to aid those investigations. Thus, the newly proposed requirements are not proportional to the utility of the expanded data collection.

Overreach and Cybersecurity Risk:

The mandatory collection and storage of extensive metadata on millions of users not only poses privacy concerns but also creates a substantial cybersecurity risk. Centralizing sensitive communication logs, usage patterns, and access data makes DSPs high-value targets for cybercriminals and foreign intelligence services. Very large volumes of collected metadata, if compromised, be utilized by adversaries to aid their illicit aims, and in the process could create greater operational risks that could undermine DSPs' ability to cooperate with law enforcement at all.

3. Incompatibility with EU and International Legal Norms

Switzerland, though not an EU member, has historically aligned its digital and privacy laws closely with the EU to maintain interoperability and trust in its services. The proposed changes deviate significantly from recent rulings from 2014 to 2020 by the European Court of Justice (e.g., Cases C-293/12, C-594/12, C-623/17, C-511/18, C-512/18, C-520-18), where equivalent directives on data retention were annulled due to the fact that they infringed the right to privacy and personal data protection.

Risks:

- **Legal Isolation:** Divergence from EU norms could reduce data-sharing arrangements with European partners and hurt cross-border cooperation.

- **Privacy Conflicts:** Obligations to collect and share data may violate users' rights under the European Convention on Human Rights.
 - **Regulatory Fragmentation:** Tech companies operating in multiple jurisdictions could be forced to fragment their systems or abandon the Swiss market altogether.
-

4. Risk of Flight of Swiss Digital and Technology Businesses

Switzerland's reputation as a bastion of privacy and digital freedom has helped attract innovative tech firms and talent. This revision would reverse that trend, pushing both start-ups and established DSPs to relocate to more privacy-friendly jurisdictions.

Economic Impacts:

- **Brain Drain:** Developers and technologists may seek environments where their work in privacy-enhancing technologies is not criminalized or undermined.
 - **Loss of Investment:** Venture capital and international partnerships may dry up in response to regulatory uncertainty, especially given the conflict with EU laws.
 - **Damage to Switzerland's Brand:** Swiss neutrality and privacy are key to the country's identity in the digital space. This law undermines that brand value, with long-term implications.
-

Conclusion

The revised OSCPT undermines fundamental privacy protections, places an unrealistic and costly burden on derived communication service providers, and damages Switzerland's credibility as a global leader in digital rights. The Federal Council should suspend the planned revisions and instead initiate an inclusive dialogue with stakeholders—technical experts, legal scholars, DSP representatives, and civil society—on how to balance security and privacy in a technically feasible, economically sustainable, and legally compliant manner.

Recommendation:

The proposed revisions should be withdrawn. A new framework should be developed that is:

- Technologically sound and aligned with the Internet-based communication realities of DSPs
- Proportionate and evidence-based in its approach to crime prevention
- Harmonized with EU and international human rights standards
- Supportive of innovation and the growth of Swiss technology businesses

Vernehmlassung zu den Teilrevisionen der VÜPF und der VD-ÜPF

Datum	05. Mai 2025
Unternehmen	Suisse-digital - Verband für Kommunikationsnetze
Kontaktperson bei Fragen (Name/Tel./E-Mail)	Fürsprecher Stefan Flück, Leiter Rechtsdienst 031 328 27 28, stefan.flueck@suisse-digital.ch

Allgemeine Bemerkungen:

Wir begrüssen grundsätzlich die Teilrevisionen der VÜPF und der VD-ÜPF

JA NEIN

Suissedigital ist der Dachverband der Schweizer Telekommunikationsnetzunternehmen und vertritt die Interessen von ca. 180 privatrechtlich oder öffentlich-rechtlich organisierten Unternehmen verschiedener Grösse, die lokal, regional oder landesweit Telekommunikationsinfrastrukturen besitzen und betreiben und darüber verschiedene Fernmelde- inklusive Radio- und Fernsehdienste erbringen. Die Bereitstellung dieser Fernmeldedienste erfolgt in arbeitsteiligen Prozessen unter Mithilfe technischer Lieferanten, wobei je nach Grösse und Struktur der Unternehmen in unterschiedlichem Ausmass und unterschiedlicher Organisation auf Dienste und Produkte von Dritten (Dienstleister) zurückgegriffen wird. Fördermitglieder bei Suissedigital erbringen Dienstleistungen im Zusammenhang mit dem Betrieb der Mitglieder-Kommunikationsnetze. Diese B2B-Dienstleistungen reichen von der Beratung über die Projektabwicklung bis hin zur Bereitstellung und zum Betrieb von Netzkomponenten (Leitungen, Netzwerkkontenpunkte, etc.).

Die drei grössten Organisationen von Suissedigital sind die Sunrise Communications AG (nachfolgend «Sunrise»), der Quickline-Verbund sowie in der französischen Schweiz der net+-Verbund. Bei der überwiegenden Mehrheit der Mitglieder von Suissedigital handelt es sich nach der überwachungsrechtlichen Terminologie um sogenannte Anbieterinnen mit reduzierten Überwachungspflichten. Ein Mitglied, die Sunrise, betreibt ein Mobilfunknetz.

Unsere Mitglieder sind FDA nach FMG und bieten keine OTT-Kommunikationsdienste im Sinne der Erläuterungen zur VÜPF-Teilrevision an, d.h. keine alleinstehenden E-Mail- und Messenger-Dienste ohne Internetzugang. Unsere Stellungnahme konzentriert sich daher in erster Linie und im Rahmen der Betroffenheit unserer Mitglieder auf die vorgeschlagenen Änderungen bezüglich FDA und geht nur am Rande auf die Änderungen bezüglich AAKD ein.

Auch nach der Überarbeitung der Verordnungssystematik ist die angepasste VÜPF (nachfolgend E-VÜPF) inkl. Erläuterungsbericht schwer zu lesen und zu verstehen. Für Unternehmen und KMU ohne spezialisierte Rechts- und Fachabteilung ist es daher schwierig, die konkreten Anforderungen und Handlungsanweisungen nachvollziehen und erfassen zu können. Diese schwere Lesbarkeit von Verordnung und Erläuterungen stehen dem erklärten Ziel entgegen, die Ausführungsvorschriften KMU-freundlich zu machen.

Im Übrigen verweisen wir auf die Stellungnahme unseres Mitglieds Sunrise insbesondere auf die Ausführungen zu den neuen Auskunfts- und Überwachungstypen und unterstützen die dortigen Vorbringen integral. Keine Bemerkungen haben wir zu den geplanten Änderungen der VD-ÜPF.

Suissedigital lehnt die Vorlage in Teilbereichen ab. Diese sind zu überarbeiten. Unsere Hauptkritik betrifft die folgenden Revisionspunkte (mit unseren unten tabellarisch aufgeführten Anträgen):

- I) Die Mitberücksichtigung telekommunikationsfremder Umsätze bei der Bestimmung des massgeblichen Jahresumsatzes zur Einstufung als FDA mit reduzierten Pflichten (vgl. nachfolgend zu Art. 16b E-VÜPF);
- II) die unklare und offene Begriffsdefinition der FDA (vgl. nachfolgend zu Art. 16a E-VÜPF);

III) die Kriterien zu den zu «überwachenden» öffentlichen WLAN-Zugängen von PZD (vgl. nachfolgend zu Art. 16h E-VÜPF) sowie

IV) die zu kurz bemessenen Umsetzungsfristen für die neuen Auskunfts- und Überwachungstypen.

Die Vorlage widerspricht dem erklärten Ziel, die Überwachungspflichten klar voraussehbar und KMU-freundlich auszugestalten sowie die finanzielle Belastung für KMU gering zu halten. Stattdessen führen die Änderungen im Ergebnis zu einer kostspieligen Ausweitung der Überwachung. Dies gilt im Übrigen auch in Bezug auf die AAKD, wo die Schwelle für ein Upgrade der Mitwirkungspflichten gesenkt werden soll (vgl. dreistufige Regelung in Art. 16e-16g E-VÜPF) und damit viele AAKD strengeren Mitwirkungspflichten unterstellt werden würden.

Zielsetzung der Revision

Laut dem Begleitschreiben zur Vernehmlassungseröffnung sollen durch eine Teilrevision der VÜPF die Definitionen bestimmter Kategorien von Mitwirkungspflichtigen (MWP) bei der Überwachung des Fernmeldeverkehrs näher umschrieben werden: Die Anbieterinnen von Fernmeldediensten (FDA gemäss Art. 2 Bst. b BÜPF), die Anbieterinnen abgeleiteter Kommunikationsdienste mit neuen Unterkategorien (AAKD gemäss Art. 2 Bst. c BÜPF) sowie die Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen (PZD gemäss Art. 2 Bst. e BÜPF). Diese Konkretisierungen der MWP stützen sich auf die letzte FMG-Revision, wo I) in Bst. b von Art. 2 BÜPF die Referenz auf das Fernmeldegesetz gestrichen und II) ein neuer Absatz 2 in Art. 2 BÜPF eingefügt wurde, wonach der Bundesrat die Kategorien insbesondere der FDA, der AAKD und der PZD näher umschreiben kann. Es ist geplant, die BÜPF-Änderungen mit der vorliegenden Teilrevision der VÜPF und der VD-ÜPF in Kraft treten zu lassen. Zudem sollen in der VÜPF drei neue Auskunfts- und zwei Überwachungstypen geschaffen werden. Diese Änderungen ziehen auch Anpassungen der VD-ÜPF nach sich.

Bei den Konkretisierungen der MWP gehe es darum, dass die Zuordnung einfach ersichtlich werde und somit die auferlegten Pflichten für die betroffenen Unternehmen klar ableitbar würden. Die VÜPF soll für MWP, insbesondere FDA und AAKD, klare Definitionen vorsehen, damit leicht ersichtlich sei, in welche Kategorie eine Anbieterin falle und welche Pflichten und Kosten auf sie zukommen würden (Teilrevision VÜPF, FD-ÜPF, Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahren vom 08.01.2025, Kap. 1.1, Seite 3, erster Absatz, Seite 4, zweiter Absatz und Kap. 5.1, Seite 53, erster Absatz). Weiter soll die vorliegende Revision die Ausführungserlasse KMU-freundlicher machen, weshalb der Bundesrat laut Erläuterungsbericht in Erfüllung des Postulats 19.4031 (von Albert Vitali) Handlungsbedarf in der VÜPF sieht. Die Änderungen sollen pragmatisch sein, um die finanzielle Belastung der KMU gering zu halten (Erläuternder Bericht, a.a.O., Kap. 5.1, Seite 53, erster Absatz).

Anmerkungen AAKD Entfernung von Verschlüsselungen

Die von den Anbieterinnen angebrachten Verschlüsselungen sollen neu generell, also auch von allen AAKD, auf Aufforderung hin entfernt werden müssen (vgl. Art. 50a E-VÜPF). Die Möglichkeit, den Kommunikationsverkehr an bestimmten Punkten ausleiten zu können, bedeutet aber nichts anderes, als dass von Gesetzes wegen nun neu in allen von AAKD verwendeten Verschlüsselungsanwendungen «Hintertüren» einzubauen sind. Dies schwächt jedoch das

gesamte System und macht es anfälliger für Hackerangriffe und unerlaubte Datenzugriffe. Aus rechtsstaatlicher Sicht mag dies zur Aufklärung von Verbrechen gerechtfertigt sein; es fragt sich aber, wie diese ausgebauten Zugriffsmöglichkeiten wettbewerbsneutral auf alle in der Schweiz zugänglichen, also auch auf ausländische E-Mail- und Messengerdienste angewendet werden sollen. Die entsprechenden Dienste werden heutzutage oft grenzüberschreitend aus dem Ausland erbracht. Eine Regelung, die nur bei den in der Schweiz ansässigen Anbieterinnen durchgesetzt werden kann, schwächt im Ergebnis die hiesige Wirtschaft. Weiter muss erwähnt werden, dass Verschlüsselungsprogramme einfach erhältlich und benutzerseitig installierbar sind, so dass die für die Strafverfolgung relevante Kommunikation schliesslich auf selbst erstellte Verschlüsselungsmethoden oder schlicht auf ausländische Anbieter ausweichen wird. Damit wird die strenge Regelung also kaum den erwarteten Erfolg zeitigen und im Ergebnis lediglich die Geschäftsmodelle der schweizerischen Anbieter von Sicherheitskommunikation untergraben, was letztlich zu einer Schwächung des Innovations- und Wirtschaftsstandorts Schweiz führen wird.

Bemerkungen zu einzelnen Artikeln der VÜPF

Artikel	Antrag	Begründung / Bemerkung
VÜPF		
16a	<p>In Absatz 1 ist Bst. a zu streichen:</p> <p>1 Als FDA gilt für den betreffenden Dienst, wer einen Fernmeldedienst erbringt. Fernmeldedienste sind:</p> <p>a. Betrieb eines öffentlichen Fernmeldenetzes;</p> <p>b. direkter Zugangsdienst zu einem öffentlichen (...)</p>	<p>Im Zusammenhang mit der Einschränkung der Registrierungspflicht für in der Schweiz tätige FDA und der Ungleichbehandlung insbesondere gegenüber ausländischen OTT-Anbieterinnen nahm das Parlament anlässlich der letzten FMG-Revision vom 22. März 2019 auch eine Anpassung im persönlichen Geltungsbereich des BÜPF vor. Der Bundesrat begründete diese Anpassung mit dem Umstand, dass der Begriff der FDA nach FMG im Gegensatz zum BÜPF weiter gefasst sei und auch sogenannte OTT-Anbieterinnen mitumfasse. Denn das BÜPF kennt seit der Revision vom 18. März 2016 nebst den FDA auch die MWP-Kategorie der AAKD.</p> <p>Mit der Streichung der Referenz auf das FMG durch den Gesetzgeber ging jedoch keine Änderung der Begriffsmerkmale einer FDA einher. Dazu lassen sich keine Hinweise in der Botschaft sowie den Debatten im Parlament finden. Die Referenz wurde deshalb gestrichen, weil nach Meinung des Bundesrats in der Gruppe der FDA nach FMG, die AAKD bereits enthalten sind und diese ansonsten im persönlichen Geltungsbereich des BÜPF doppelt adressiert wären, nämlich einmal als FDA nach FMG und einmal als AAKD nach BÜPF. Weiter hat das Parlament dem Bundesrat nicht die Kompetenz eingeräumt, den Begriff der FDA nach BÜPF in einem Ausführungserlass neu zu definieren, dies wäre verfassungsrechtlich auch gar nicht zulässig. Der Bundesrat sollte lediglich die Kategorien (im vorgegebenen Rahmen des BÜPF) näher umschreiben.</p> <p>So geht die VÜPF-Vorlage im Grundsatz auch, wie das FMG, von einem wirtschaftlich orientierten Anknüpfungsmerkmal beim Anbieten eines Fernmeldedienstes aus, indem ausgeführt wird, dass eine FDA nicht zwingend selbst physisch die fernmeldetechnische Übertragung durchführen müsse. Entscheidend sei, wer den Dienst anbiete und die Verantwortung für die fernmeldetechnische Übertragung der Informationen übernehme (Erläuternder Bericht, a.a.O., Kap. 3.1 zu Art. 16a E-VÜPF, Seite 13). Wer demnach für die Informationsübermittlung gegenüber einem Kunden vertraglich einsteht, gilt als FDA, unabhängig davon, wie dieser Informationstransport organisiert ist, ob die Infrastruktur dazu gemietet oder selber betrieben wird</p>

Artikel	Antrag	Begründung / Bemerkung
		<p>oder ob die Tätigkeit ganz oder teilweise an einen Dritten ausgelagert ist.</p> <p>Laut Art. 16a Abs. 1 Bst. a E-VÜPF soll nun aber bereits auch der <u>Betrieb</u> eines öffentlichen Fernmeldenetzes einen Fernmelddienst durch eine verpflichtete FDA nach BÜPF darstellen. Denn das Erbringen eines Fernmelddienstes beinhaltet zwei Komponenten, eine wirtschaftliche und eine technische. Und im Überwachungsrecht müsste [auch] auf die technische Ebene abgestellt werden (Erläuternder Bericht, a.a.O., Kap. 3.1, Seite 10, zweiter Absatz und Seite 9, dritter Absatz). Es ist daher anzunehmen, dass neu nun auch Dienstleister im Betrieb von Netzabschnitten, technischen Netzkomponenten, Teilsystemen, Nodes etc., einfach allem, was technisch für den Betrieb eines öffentlichen Fernmeldenetzes notwendig sein kann und allenfalls durch Dritte zur Verfügung gestellt und betrieben wird, zu Adressaten der mitwirkungsverpflichteten Tätigkeiten werden. Diese Erweiterung ist unnötig und widerspricht der Aussage im Erläuternden Bericht (S. 9), wonach für die Qualifikation als FDA entscheidend sei, wer einen Dienst anbietet und wer am Ende die Verantwortung für die fernmeldetechnische Übertragung von Informationen übernimmt. Folglich kann allein der Betrieb einer technischen Infrastruktur nicht zur Qualifikation eines FDA im Sinne des BÜPF führen.</p> <p>Diese Neuinterpretation der FDA geht über die vorgegebenen (und vom Parlament nicht abgeänderten) Begriffsmerkmale einer FDA nach BÜPF hinaus, ist somit nicht durch das Gesetz legitimiert und steht schliesslich auch in gravierendem Widerspruch zum kommunizierten Ziel der Revision, klar und voraussehbar zu definieren, wer den Mitwirkungspflichten gemäss BÜPF nun effektiv untersteht. Die Formulierung ist verwirrlt und bringt viel Rechtsunsicherheit mit sich. Dies ist vor dem Hintergrund des grundrechtlich geschützten Fernmeldegeheimnisses sehr heikel für die betroffenen Unternehmen, mit schwierig abschätzbaren Kosten verbunden und deshalb nicht vertretbar. Der Bundesrat würde damit die Kategorie der FDA nicht nur näher umschreiben, sondern geradezu eine neue Klasse von MWP schaffen. Bst. a von Art. 16a Abs. 1 E-VÜPF ist deshalb ersatzlos zu streichen.</p>
16b	<p>In Absatz 1 Bst. b ist Ziff. 2 umzuformulieren (und bestehende Regelung beizubehalten):</p> <p>b. keine der nachstehenden</p>	<p>Die neue Formulierung in Art. 16b Abs. 1 Bst. b Ziff. 2 E-VÜPF macht das Überwachungsrecht entgegen dem erklärten Ziel KMU-unfreundlicher, denn es könnten weitere Unternehmen, die mit ihren Fernmelddiensten (und abgeleiteten Kommunikationsdiensten) alleine</p>

Artikel	Antrag	Begründung / Bemerkung
	<p>Grössen erreicht: (...)</p> <p>2. Jahresumsatz in der Schweiz <i>mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten des gesamten Unternehmens</i> von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.</p>	<p>den Schwellenwert der CHF 100 Millionen nicht erreichen würden, statt lediglich unter die Duldungs- unter die vollen Mitwirkungspflichten der Überwachung gestellt werden. Die weiteren Geschäftsumsätze des <i>gesamten Unternehmens</i>, obschon diese keinen Zusammenhang zum Fernmeldeverkehr haben (<i>telekommunikationsfremder Umsatz</i>), sollen neu mitberücksichtigt werden, was die Überwachung in der Praxis ausweiten wird. Die vorgeschlagene Regelung ist weiter auch im Verhältnis zum Konzernatbestand in Abs. 2 unklar, es stellt sich nämlich die Frage, ob Abs. 2 eine Konkretisierung von Abs. 1 darstellt oder gar eigenständige Bedeutung zukommt. Sollen durch die Hervorhebung des <i>gesamten Unternehmensumsatzes</i> in Ziff. 2 von Art. 16 Abs. 1 Bst. b E-VÜPF neben den kontrollierten Unternehmen nach Abs. 2 neu allenfalls auch die Umsätze weiterer Einheiten einer Unternehmensgruppe miteinbezogen werden? Dies würde noch weniger Sinn ergeben und die Überwachung weiter ausweiten. Aufgrund dieser Überlegungen sollte die Wesentlichkeitsschwelle für reduzierte Überwachungspflichten unbedingt funktional mit dem Kriterium des <i>Umsatzes aus Telekommunikationsdiensten</i> verknüpft bleiben.</p> <p>Unter den Suissedigital-Mitgliedern befinden sich viele Querverbundunternehmen, die hauptsächlich nebst der Telekommunikation andere Versorgungsdienste leisten, wie die Versorgung mit Energie und Wasser. Unter Berücksichtigung der vorgeschlagenen Änderung wäre nicht mehr klar, ob diese bei entsprechendem Gesamtumsatz das Downgrade noch anrufen könnten.</p> <p>Beispielhaft dafür kann die St.Gallisch-Appenzellische Kraftwerke AG (www.sak.ch) mit ihrer Telekomabteilung genannt werden. Oder ein weiteres Beispiel ist die WWZ AG (www.wwz.ch), die hauptsächlich nebst den Telekommunikationsdiensten durch ihre Tochterunternehmung WWZ Telekom AG die Bevölkerung und Unternehmen des Kantons Zug und Umgebung mit Wasser und Energie versorgt: Mit einem jährlichen Gesamtumsatz von über CHF 300 Mio. könnte die WWZ AG als gesamtes Unternehmen nun neu den vollen Mitwirkungspflichten unterstehen, obschon der relevante Umsatz aus Telekommunikation klar unter CHF 100 Mio. liegt. Damit würde die Regelung aber gegen die Vorgaben von Art. 26 Abs 6 BÜPF verstossen, wonach FDA von geringer wirtschaftlicher Bedeutung von den vollen Mitwirkungspflichten zu befreien sind. Die Regelung hätte also eine Verschärfung und Ausweitung des Überwachungsrechts zur Folge und darf deshalb so nicht umgesetzt werden. Für die im Erläuternden Bericht erwähnten Schwierigkeiten bei der Ermittlung des massgeblichen anteiligen Umsatzes ist eine andere Lösung zu finden, beispielsweise könnte für FDA auf die</p>

Artikel	Antrag	Begründung / Bemerkung
		<p>entsprechenden Jahresumsätze gemäss Fernmeldestatistik des Bundes abgestellt werden. Weiter kann in diesem Zusammenhang auch unser Mitglied Energie Wasser Bern (www.ewb.ch) oder das Elektrizitätswerk der Stadt Zürich (www.ewz.ch) erwähnt werden, die einen Gesamtumsatz über dem Schwellenwert erzielen und u.a. auch Kommunikationsnetzdienstleistungen anbieten.</p> <p>Zusammen mit der unklaren Formulierung zu den unterstellten FDA in Art. 16a Abs. 1 E-VÜPF könnten diese Unternehmen nicht mehr ausschliessen, den vollen Überwachungspflichten als FDA zu unterstehen. Die Regelung würde die Überwachungspflichten ungerechtfertigterweise ausweiten, sie ist deshalb umzuformulieren und es ist materiell die bestehende Regelung beizubehalten.</p>
16d	Generelle Nennung von Online-speicherdiensten im Erläutern den Bericht ist zu streichen.	Laut Art. 2 Bst. c BÜPF ermöglichen dem Überwachungsrecht unterstellte AAKD-Dienste eine Einweg- oder Mehrwegkommunikation. Speicherdiene, die rein zum Speichern von Dateien oder kundenseitigen Applikationen zur Verfügung stehen und genutzt werden, beinhalten keine Kommunikationsmöglichkeiten im Sinne des Gesetzes, sie sind deshalb nicht als Beispiele für Dienste der AAKD in den Erläuterungen zu den Änderungen der VÜPF zu nennen.
16h	<p>Absatz 2 ist zu streichen:</p> <p>(...)</p> <p>² Ein öffentlicher WLAN-Zugang gilt als professionell betrieben, wenn kumuliert maximal mehr als 1000 Endbenutzerinnen und -benutzer alle von der gleichen Person gemäss Absatz 1 zur Verfügung gestellten öffentlichen WLAN-Zugänge nutzen können.</p>	<p>Wenn aktuell neben einer FDA ein technischer Dienstleister einen öffentlichen WLAN-Zugang einrichtet und unterhält, ist die Anforderung klar, dass die Nutzer des WLAN-Zugangs identifiziert werden müssen. Diese Anforderung ist bekannt und der Identifikationsprozess wird jeweils bereits im Projekt vorgesehen und dann mitimplementiert.</p> <p>Nach den neuen geplanten Kriterien wäre die Frage der Identifikationspflicht jedoch nicht mehr klar im Voraus zu beantworten. Die FDA wird keine Kenntnis darüber haben, ob bei einem bestimmten WLAN-Zugang die Identifikation der Nutzer zwingend ist, da ihr nicht bekannt ist, wie der Zugang resp. der eingesetzte Router konfiguriert ist (Kapazität). Sie hat auch keinen direkten Zugriff auf den Router, so dass sie nicht überprüfen kann, ob der Router potentiell für > 1'000 Clients eingerichtet ist oder nicht, und sie kann die Einstellungen auch nicht ändern.</p> <p>Zudem ist es technisch relativ einfach, einen Zugang potentiell für über 1'000 Nutzer zu öffnen. Dies lässt sich bereits mit einem handelsüblichen Router für den Privatkundenmarkt umsetzen. Dies hätte dann für die durch Art. 19 E-VÜPF verpflichtete FDA viel Rechtsunsicherheit zur Folge, weil die Voraussehbarkeit der bestehenden Pflicht nicht mehr gegeben wäre. Im Ergebnis würde die Änderung zu einer Ausweitung der Überwachung führen, da bei vielen</p>

Artikel	Antrag	Begründung / Bemerkung
		<p>WLAN-Zugängen, bspw. in Restaurants oder Hotels schon aus Gründen der Vorsicht ein Identifikationsprozess nachgerüstet werden müsste. Auch das wäre eine Massnahme, die in der KMU-Welt zu mehr Komplexität führen würde.</p> <p>Die Bestimmung ist ersatzlos zu streichen und die bestehende Regelung ist unverändert beizubehalten.</p>
19	<p>Absatz 2 ist umzuformulieren (und die bestehende Regelung beizubehalten):</p> <p>(...)</p> <p>² Die FDA haben bei professionell betriebenen öffentlichen WLAN-Zugängen, bei denen sie den Internetzugang erbringen, sicherzustellen, dass alle Endbenutzerinnen und -benutzer mit geeigneten Mitteln identifiziert werden.</p>	<p>Wer einen professionell betriebenen WLAN-Zugang Dritten/der Öffentlichkeit zur Verfügung stellt, sollte entsprechend der bisherigen Regelung für die Identifizierung der Endbenutzerinnen und -benutzer verantwortlich sein, da diese Person Dritten einen Internetzugang zur Verfügung stellt.</p> <p>Die FDA, welche den zugrundeliegenden Internetzugangsdienst erbringt, hat demgegenüber keine Kontrolle darüber, ob bei einem bestimmten WLAN-Zugang eine Identifizierung vorzunehmen ist oder nicht. Und es ist auch nicht ihre Aufgabe, ihre Kunden zu überwachen, ob diese die Vorgaben der Überwachung einhalten oder nicht. Die bisherige Regelung ist deshalb unverändert beizubehalten.</p>
27	<p>Absatz 2 ist umzuformulieren (und die bestehende Regelung beizubehalten):</p> <p>(...)</p> <p>² Das Auskunftsgesuch enthält bei natürlichen Personen jeweils das erste sowie mindestens ein weiteres Anfragekriterium des zugrundeliegenden Auskunftstyps, bei juristischen Personen jeweils den Namen und optional den Sitz.</p>	<p>Die Erweiterung der flexiblen Namenssuche auf juristische Personen ist aufgrund der Erfahrungen in der Praxis unnötig und würde auf Seiten der MWP nur unnötig Kosten für die technische Implementierung verursachen. Die bisherige Regelung ist unverändert beizubehalten.</p>

Artikel	Antrag	Begründung / Bemerkung
55a	<p>Der ganze Artikel ist ersatzlos zu streichen:</p> <p>Überwachungstyp RT_61_NA_CC-TRUNC_IRI: Echtzeitüberwachung von Randdaten (...)</p>	<p>Das Aussortieren gewisser IP-Pakete aus dem Inhalt eines Fernmeldeverkehrs gemäss Angaben der anordnenden Behörde stellt eine Aufgabe des Dienstes ÜPF dar (vgl. Art. 17 Bst. g BÜPF) und darf nicht auf die MWP abgewälzt werden. Die Regelung ist deshalb ersatzlos zu streichen.</p>
60a	<p>Der ganze Artikel ist ersatzlos zu streichen.</p> <p>Überwachungstyp HD_62_IP: rückwirkende Überwachung zum Zweck (...)</p>	<p>Der geplante Überwachungstyp ist unverhältnismässig und kommt einer verpönten «fishing expedition» gleich. Die Regelung ist deshalb ersatzlos zu streichen.</p>
74c	<p>Absätze 2 und 3 sind umzuformulieren:</p> <p>² Die FDA mit vollen Pflichten müssen Auskünfte gemäss den Artikeln 38a, 42a und 43a innerhalb von 6 12 Monaten nach Inkrafttreten dieser Änderung erteilen können.</p> <p>³ Sie müssen die Überwachungen gemäss Artikel 55a innerhalb von 12 18 Monaten und diejenigen gemäss Artikel 60a innerhalb von</p>	<p>Für die Umsetzung der neuen Auskunftstypen gemäss Art. 38a, 42a und 43a ist eine längere Übergangsfrist vorzusehen, da die entsprechenden Entwicklungs- und Implementierungsarbeiten komplex sind. Es ist mindestens eine Übergangsfrist von 12 Monaten vorzusehen.</p> <p>Obenstehend wird die Streichung der neuen Überwachungstypen gemäss Art. 55a und 60a E-VÜPF beantragt. Sollte dem nicht entsprochen werden, so ist mindestens eine Übergangsfrist von 18 Monaten für diese neuen Überwachungsmassnahmen vorzusehen, da diese teilweise von Grund auf in Zusammenarbeit mit externen Lieferanten neu entwickelt werden müssen.</p>

*Vernehmlassungsantwort zu den Teilrevisionen der VÜPF und der VD-ÜPF
gemäss Schreiben des EJPD vom 29. Januar 2025*

Datum	5. Mai 2025
Verfasser (Unternehmen)	Ronzani Schlauri Anwälte, Signaustrasse 33, 8008 Zürich
Kontaktperson bei Fragen (Name/Tel./E-Mail)	Prof. Dr. Simon Schlauri, Rechtsanwalt 044 500 57 22 schlauri@ronzani-schlauri.com MLaw Jonathan Messmer 044 500 57 23 messmer@ronzani-schlauri.com

Dieses Dokument geht an:

Eidgenössisches Justiz- und Polizeidepartement EJPD, ptss-aemterkonsultationen@isc-ejpd.admin.ch

Sehr geehrter Herr Bundesrat Jans, sehr geehrte Damen und Herren

Wir beziehen uns auf das am 29. Januar 2025 eröffnete Vernehmlassungsverfahren zu Teilrevisionen von VÜPF und VD-ÜPF und bedanken uns für die Möglichkeit einer Stellungnahme.

Wir lehnen die geplante Teilrevisionen der VÜPF und der VD-ÜPF in aller Deutlichkeit und vollumfänglich ab.

Im Bericht des Bundesrates zur aktuellen Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF und der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) ist zu lesen, dass die Revision im Wesentlichen auf die Anpassung der Verordnungen an die KMU-Freundlichkeit abziele. Ein grosser Teil der vorgeschlagenen Änderungen *verfolgt aber gerade das Gegenteil*.

Die Geschäftsgrundlagen von Schweizer Unternehmen wie Threema, Proton und anderer KMU, die weltweit einen hervorragenden Ruf als Anbieterinnen sicherer Kommunikationsdienste im Internet geniessen, drohen durch die Vorlage zerstört zu werden. Die Sicherheit des Internets in der Schweiz soll mit der Revision der Überwachung jeglichen Internetverkehrs regelrecht untergeordnet werden: «**Sicherheit vor Freiheit» ist das neue Paradigma**. Dieses zieht sich wie ein roter Faden quer durch diese völlig verunglückte Reform. KMU, die aus der Schweiz heraus Internet-Dienste anbieten («abgeleitete Kommunikationsdienste» in der Terminologie des Gesetzes), soll die Schweiz als Standort geradezu vergällt werden. Dies scheint denn auch zu gelingen: **Erste der betroffenen Unternehmen haben bereits angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen** (siehe Tages-Anzeiger vom 1. April 2025).

Ein derartiger Paradigmenwechsel, weg von KMU-Schutz und Überwachung mit Augenmass, hin zu knallharter Überwachung, die alle anderen Interessen unterordnet, wird durch das geltende Gesetz (BÜPF) keineswegs gestützt. Der Paradigmenwechsel widerspricht vielmehr geradezu dem Geist des ursprünglichen BÜPF, das Internetdienste, die in der Schweiz meist von KMU betrieben werden, vor der Implementierung teurer Überwachungsmassnahmen schützen wollte, und das eine austarierte Interessenabwägung vorsah zwischen Privatsphäre und Freiheit auf der einen Seite und staatlicher Überwachung auf der anderen Seite.

Entgegen dem im Begleitbericht zum vorgelegten Entwurf erklärten Ziel, die «finanzielle Belastung der KMU gering zu halten», stuft die Vorlage eine grosse Mehrheit der Schweizer Anbieterinnen von Internetdiensten in eine höhere Stufe auf, und zwingt sie neu auch in jenen Bereichen zu einer kostspieligen aktiven Überwachungstätigkeit, wo bisher nur eine KMU-freundliche Duldungspflicht bestand. Dies verschiebt das bisherige Gleichgewicht der Interessen zwischen Strafverfolgung und betroffenen Anbieterinnen in drastischer Weise zugunsten der betroffenen Anbieterinnen.

Die vorgeschlagenen Anpassungen bringen ganz erhebliche Risiken für den Innovations- und Wirtschaftsstandort Schweiz mit sich und erfüllen die Kernziele der Revision, die Entlastung von KMU, gerade nicht. Der Ruf der Schweiz als sicherer Hafen für vertrauenswürdige IT-Anbieter droht durch die Revision nachhaltig beschädigt zu werden. Deshalb lehnen wir die Revision vollumfänglich ab.

Auch **die Schweizer Armee** nutzt solche Dienste, wie beispielsweise Threema, und zwar gerade aufgrund des hohen gebotenen Sicherheitsstandards. Die Annahme dieser Revision, welche dieses Sicherheitsniveau gezielt untergraben will, verletzt damit indirekt auch das direkte Interesse der Schweiz an lokal betriebenen Hochsicherheitsanwendungen. Gerade in der heutigen Zeit, in der die Zuverlässigkeit der grossen US-Anbieter in ihrer Abhängigkeit von einer zunehmend erratisch agierenden US-Regierung mehr und mehr in Frage steht, erscheint dies als **inakzeptable Hochrisikostrategie**.

Nicht zuletzt ist mit Nachdruck darauf hinzuweisen, dass die Revision die Überwachung ganz allgemein stark ausweitet. Dies ist mit der durch den Gesetzgeber im BÜPF festgelegten, fein austarierten Interessenabwägung zwischen Freiheit und Privatsphäre der Einwohner der Schweiz einerseits und Sicherheit durch Überwachungsmassnahmen andererseits absolut nicht vereinbar. Die Revision entpuppt sich geradezu als eine Art Wunschkonzert für Überwachungsbehörden. Insbesondere ist künftig auch **eine komplette inhaltliche Überwachung des gesamten Internetverkehrs** der Schweiz vorgesehen. Dies ohne dass eine solche inhaltliche Überwachung durch die gesetzlichen Grundlagen des BÜPF in irgend einer Weise gedeckt wäre: Zulässig ist gemäss BÜPF einzig und allein die Überwachung von Randdaten des Fernmeldeverkehrs, und selbst die Zulässigkeit der in diesem Kontext angewendeten anlasslosen Vorratsdatenspeicherung von Randdaten ist bis heute umstritten und Gegenstand von Gerichtsverfahren, ja in der EU bereits höchstrichterlich als menschenrechtswidrig erkannt. Die durch die Verordnungsrevision eingeführte *Inhaltsüberwachung* ist in der Schweiz damit erst recht **offensichtlich illegal und verfassungswidrig**.

Abschliessend sei noch der Hinweis angebracht, dass wir die Gesetzgebungstechnik des Entwurfs für überaus schlecht halten. **Sowohl der Verordnungstext als auch der zugehörige erläuternde Bericht sind über weite Strecken höchst verwirrend und unverständlich formuliert**, unter anderem mit einer Vielzahl von Querverweisen, technischen Fehlern und unklarer Begrifflichkeit (für ein Beispiel hierfür siehe unten, Bemerkungen zu Art. 43a). Die Texte sind in dieser Form selbst für uns Fachleute über weite Strecken nicht zu verstehen, geschweige denn als Ganzes zu überblicken. Für KMU, die durch die Revision neu mit erheblich strengeren Pflichten konfrontiert werden, ist eine rechtskonforme Umsetzung dieser Vorlage daher ein schlicht aussichtloses Unterfangen.

Das Legalitätsprinzip gemäss Art. 5 Bundesverfassung fordert vom Gesetzgeber, dass Gesetzestexte für die Adressaten verständlich formuliert sind. Die Texte der Verordnungsrevision genügen dieser Anforderung offensichtlich in keiner Weise. Nur schon aufgrund der völlig fehlenden Verständlichkeit ist die Verfassungsmässigkeit der Revision insgesamt *höchst zweifelhaft*. Wir fordern nur schon deshalb einen Rückzug der vorgelegten Texte, eine komplette Überarbeitung zur Verbesserung der Verständlichkeit und eine erneute Auflage zur Vernehmlassung.

Mit freundlichen Grüßen

Prof. Dr. Simon Schlauri, Rechtsanwalt

Bemerkungen zu einzelnen Artikeln der VÜPF

Nr.	Artikel	Antrag	Begründung / Bemerkung
VÜPF / OSCPT / OSCPT			
0.	Alle Artikel	Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.	<p>Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kunden auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.</p> <p>Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.dgl. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.</p>
1.	16b, Abs. 1	Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.»	Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile, wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Anforderungen in Kauf nehmen.
2.	16c, Abs. 3	Streichung von lit. a «automatisierte Erteilung der Auskünfte (Art. 18 Abs. 2);»	Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Dies untergräbt rechtsstaatliche Prinzipien doppelt: Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>«natürliche» Schutzmechanismen gegen eine überschiessende, missbräuchliche oder zumindest unverhältnismässige Nutzung solcher Massnahmen durch die Untersuchungsbehörden.</p> <p>Der vorgesehene Umsetzungszeitraum von 12 Monaten für die rechtssichere Implementierung eines derart komplexen Systems völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.</p>
3.	Art. 16d	<p>Streichung von Online-speicherdiensten und VPN-Anbietern in der Auslegung</p>	<p>Eine klarere Definition des Begriffs AAKD ist begrüssenswert, doch die neue Auslegung gemäss erläuterndem Bericht geht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdiensten wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter, etc.) genutzt werden.</p> <p>Art. 2 lit. c BüPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug den gesetzlichen Rahmen sprengt. Onlinespeicherdiene sind deshalb aus Art. 16d zu streichen.</p> <p>Zudem anerkennt der erläuternde Bericht, dass VPNs zur Anonymisierung der Nutzer*innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Anbieter von VPNs sind daher ebenfalls aus dem Geltungsbereich von Art. 16d auszunehmen.</p>
4.	Art. 16e, Art. 16f und Art. 16g	<p>Streichung der Artikel und Beibehaltung der bestehenden Kriterien</p> <p>Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).</p>	<p>Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch diametral entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung. Dies daher, weil neu KMU bereits mit mehr als 5'000 Nutzern erfasst werden.</p> <p>Die Einführung von 5000 Nutzern als gesondert zu beurteilende Untergrenze verletzt aus unserer Sicht bereits Art. 27 Abs. 3 BüPF, denn 5000 Personen keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strenger Überwachungsmassnahmen, gerechtfertigt wären. 5000 Nutzer werden in der digitalen Welt vielmehr sehr rasch erreicht.</p> <p>Zusätzlich führt das Einführen eines «Konzerntatbestandes» in Art. 16f Abs. 3 zu massiven Problemen, da die Produkte nun nicht mehr für sich alleine eine bestimmte Grösse erreichen müssen, sondern die rele-</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>vanten Zahlen anhand des Umsatzes des Unternehmens, bzw. in Konzernverhältnissen sogar des Konzerns bestimmt werden. Vor allem bei Unternehmen mit Beteiligungsfirmen im Hintergrund fallen nun neu alle Dienstleistungen und Produkte automatisch unter die härteste Stufe, egal ob sie sich erst in einem frühen Entwicklungsstadium befinden. Dies behindert Innovation, da jedes Projekt bereits mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden müsste. Durch diese extreme Einstiegshürde wird der Innovationsstandort Schweiz nachhaltig geschädigt.</p> <p>Gleichzeitig wird auch der Wirkungsbereich der VÜPF stark erweitert. Während heute ein Unternehmen einen grossen Teil seiner Geschäftstätigkeit durch abgeleitete Kommunikationsdienste erbringen muss (Art. 22 Abs. 1 lit. b und Art. 52 Abs. 1 lit. b VÜPF), fällt dieses Kriterium neu weg. Dadurch können künftig auch Unternehmen, deren Geschäftstätigkeit nur am Rande auf abgeleiteten Kommunikationsdiensten basiert, wie Onlineshops, Marktplätze, Auktionsplattformen, Zeitungen, Computerspielhersteller und zahlreiche weitere Unternehmen, unter die VÜPF fallen – allein deshalb, weil ihre Produkte irgendeine Form privater Kommunikation zwischen Nutzer*innen und/oder Drittanbietern ermöglichen.</p> <p>Die vorgeschlagene Regelung stünde sodann im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali, das die zu weite Betroffenheit und die seltene Anwendung von Downgrades kritisierte: «Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»</p> <p>Statt KMU zu entlasten, führt die Revision neu sogar zu einer «automatischen Hochstufung per Verordnung ohne konkretisierende Verfügung (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.</p> <p>Die neue Regelung steht zudem in offensichtlichem Widerspruch zur bisherigen Praxis, denn bis heute wurde gemäss Angaben des Dienst-ÜPF keine einzige AAKD hochgestuft. Auch der Bundesrat stützte sich ausdrücklich auf die geltende Kombination von drei Schranken – einem Unternehmensfokus auf Kommunikationsdienste, einer Umsatzgrenze von 100 Millionen Franken sowie einer grossen Nutzerzahl – als er noch 2023 begründete, die Umsetzung des BÜPF sei gerade wegen der genannten Schranken als KMU-freundlich zu verstehen. Die vorliegende Revision hebt jedoch genau diese Kombination kumulativer Kriterien auf und will die einzelnen Kriterien künftig alternativ anwenden bzw. streicht sie sogar vollständig. Dadurch verlieren die bisherigen Schutzmechanismen ihre Wirkung, und das BÜPF soll neu auf viele KMU Anwendung finden, die früher nicht unter Gesetz und Verordnung fielen.</p> <p>Die Analyse der offiziellen Statistik des Dienstes ÜPF macht die offensichtliche Unverhältnismässigkeit dieses Ansinnens deutlich. Im Jahr 2023 betrafen 98,95 % der total 9'430 Überwachungen allein</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,05 % für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,73 % wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100 % des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.</p> <p>Wesentlich ist insbesondere eine neue Pflicht zur Identifikation der Nutzer: Hiervon betroffen sind nicht nur alle AAKD mit reduzierten oder vollen Pflichten (und damit de facto fast alle AAKD der Schweiz), sondern auch all deren Wiederverkäufer. Im Ergebnis führt die neue Verordnung aus unserer Sicht dazu, dass man sich bei keinem marktrelevanten Dienst mehr anmelden kann, ohne den Pass, Führerschein oder ID zu hinterlegen oder zumindest Daten wie eine Telefonnummer anzugeben, die man ohne Pass oder ID nicht erhalten kann.</p> <p>Die automatische Hochstufung an sich führt bereits zu erheblicher Rechtsunsicherheit bei den betroffenen Unternehmen. Unter dem bestehenden System werden die generell-abstrakten Normen der VÜPF mittels Verfügung auf einen konkreten Einzelfall angewendet. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes ist aber im Zweifelsfall möglicherweise nur schwer zu beantworten. Zweifelsohne besteht hier ein schutzwürdiges Interesse seitens der AAKD daran, zu wissen, ob sie die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Nur das bisherige System entspricht den allgemeinen Grundsätzen des Verwaltungsverfahrens, welches für die Anwendung einer generell-abstrakten Norm eine Konkretisierung durch die Verwaltung voraussetzt. Von einer automatischen Hochstufung von AAKD ist daher aus Gründen der Rechtssicherheit abzusehen. Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.</p> <p>Gegenüber der alten VÜPF erweitert die Revision die Pflichten zur Automatisierung sodann noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragen wie z.B. IR_59 und IR_60, welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen. Genau diese Möglichkeit einer manuellen Intervention ist aber für die Provider kritisch, um Missbräuche zu verhindern, die wiederum die Verträge mit ihren Kunden und das Fernmeldegeheimnis verletzen könnten. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente damit erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 Bst. b der alten VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grossen[n] Teil ihrer Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. Damit fallen insbesondere bereits Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitzustellen, von Anfang an voll unter das Gesetz. Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Dies setzt der Innovation in der Schweiz neue riesige Hürden entgegen.</p> <p>Auch Non-Profit-Organisationen wie die Signal Foundation, die kaum Umsätze erwirtschaften, geraten unter diese verschärften Vorgaben. Während sie bisher unter Duldungspflichten verbleiben konnten, solange sie Art. 22 Abs. 1 VÜPF nicht erfüllten, wird neu allein auf die Anzahl der Nutzer*innen abgestellt, womit z.B. Signal neu als AAKD mit vollen Pflichten erfasst würde. Dies würde dazu führen, dass Signal in der Schweiz entweder zu einem Rückzug aus dem Markt gezwungen wird oder erhebliche rechtliche Konsequenzen riskiert, da Signal keine IP-Adressen speichert und somit gegen Art. 19 RevVÜPF verstößt.</p> <p>Die Regelung ignoriert zudem wirtschaftliche Realitäten: Ein hoher Nutzerkreis bedeutet bei Non-Profits keine finanzielle Tragfähigkeit für umfangreiche Überwachungsmassnahmen. Damit werden Open-Source- und Non-Profit-Lösungen gezielt aus dem Markt gedrängt, während bestehende Monopole wie WhatsApp (96 % Marktanteil in der Schweiz) gestärkt werden. Die neue Regelung ist daher aus ökonomischer Sicht zu verwerfen. Das Kriterium der reinen Nutzerzahl ist ungeeignet und muss gestrichen werden.</p> <p>Nicht zuletzt schwächt die Regelung auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger*innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, Ende-zu-Ende-verschlüsselter Kommunikation ist heute wichtiger denn je.</p> <p>Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade als rechtswidrig gilt (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer*innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, sondern allein diese Anhäufung an Daten malt eine Zielscheibe auf den Rücken von Schweizer Unternehmen und Dienstleistungen für Hackerangriffe aus der ganzen Welt.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Weiters ist zu erwähnen, dass es gar nicht erwiesen ist, dass die Speicherung der fraglichen Daten eine merklich höhere Quote erfolgreicher Ermittlungen durch die Strafverfolgungsbehörden mit sich bringen würde. Im Gegenteil müssen die bereits existierenden Sekundärdaten, die allein durch die Bereitstellung eines Dienstes für den Nutzer entstehen, besser genutzt werden. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisbrauch via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfügt, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden. Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren.</p> <p>Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Souveränität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.</p> <p>Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das Datenschutzgesetz. Der Entwurf bringt nicht, wie der Begleitbericht dem Leser in geradezu in Orwell'scher Manier weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit und steht in direktem Gegensatz zum besagten Postulat 19.4031.</p> <p>Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen, und das bestehende System muss beibehalten werden.</p>
5.	Art. 16h Abs. 2	Streichung der Ausführung im erläuternden Bericht und ein Abstellen der Formulierung auf die gleichzeitige Anzahl Nutzer.	Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Nutzer*innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 Rev.VÜPF, gemäss dem die das WLAN erschliessenden FDA die Verantwortung für die Identifikation der Nutzer der WLANs tragen.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer*innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24) oder die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22). Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDAs unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden. Unter der bestehenden Regelung konnte eine FDA anhand der Lokation (z.B. Bibliothek, Flughafen) eine Einschätzung treffen. Die neue Definition hingegen würde von ihr verlangen, Zugriff auf jedes private Netzwerk zu erhalten, um Hardware und Einstellungen zu prüfen – ein offensichtlich verfassungswidriges und auch praktisch unmögliches Unterfangen. Diese vage Formulierung führt zu anhaltender Rechtsunsicherheit für FDA.</p> <p>Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten.</p> <p>Zudem könnte Art. 16h dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist*innen, Whistleblower*innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer*innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen. Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt.</p>
	Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2	Streichung des «Konzernatbestand» und Beibehaltung der bestehenden Regelung	Die Verordnung nimmt neu nicht mehr die Umsatz- und Nutzerzahlen der betroffenen Unternehmen, sondern die Zahlen des jeweiligen Konzerns als Basis für Up- und Downgrades. Die Begründung zur Einführung dieses «Konzernatbestands», wonach die neue Regelung für die betroffenen Unternehmen zu einer Vereinfachung führe, ist kontraintuitiv, ja offensichtlich falsch und irreführend. In der Praxis sind die betroffenen Unternehmen nämlich schon heute verpflichtet, ihre Buchhaltung nach Produkten aufzugliedern. Somit können die Kennzahlen bereits heute sehr einfach festgestellt werden. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.
6.	Art. 19 Abs. 1	Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation	<p>Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vor sieht.</p> <p>Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des Schweizer Datenschutzgesetzes, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch der Schutz der Schweizer Kundschaft massiv</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
		von Teilnehmenden.	<p>beeinträchtigt wird. Datenschutzfreundliche Unternehmen werden bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.</p> <p>Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Dies wahrt nicht nur den Datenschutz, sondern schützt auch die Wettbewerbsfähigkeit von KMU, stärkt den Innovationsstandort Schweiz und die digitale Souveränität unseres Landes.</p>
7.	Art. 18	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.
8.	Art. 19 Abs. 2	Ersatzlose Streichung zugunsten bestehender Regelung	Eine Überwachung von Kunden durch FDA, ob diese die neuen Vorgaben der VÜPF zu WLANs einhalten (Art. 19 Abs. 2 Rev. VÜPF), und erst recht die dazu gelieferte Erklärung im erläuternden Bericht, wonach die FDA die Identifikation der WLAN-Nutzer vorzunehmen hätten, ist weder gesetzeskonform noch zumutbar (siehe vorstehend). Art. 19 Abs. 2 ist ersatzlos zu streichen.
9.	Art. 21 Abs. 1 lit. a	Streichung	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.
10.	Art. 22	beibehalten	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.
11.	Art. 11 Abs. 4	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.
12.	Art. 16b	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.
13.	Art. 31 Abs. 1	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.
14.	Art. 51 und 52	beibehalten	Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.
15.	Art. 60a	Streichung des Artikels	Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Art. 60a VÜPF (Erläuterung Bundesrat: «...lediglich redaktionelle Änderungen....») sieht vor, dass Fernmeldedienstanbieterinnen über einen rückwirkenden Zeitraum von 6 Monaten alle Ziel-IP-Adressen liefern müssen, welche ihre Kunden besucht haben. Damit wird einerseits das Surfverhalten der gesamten schweizerischen Bevölkerung anlasslos und völlig unverhältnismässig ausspioniert. Andererseits wird die klare Vorgabe des BÜPF umgangen, das nur die Speicherung von Randdaten, aber nicht die Speicherung von Inhaltsdaten vorsieht.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Die geplante Überwachung des Internetverkehrs führt zu einer Überwachung, wer im Internet welche Adressen besucht hat. Dies geht zweifellos über die Schranken der gesetzlichen Regelung hinaus, dies insbesondere nachdem bereits die Aufzeichnung reiner Randdaten höchst umstritten und Gegenstand laufender Gerichtsverfahren ist. Hinzu kommt folgendes: Während bislang die Überwachung einer IP-Adresse nur im Rahmen einer sog. Echtzeit-Überwachung zulässig war, welche entsprechende Bewilligungen durch ein Gericht erforderte, muss neu nur noch ein einfaches Auskunftsbegehren durch die zuständige Behörde genehmigt werden. Die Abfragen erfolgen automatisiert.</p> <p>Art. 60a sieht weiter vor, dass bei nicht exakt zuordenbaren IP-Adressen die kompletten Listen aller Nutzerinnen und Nutzer zu liefern ist. IP-Adressen sind ein rares Gut. Alle FDA teilen diese den Nutzenden im Millisekunden-Takt zu. Da die Zeitstempel der Systemanbieter nicht immer übereinstimmen, sind diese IP-Adressen nicht immer eindeutig einem Nutzenden zuzuordnen. Neu müssen Provider nun komplettene Listen aller Nutzenden liefern. Dies bringt Zehntausende in den Fokus von Überwachungsbehörden, was auf eine Art Rasterfahndung nach Delikten über grosse Teile der Bevölkerung hinausläuft. Entdecken Strafverfolger dabei zufälligerweise etwas, können sie umgehend Strafverfahren einleiten.</p> <p>Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde sodann gemäss Bericht gezielt auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten.</p> <p>Art. 60a ist zu streichen.</p>
16.	Art. 42a und Art. 43a	Streichung des Artikels	<p>Sowohl Art. 42a als auch Art. 43a fordern die Abrufbarkeit des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Nicht nur gilt auch hier wieder die Limite von 5'000 Nutzern, was somit fast die gesamte AAKD-Landschaft der Schweiz flächendeckend umfasst, sondern solche Abfragen sollen nun auch durch eine einfach «IR_» Abfrage gemacht werden können, welche im Gegensatz zu den «HD_»-Abfragen und den «RT_»-Überwachungen ohne weitere juristische Aufsicht automatisiert abgerufen werden können, obwohl es sich auch hier um das Abrufen einer IP-Adresse in der Vergangenheit handelt, genau wie bei den «HD_» abfragen, welche deutlich strenger reglementiert sind. Es ist nicht nachvollziehbar und verletzt aus unserer Sicht die gesetzliche Grundlage des BÜPF, dass Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber.</p> <p>Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser Automatisierten Auskünfte ergibt. Durch das Fehlen solcher Limiten könnte daher z.B. alle 5 Minuten eine solche Anfrage automatisiert gestellt werden. Zunächst können sich dadurch lärmende Kosten für die betroffenen AAKD ergeben. Sodann können die Anfragen an ein automatisiertes Auskunftssystem gestellt werden, und es können auf diese Weise viele der Informationen welche ursprünglich über die juristisch</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>sichereren HD_ und RT_ Auskunfts-/Überwachungstypen liefern, neu über den rechtlich unsicheren IR_- Typ eingeholt werden. IR_59 und IR_60 ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne dass sie den benötigten Kontrollen dieser invasiven Überwachungsarten unterliegen würden.</p> <p>Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind, wie dies das BÜPF vorsieht.</p> <p>Die beiden Artikel sind daher vollumfänglich zu streichen.</p> <p>Diese neue Regelung und der zugehörige erläuternde Bericht sind im Übrigen eklatante Beispiele für die eingangs bemängelte überaus verwirrende und unverständliche Darstellung von Verordnungstext und erläuterndem Bericht.</p> <p>Im erläuternden Bericht steht auf S. 39 wörtlich:</p> <p><i>«In Absatz 1 sind die zu liefernden Angaben geregelt. Gemäss Buchstabe a ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin der oder dem Teilnehmenden einen solchen zugeteilt hat. Der «eindeutige Dienstidentifikator» gemäss Buchstabe b bezeichnet den Fernmelde- oder abgeleiteten Kommunikationsdienst, auf den sich die Antwort bezieht, eindeutig im Bereich der Anbieterin. In Buchstabe c werden die zu liefernden Angaben über den Ursprung der Verbindung bei der letzten zugriffsrelevanten Aktivität aufgezählt. Diese Angaben können für die Identifikation der Benutzerinnen und Benutzer nützlich sein.»</i></p> <p>Der Leser bzw. die Leserin urteile selber über die Verständlichkeit.</p> <p>Folgende Begriffe sind auch für den fachkundigen Leser nicht nachvollziehbar, bzw. es stellen sich folgende Verständnisfragen:</p> <ul style="list-style-type: none"> - Eindeutiger Identifikator: Was ist gemeint? Ist die Kundennummer des Internetproviders gemeint? Oder jene des genutzten dritten Fernmeldedienstes oder abgeleiteten Kommunikationsdienstes? Wie soll der Internetprovider überhaupt an diese Daten herankommen? - Eindeutiger Dienstidentifikator: Muss der Internetprovider eine Liste aller möglichen durch seine Kunden im Internet genutzten Kommunikationsdienste führen und aufzeichnen, muss er zudem aufzeichnen welcher Kunde welchen Dienst wann genau genutzt hat? Woher hat er diese Liste? Wie kann er herausfinden, ob ein Kunde gerade einen bestimmten Dienst nutzt? Gilt dies auch für ausländische Dienste? Nur für AAKD, für ausländische Fernmeldedienste, oder für alle Internetangebote weltweit? Der erläuternde Bericht bleibt hier völlig unklar.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<ul style="list-style-type: none"> - Was ist mit «Antwort» gemeint? Die Antwort des Servers des abgeleiteten Kommunikationsdienstes, den der Kunde besucht hat, oder die Antwort des Kundengeräts auf eine Nachricht von diesem Kommunikationsdienst? - Was ist mit «eindeutig im Bereich der Anbieterin» gemeint? Die Formulierung ist auch hier unverständlich. - Wie soll man sich eine «Antwort von einem anderen Fernmeldedienst» vorstellen? Muss ein Internetprovider die Herkunft sämtlicher auf seinem Netz eintreffenden Datenpakete aufzeichnen und dem Dienst ÜPF auf Anfrage diese Aufzeichnungen herausgeben? Wie soll die gigantische Masse an Daten, die durch ein solches Logging anfällt, durch die Internetprovider gemanaged werden? - Was ist mit «letzter zugriffsrelevanter Aktivitäten» gemeint? Geht es hier um die durch Kunden des Internetproviders aufgerufenen AAKD und andere Internetangebote? Wie soll der Internetprovider wissen, ob eine durch den Kunden aufgerufene IP-Adresse zu einem überwachungspflichtigen AAKD gehört, oder allenfalls zu einem nicht überwachungspflichtigen Dienst? Muss er einfach den ganzen Verkehr aufzeichnen? Wie weit zurück gehen die «zugriffsrelevanten» Aktivitäten? Müssen alle Daten für sechs Monate aufbewahrt werden? - Abgesehen davon: Wo wäre die gesetzliche Grundlage im BüPF für die vorgesehene inhaltliche Überwachung des Internetverkehrs? Das BüPF selber regelt bisher ausschliesslich die Überwachung der Randdaten, nicht aber von Inhaltsdaten, und spätestens dann, wenn Randdaten en passant auch Auskunft über die vom Kunden abgerufenen Inhalte geben, handelt es sich dabei um Inhaltsdaten, deren Sammlung erst recht gesetzes- und verfassungswidrig wäre, nachdem schon das Sammeln reiner Randdaten als menschenrechtswidrig taxiert wurde.
17.	50a	Artikel streichen	<p>Art. 50a sieht neu vor, dass Anbieter verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Diese Pflicht gilt nicht mehr nur für FDA (Art. 26 BüPF) oder ausnahmsweise für ausgewählte AAKD von hoher wirtschaftlicher Bedeutung (Art. 27 BüPF), sondern soll nun vorgabemässig und ohne Differenzierung auf sämtliche Anbieter mit mehr als 5'000 Teilnehmern angewendet werden, womit wohl fast die gesamte Schweizer AAKD-Branche betroffen ist (kaum ein Produkt ist lebensfähig mit weniger als 5000 Teilnehmern).</p> <p>Dies stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar.</p> <p>Diese Ausweitung ist nicht nur unverhältnismässig, sondern gefährdet aktiv nahezu die gesamte Schweizer IT-Branche: Indem de facto alle Anbieter vorgabemässig gezwungen werden, ihre Verschlüsselungssysteme für Behörden jederzeit entschlüsselbar zu gestalten, entstehen enorme Sicherheitsrisiken, denn</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Verschlüsselung ist wie eine Eierschale: Unversehrt ist sie stark, aber der kleinste Riss führt zu einer erheblichen Schwächung. Die betroffenen Systeme werden durch den vom Verordnungsgeber nun verpflichtend vorgesehenen Einbau von Hintertüren anfällig für Hackerangriffe, Datenmissbrauch und Spionage. Dies widerspricht Art. 13 BV und dem diesen konkretisierenden Datenschutzgesetz, das den Schutz personenbezogener Daten ausdrücklich durch wirksame technische Massnahmen – insbesondere Verschlüsselung – vorschreibt. Eine durch den Anbieter aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung in jedem Fall.</p> <p>Genau eine solche Schwächung der Verschlüsselung wurde kürzlich vom Europäischen Gerichtshof für Menschenrechte im Fall PODCHASOV gegen Russland (33696/19) als Verstoss gegen Grundrechte gewertet. Art. 50a verstösst somit auch gegen geltendes Völkerrecht.</p> <p>Nebst diesem Verstoss gegen das Völkerrecht wird aber auch das Gebot der Verhältnismässigkeit aus Art. 36 BV nicht eingehalten, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Wie bereits bei Art. 16e, Art. 16f und Art. 16g erwähnt, müssen zuerst die einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.</p> <p>Zusätzlich, und wie bereits bei Art. 16d erwähnt, verhindert Art. 50a die effektive Erbringung von VPN-Diensten. Bei solch einem VPN kontrolliert der Betreiber sowohl den Eingangs- als auch den Endpunkt. Da die Kommunikation vom Endpunkt zu einer Webseite aufgrund der vorherrschenden Struktur im allgemeinen Internet nicht End-zu-End-Verschlüsselt erfolgen kann, werden schon kleine VPNs (mit 5000 Nutzern) dazu gezwungen ihre eigene Verschlüsselung zu entfernen und ihre Kunden zu überwachen. Da der Schutz der Privatsphäre der Nutzer*innen von VPNs just den Kernpunkt oder USP der Dienstleistung darstellt, werden Schweizer VPN-Anbieterinnen hierdurch am internationalen Markt übermässig benachteiligt, ja ihres eigentlichen Daseinszwecks beraubt.</p> <p>Wesentlich ist zudem, dass Anbieter von Mail- oder Messaging-Apps zwangsläufig die Nachricht in der App in einer menschenlesbaren Version anzeigen muss, und dass an dieser Stelle die End-zu-End-Verschlüsselung notwendigerweise bereits entfernt ist. Der Wortlaut von Art. 50a lässt entgegen sämtlichen Beteuerungen des Dienstes ÜPF bereits anlässlich der letzten Revision der VÜPF weiterhin offen, ob eine Entfernung der Verschlüsselung auch an dieser Stelle gefordert werden können soll. Angesichts der seit</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			Jahren erkennbaren Tendenz der Schweizer Überwachungsbehörden, die Anwendbarkeit des Überwachungsrechts laufend weiter auszudehnen und sich dabei nur durch Gerichte bremsen zu lassen, ist bei dieser Gelegenheit erneut die Klarstellung zu fordern, wonach die Entfernung von Verschlüsselungen, die erst in der Sphäre des Benutzers angebracht werden (wenngleich auch durch Software der Anbieterin) nicht verlangt werden darf. Dies ist zumindest im erläuternden Bericht zu erwähnen. Der erneute Verzicht wäre nichts anderes als eine Einladung an die Überwachungsbehörden, die Einführung einer offensichtlich illegalen und vom BÜPF keineswegs vorgesehenen «Chatkontrolle» auf dem «Auslegungsweg» vorzunehmen.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Artikel	Antrag	Begründung / Bemerkung	
VD-ÜPF / OME-SCPT / OE-SCPT			
Art. 14 Abs. 3 VD-ÜPF	Streichung	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit 5000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Absatz ist daher ersatzlos zu streichen.	
Art. 14 Abs. 4 VD-ÜPF	Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten.	Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der unterworfenen AAKD massiv. Dies ist wie beschrieben weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.	
Art. 20 Abs. 1 VD-ÜPF	Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.	

*Vernehmlassungsantwort zu den Teilrevisionen der VÜPF und der VD-ÜPF
gemäss Schreiben des EJPD vom 29. Januar 2025*

Datum	05.05.2025
Verfasser (Unternehmen)	Netwolk GmbH, Aathalstrasse 84, 8610 Uster
Kontaktperson bei Fragen (Name/Tel./E-Mail)	Yvan Kuonen 044 515 93 00 yvan.kuonen@netwolk.com

Dieses Dokument geht an:

Eidgenössisches Justiz- und Polizeidepartement EJPD, ptss-aemterkonsultationen@isc-ejpd.admin.ch

Sehr geehrter Herr Bundesrat Jans, sehr geehrte Damen und Herren

Wir beziehen uns auf das am 29. Januar 2025 eröffnete Vernehmlassungsverfahren zu Teilrevisionen von VÜPF und VD-ÜPF und bedanken uns für die Möglichkeit einer Stellungnahme.

Wir lehnen die geplante Teilrevisionen der VÜPF und der VD-ÜPF in aller Deutlichkeit und vollumfänglich ab.

Im Bericht des Bundesrates zur aktuellen Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF und der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) ist zu lesen, dass die Revision im Wesentlichen auf die Anpassung der Verordnungen an die KMU-Freundlichkeit abziele. Ein grosser Teil der vorgeschlagenen Änderungen *verfolgt aber gerade das Gegenteil*.

Die Geschäftsgrundlagen von Schweizer Unternehmen wie Threema, Proton und anderer KMU, die weltweit einen hervorragenden Ruf als Anbieterinnen sicherer Kommunikationsdienste im Internet geniessen, drohen durch die Vorlage zerstört zu werden. Die Sicherheit des Internets in der Schweiz soll mit der Revision der Überwachung jeglichen Internetverkehrs regelrecht untergeordnet werden: «**Sicherheit vor Freiheit» ist das neue Paradigma**. Dieses zieht sich wie ein roter Faden quer durch diese völlig verunglückte Reform. KMU, die aus der Schweiz heraus Internet-Dienste anbieten («abgeleitete Kommunikationsdienste» in der Terminologie des Gesetzes), soll die Schweiz als Standort geradezu vergällt werden. Dies scheint denn auch zu gelingen: **Erste der betroffenen Unternehmen haben bereits angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen** (siehe Tages-Anzeiger vom 1. April 2025).

Ein derartiger Paradigmenwechsel, weg von KMU-Schutz und Überwachung mit Augenmass, hin zu knallharter Überwachung, die alle anderen Interessen unterordnet, wird durch das geltende Gesetz (BÜPF) keineswegs gestützt. Der Paradigmenwechsel widerspricht vielmehr geradezu dem Geist des ursprünglichen BÜPF, das Internetdienste, die in der Schweiz meist von KMU betrieben werden, gerade von der Implementierung teurer Überwachungsmassnahmen schützen wollte, und das eine austarierte Interessenabwägung vorsah zwischen Privatsphäre und Freiheit auf der einen Seite und staatlicher Überwachung auf der anderen Seite.

Entgegen dem im Begleitbericht zum vorgelegten Entwurf erklärten Ziel, die «finanzielle Belastung der KMU gering zu halten», stuft die Vorlage eine grosse Mehrheit der Schweizer Anbieterinnen von Internetdiensten in eine höhere Stufe auf, und zwingt sie neu auch in jenen Bereichen zu einer kostspieligen aktiven Überwachungstätigkeit, wo bisher nur eine KMU-freundliche Duldungspflicht bestand. Dies verschiebt das bisherige Gleichgewicht der Interessen zwischen Strafverfolgung und betroffenen Anbieterinnen in drastischer Weise zulasten der betroffenen Anbieterinnen.

Die vorgeschlagenen Anpassungen bringen ganz erhebliche Risiken für den Innovations- und Wirtschaftsstandort Schweiz mit sich und erfüllen die Kernziele der Revision, die Entlastung von KMU, gerade nicht. Der Ruf der Schweiz als sicherer Hafen für vertrauenswürdige IT-Anbieter droht durch die Revision nachhaltig beschädigt zu werden. Deshalb lehnen wir die Revision vollumfänglich ab.

Auch **die Schweizer Armee** nutzt solche Dienste, wie beispielsweise Threema, und zwar gerade aufgrund des hohen gebotenen Sicherheitsstandards. Die Annahme dieser Revision, welche dieses Sicherheitsniveau gezielt untergraben will, verletzt damit indirekt auch das direkte Interesse der Schweiz an lokal betriebenen Hochsicherheitsanwendungen. Gerade in der heutigen Zeit, in der die Zuverlässigkeit der grossen US-Anbieter in ihrer Abhängigkeit von einer zunehmend erratisch agierenden US-Regierung mehr und mehr in Frage steht, erscheint dies als **inakzeptable Hochrisikostrategie**.

Nicht zuletzt ist mit Nachdruck darauf hinzuweisen, dass die Revision die Überwachung ganz allgemein stark ausweitet. Dies ist mit der durch den Gesetzgeber im BÜPF festgelegten, fein austarierten Interessenabwägung zwischen Freiheit und Privatsphäre der Einwohner der Schweiz einerseits und Sicherheit durch Überwachungsmassnahmen andererseits absolut nicht vereinbar. Die Revision entpuppt sich geradezu als eine Art Wunschkonzert für Überwachungsbehörden. Insbesondere ist künftig auch **eine komplette inhaltliche Überwachung des gesamten Internetverkehrs** der Schweiz vorgesehen. Dies ohne dass eine solche inhaltliche Überwachung durch die gesetzlichen Grundlagen des BÜPF in irgend einer Weise gedeckt wäre: Zulässig ist gemäss BÜPF einzig und allein die Überwachung von Randdaten des Fernmeldeverkehrs, und selbst die Zulässigkeit der in diesem Kontext angewendeten anlasslosen Vorratsdatenspeicherung von Randdaten ist bis heute umstritten und Gegenstand von Gerichtsverfahren, ja in der EU bereits höchstrichterlich als menschenrechtswidrig erkannt. Die durch die Verordnungsrevision eingeführte *Inhaltsüberwachung* ist in der Schweiz damit erst recht **offensichtlich illegal und verfassungswidrig**.

Abschliessend sei noch der Hinweis angebracht, dass wir die Gesetzgebungstechnik des Entwurfs für überaus schlecht halten. **Sowohl der Verordnungstext als auch der zugehörige erläuternde Bericht sind über weite Strecken höchst verwirrend und unverständlich formuliert**, unter anderem mit einer Vielzahl von Querverweisen, technischen Fehlern und unklarer Begrifflichkeit (für ein Beispiel hierfür siehe unten, Bemerkungen zu Art. 43a). Die Texte sind in dieser Form selbst für Fachleute über weite Strecken nicht zu verstehen, geschweige denn als Ganzes zu überblicken. Für KMU, die durch die Revision neu mit erheblich strengerem Pflichten konfrontiert werden, ist eine rechtskonforme Umsetzung dieser Vorlage daher ein schlicht aussichtloses Unterfangen.

Das Legalitätsprinzip gemäss Art. 5 Bundesverfassung fordert vom Gesetzgeber, dass Gesetzestexte für die Adressaten verständlich formuliert sind. Die Texte der Verordnungsrevision genügen dieser Anforderung offensichtlich in keiner Weise. Nur schon aufgrund der völlig fehlenden Verständlichkeit ist die Verfassungsmässigkeit der Revision insgesamt *höchst zweifelhaft*. Wir fordern nur schon deshalb einen Rückzug der vorgelegten Texte, eine komplette Überarbeitung zur Verbesserung der Verständlichkeit und eine erneute Auflage zur Vernehmlassung.

Mit freundlichen Grüßen



■■ Yvan Kuonen, Netwolk GmbH

Bemerkungen zu einzelnen Artikeln der VÜPF

Nr.	Artikel	Antrag	Begründung / Bemerkung
VÜPF / OSCPT / OSCPT			
0.	Alle Artikel	Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.	<p>Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kunden auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.</p> <p>Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.dgl. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.</p>
1.	16b, Abs. 1	Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.»	Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile, wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Anforderungen in Kauf nehmen.
2.	16c, Abs. 3	Streichung von lit. a «automatisierte Erteilung der Auskünfte (Art. 18 Abs. 2);»	Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Dies untergräbt rechtsstaatliche Prinzipien doppelt: Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>«natürliche» Schutzmechanismen gegen eine überschiessende, missbräuchliche oder zumindest unverhältnismässige Nutzung solcher Massnahmen durch die Untersuchungsbehörden.</p> <p>Der vorgesehene Umsetzungszeitraum von 12 Monaten für die rechtssichere Implementierung eines derart komplexen Systems völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.</p>
3.	Art. 16d	<p>Streichung von Online-speicherdiensten und VPN-Anbietern in der Auslegung</p>	<p>Eine klarere Definition des Begriffs AAKD ist begrüssenswert, doch die neue Auslegung gemäss erläuterndem Bericht geht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdiensten wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter, etc.) genutzt werden.</p> <p>Art. 2 lit. c BüPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug den gesetzlichen Rahmen sprengt. Onlinespeicherdienste sind deshalb aus Art. 16d zu streichen.</p> <p>Zudem anerkennt der erläuternde Bericht, dass VPNs zur Anonymisierung der Nutzer*innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Anbieter von VPNs sind daher ebenfalls aus dem Geltungsbereich von Art. 16d auszunehmen.</p>
4.	Art. 16e, Art. 16f und Art. 16g	<p>Streichung der Artikel und Beibehaltung der bestehenden Kriterien</p> <p>Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).</p>	<p>Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch diametral entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung. Dies daher, weil neu KMU bereits mit mehr als 5'000 Nutzern erfasst werden.</p> <p>Die Einführung von 5000 Nutzern als gesondert zu beurteilende Untergrenze verletzt aus unserer Sicht bereits Art. 27 Abs. 3 BüPF, denn 5000 Personen keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strengereren Überwachungsmassnahmen, gerechtfertigt wären. 5000 Nutzer werden in der digitalen Welt vielmehr sehr rasch erreicht.</p> <p>Zusätzlich führt das Einführen eines «Konzerntatbestandes» in Art. 16f Abs. 3 zu massiven Problemen, da die Produkte nun nicht mehr für sich alleine eine bestimmte Grösse erreichen müssen, sondern die rele-</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>vanten Zahlen anhand des Umsatzes des Unternehmens, bzw. in Konzernverhältnissen sogar des Konzerns bestimmt werden. Vor allem bei Unternehmen mit Beteiligungsfirmen im Hintergrund fallen nun neu alle Dienstleistungen und Produkte automatisch unter die härteste Stufe, egal ob sie sich erst in einem frühen Entwicklungsstadium befinden. Dies behindert Innovation, da jedes Projekt bereits mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden müsste. Durch diese extreme Einstieghürde wird der Innovationsstandort Schweiz nachhaltig geschädigt.</p> <p>Gleichzeitig wird auch der Wirkungsbereich der VÜPF stark erweitert. Während heute ein Unternehmen einen grossen Teil seiner Geschäftstätigkeit durch abgeleitete Kommunikationsdienste erbringen muss (Art. 22 Abs. 1 lit. b und Art. 52 Abs. 1 lit. b VÜPF), fällt dieses Kriterium neu weg. Dadurch können künftig auch Unternehmen, deren Geschäftstätigkeit nur am Rande auf abgeleiteten Kommunikationsdiensten basiert, wie Onlineshops, Marktplätze, Auktionsplattformen, Zeitungen, Computerspielhersteller und zahlreiche weitere Unternehmen, unter die VÜPF fallen – allein deshalb, weil ihre Produkte irgendeine Form privater Kommunikation zwischen Nutzer*innen und/oder Drittanbietern ermöglichen.</p> <p>Die vorgeschlagene Regelung stünde sodann im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali, das die zu weite Betroffenheit und die seltene Anwendung von Downgrades kritisierte: «Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»</p> <p>Statt KMU zu entlasten, führt die Revision neu sogar zu einer «automatischen Hochstufung per Verordnung ohne konkretisierende Verfügung (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.</p> <p>Die neue Regelung steht zudem in offensichtlichem Widerspruch zur bisherigen Praxis, denn bis heute wurde gemäss Angaben des Dienst-ÜPF keine einzige AAKD hochgestuft. Auch der Bundesrat stützte sich ausdrücklich auf die geltende Kombination von drei Schranken – einem Unternehmensfokus auf Kommunikationsdienste, einer Umsatzgrenze von 100 Millionen Franken sowie einer grossen Nutzerzahl – als er noch 2023 begründete, die Umsetzung des BÜPF sei gerade wegen der genannten Schranken als KMU-freundlich zu verstehen. Die vorliegende Revision hebt jedoch genau diese Kombination kumulativer Kriterien auf und will die einzelnen Kriterien künftig alternativ anwenden bzw. streicht sie sogar vollständig. Dadurch verlieren die bisherigen Schutzmechanismen ihre Wirkung, und das BÜPF soll neu auf viele KMU Anwendung finden, die früher nicht unter Gesetz und Verordnung fielen.</p> <p>Die Analyse der offiziellen Statistik des Dienstes ÜPF macht die offensichtliche Unverhältnismässigkeit dieses Ansinnens deutlich. Im Jahr 2023 betrafen 98,95 % der total 9'430 Überwachungen allein</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,05 % für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,73 % wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100 % des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.</p> <p>Wesentlich ist insbesondere eine neue Pflicht zur Identifikation der Nutzer: Hiervon betroffen sind nicht nur alle AAKD mit reduzierten oder vollen Pflichten (und damit de facto fast alle AAKD der Schweiz), sondern auch all deren Wiederverkäufer. Im Ergebnis führt die neue Verordnung aus unserer Sicht dazu, dass man sich bei keinem marktrelevanten Dienst mehr anmelden kann, ohne den Pass, Führerschein oder ID zu hinterlegen oder zumindest Daten wie eine Telefonnummer anzugeben, die man ohne Pass oder ID nicht erhalten kann.</p> <p>Die automatische Hochstufung an sich führt bereits zu erheblicher Rechtsunsicherheit bei den betroffenen Unternehmen. Unter dem bestehenden System werden die generell-abstrakten Normen der VÜPF mittels Verfügung auf einen konkreten Einzelfall angewendet. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes ist aber im Zweifelsfall möglicherweise nur schwer zu beantworten. Zweifelsohne besteht hier ein schutzwürdiges Interesse seitens der AAKD daran, zu wissen, ob sie die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Nur das bisherige System entspricht den allgemeinen Grundsätzen des Verwaltungsverfahrens, welches für die Anwendung einer generell-abstrakten Norm eine Konkretisierung durch die Verwaltung voraussetzt. Von einer automatischen Hochstufung von AAKD ist daher aus Gründen der Rechtssicherheit abzusehen. Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.</p> <p>Gegenüber der alten VÜPF erweitert die Revision die Pflichten zur Automatisierung sodann noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragen wie z.B. IR_59 und IR_60, welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen. Genau diese Möglichkeit einer manuellen Intervention ist aber für die Provider kritisch, um Missbräuche zu verhindern, die wiederum die Verträge mit ihren Kunden und das Fernmeldegeheimnis verletzen könnten. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente damit erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 Bst. b der alten VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grossen[n] Teil ihrer Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. Damit fallen insbesondere bereits Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz. Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Dies setzt der Innovation in der Schweiz neue riesige Hürden entgegen.</p> <p>Auch Non-Profit-Organisationen wie die Signal Foundation, die kaum Umsätze erwirtschaften, geraten unter diese verschärften Vorgaben. Während sie bisher unter Duldungspflichten verbleiben konnten, solange sie Art. 22 Abs. 1 VÜPF nicht erfüllten, wird neu allein auf die Anzahl der Nutzer*innen abgestellt, womit z.B. Signal neu als AAKD mit vollen Pflichten erfasst würde. Dies würde dazu führen, dass Signal in der Schweiz entweder zu einem Rückzug aus dem Markt gezwungen wird oder erhebliche rechtliche Konsequenzen riskiert, da Signal keine IP-Adressen speichert und somit gegen Art. 19 RevVÜPF verstößt.</p> <p>Die Regelung ignoriert zudem wirtschaftliche Realitäten: Ein hoher Nutzerkreis bedeutet bei Non-Profits keine finanzielle Tragfähigkeit für umfangreiche Überwachungsmassnahmen. Damit werden Open-Source- und Non-Profit-Lösungen gezielt aus dem Markt gedrängt, während bestehende Monopole wie WhatsApp (96 % Marktanteil in der Schweiz) gestärkt werden. Die neue Regelung ist daher aus ökonomischer Sicht zu verwerfen. Das Kriterium der reinen Nutzerzahl ist ungeeignet und muss gestrichen werden.</p> <p>Nicht zuletzt schwächt die Regelung auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger*innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, Ende-zu-Ende-verschlüsselter Kommunikation ist heute wichtiger denn je.</p> <p>Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade als rechtswidrig gilt (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer*innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, sondern allein diese Anhäufung an Daten malt eine Zielscheibe auf den Rücken von Schweizer Unternehmen und Dienstleistungen für Hackerangriffe aus der ganzen Welt.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Weiters ist zu erwähnen, dass es gar nicht erwiesen ist, dass die Speicherung der fraglichen Daten eine merklich höhere Quote erfolgreicher Ermittlungen durch die Strafverfolgungsbehörden mit sich bringen würde. Im Gegenteil müssen die bereits existierenden Sekundärdaten, die allein durch die Bereitstellung eines Dienstes für den Nutzer entstehen, besser genutzt werden. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisbrauch via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfügt, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden. Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren.</p> <p>Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Souveränität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.</p> <p>Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das Datenschutzgesetz. Der Entwurf bringt nicht, wie der Begleitbericht dem Leser in geradezu in Orwell'scher Manier weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit und steht in direktem Gegensatz zum besagten Postulat 19.4031.</p> <p>Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen, und das bestehende System muss beibehalten werden.</p>
5.	Art. 16h Abs. 2	Streichung der Ausführung im erläuternden Bericht und ein Abstellen der Formulierung auf die gleichzeitige Anzahl Nutzer.	Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Nutzer*innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 Rev.VÜPF, gemäss dem die das WLAN erschliessenden FDA die Verantwortung für die Identifikation der Nutzer der WLANs tragen.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer*innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24) oder die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22). Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDAs unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden. Unter der bestehenden Regelung konnte eine FDA anhand der Lokation (z.B. Bibliothek, Flughafen) eine Einschätzung treffen. Die neue Definition hingegen würde von ihr verlangen, Zugriff auf jedes private Netzwerk zu erhalten, um Hardware und Einstellungen zu prüfen – ein offensichtlich verfassungswidriges und auch praktisch unmögliches Unterfangen. Diese vage Formulierung führt zu anhaltender Rechtsunsicherheit für FDA.</p> <p>Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten.</p> <p>Zudem könnte Art. 16h dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist*innen, Whistleblower*innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer*innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen. Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt.</p>
	Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2	Streichung des «Konzernatbestand» und Beibehaltung der bestehenden Regelung	<p>Die Verordnung nimmt neu nicht mehr die Umsatz- und Nutzerzahlen der betroffenen Unternehmen, sondern die Zahlen des jeweiligen Konzerns als Basis für Up- und Downgrades. Die Begründung zur Einführung dieses «Konzernatbestands», wonach die neue Regelung für die betroffenen Unternehmen zu einer Vereinfachung führe, ist kontraintuitiv, ja offensichtlich falsch und irreführend. In der Praxis sind die betroffenen Unternehmen nämlich schon heute verpflichtet, ihre Buchhaltung nach Produkten aufzugliedern. Somit können die Kennzahlen bereits heute sehr einfach festgestellt werden. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.</p>
6.	Art. 19 Abs. 1	Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation	<p>Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vor sieht.</p> <p>Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des Schweizer Datenschutzgesetzes, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch der Schutz der Schweizer Kundschaft massiv</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
		von Teilnehmenden.	<p>beeinträchtigt wird. Datenschutzfreundliche Unternehmen werden bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.</p> <p>Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Dies wahrt nicht nur den Datenschutz, sondern schützt auch die Wettbewerbsfähigkeit von KMU, stärkt den Innovationsstandort Schweiz und die digitale Souveränität unseres Landes.</p>
7.	Art. 18	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.
8.	Art. 19 Abs. 2	Ersatzlose Streichung zugunsten bestehender Regelung	Eine Überwachung von Kunden durch FDA, ob diese die neuen Vorgaben der VÜPF zu WLANs einhalten (Art. 19 Abs. 2 Rev. VÜPF), und erst recht die dazu gelieferte Erklärung im erläuternden Bericht, wonach die FDA die Identifikation der WLAN-Nutzer vorzunehmen hätten, ist weder gesetzeskonform noch zumutbar (siehe vorstehend). Art. 19 Abs. 2 ist ersatzlos zu streichen.
9.	Art. 21 Abs. 1 lit. a	Streichung	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.
10.	Art. 22	beibehalten	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.
11.	Art. 11 Abs. 4	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.
12.	Art. 16b	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.
13.	Art. 31 Abs. 1	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.
14.	Art. 51 und 52	beibehalten	Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.
15.	Art. 60a	Streichung des Artikels	Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Art. 60a VÜPF (Erläuterung Bundesrat: «...lediglich redaktionelle Änderungen....») sieht vor, dass Fernmelddenstanbieterinnen über einen rückwirkenden Zeitraum von 6 Monaten alle Ziel-IP-Adressen liefern müssen, welche ihre Kunden besucht haben. Damit wird einerseits das Surfverhalten der gesamten schweizerischen Bevölkerung anlasslos und völlig unverhältnismässig ausspioniert. Andererseits wird die klare Vorgabe des BÜPF umgangen, das nur die Speicherung von Randdaten, aber nicht die Speicherung von Inhaltsdaten vorsieht.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Die geplante Überwachung des Internetverkehrs führt zu einer Überwachung, wer im Internet welche Adressen besucht hat. Dies geht zweifellos über die Schranken der gesetzlichen Regelung hinaus, dies insbesondere nachdem bereits die Aufzeichnung reiner Randdaten höchst umstritten und Gegenstand laufender Gerichtsverfahren ist. Hinzu kommt folgendes: Während bislang die Überwachung einer IP-Adresse nur im Rahmen einer sog. Echtzeit-Überwachung zulässig war, welche entsprechende Bewilligungen durch ein Gericht erforderte, muss neu nur noch ein einfaches Auskunftsbegehren durch die zuständige Behörde genehmigt werden. Die Abfragen erfolgen automatisiert.</p> <p>Art. 60a sieht weiter vor, dass bei nicht exakt zuordenbaren IP-Adressen die kompletten Listen aller Nutzerinnen und Nutzer zu liefern ist. IP-Adressen sind ein rares Gut. Alle FDA teilen diese den Nutzenden im Millisekunden-Takt zu. Da die Zeitstempel der Systemanbieter nicht immer übereinstimmen, sind diese IP-Adressen nicht immer eindeutig einem Nutzenden zuzuordnen. Neu müssen Provider nun komplettene Listen aller Nutzenden liefern. Dies bringt Zehntausende in den Fokus von Überwachungsbehörden, was auf eine Art Rasterfahndung nach Delikten über grosse Teile der Bevölkerung hinausläuft. Entdecken Strafverfolger dabei zufälligerweise etwas, können sie umgehend Strafverfahren einleiten.</p> <p>Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde sodann gemäss Bericht gezielt auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten.</p> <p>Art. 60a ist zu streichen.</p>
16.	Art. 42a und Art. 43a	Streichung des Artikels	<p>Sowohl Art. 42a als auch Art. 43a fordern die Abrufbarkeit des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Nicht nur gilt auch hier wieder die Limite von 5'000 Nutzern, was somit fast die gesamte AAKD-Landschaft der Schweiz flächendeckend umfasst, sondern solche Abfragen sollen nun auch durch eine einfach «IR_» Abfrage gemacht werden können, welche im Gegensatz zu den «HD_»-Abfragen und den «RT_»-Überwachungen ohne weitere juristische Aufsicht automatisiert abgerufen werden können, obwohl es sich auch hier um das Abrufen einer IP-Adresse in der Vergangenheit handelt, genau wie bei den «HD_» abfragen, welche deutlich strenger reglementiert sind. Es ist nicht nachvollziehbar und verletzt aus unserer Sicht die gesetzliche Grundlage des BÜPF, dass Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber.</p> <p>Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser Automatisierten Auskünfte ergibt. Durch das Fehlen solcher Limiten könnte daher z.B. alle 5 Minuten eine solche Anfrage automatisiert gestellt werden. Zunächst können sich dadurch lärmende Kosten für die betroffenen AAKD ergeben. Sodann können die Anfragen an ein automatisiertes Auskunftssystem gestellt werden, und es können auf diese Weise viele der Informationen welche ursprünglich über die juristisch</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>sichereren HD_ und RT_ Auskunfts-/Überwachungstypen liefern, neu über den rechtlich unsicheren IR_- Typ eingeholt werden. IR_59 und IR_60 ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne dass sie den benötigten Kontrollen dieser invasiven Überwachungsarten unterliegen würden.</p> <p>Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind, wie dies das BÜPF vorsieht.</p> <p>Die beiden Artikel sind daher vollumfänglich zu streichen.</p> <p>Diese neue Regelung und der zugehörige erläuternde Bericht sind im Übrigen eklatante Beispiele für die eingangs bemängelte überaus verwirrende und unverständliche Darstellung von Verordnungstext und erläuterndem Bericht.</p> <p>Im erläuternden Bericht steht auf S. 39 wörtlich:</p> <p><i>«In Absatz 1 sind die zu liefernden Angaben geregelt. Gemäss Buchstabe a ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin der oder dem Teilnehmenden einen solchen zugeteilt hat. Der «eindeutige Dienstidentifikator» gemäss Buchstabe b bezeichnet den Fernmelde- oder abgeleiteten Kommunikationsdienst, auf den sich die Antwort bezieht, eindeutig im Bereich der Anbieterin. In Buchstabe c werden die zu liefernden Angaben über den Ursprung der Verbindung bei der letzten zugriffsrelevanten Aktivität aufgezählt. Diese Angaben können für die Identifikation der Benutzerinnen und Benutzer nützlich sein.»</i></p> <p>Der Leser bzw. die Leserin urteile selber über die Verständlichkeit.</p> <p>Folgende Begriffe sind auch für den fachkundigen Leser nicht nachvollziehbar, bzw. es stellen sich folgende Verständnisfragen:</p> <ul style="list-style-type: none"> - Eindeutiger Identifikator: Was ist gemeint? Ist die Kundennummer des Internetproviders gemeint? Oder jene des genutzten dritten Fernmeldedienstes oder abgeleiteten Kommunikationsdienstes? Wie soll der Internetprovider überhaupt an diese Daten herankommen? - Eindeutiger Dienstidentifikator: Muss der Internetprovider eine Liste aller möglichen durch seine Kunden im Internet genutzten Kommunikationsdienste führen und aufzeichnen, muss er zudem aufzeichnen welcher Kunde welchen Dienst wann genau genutzt hat? Woher hat er diese Liste? Wie kann er herausfinden, ob ein Kunde gerade einen bestimmten Dienst nutzt? Gilt dies auch für ausländische Dienste? Nur für AAKD, für ausländische Fernmeldedienste, oder für alle Internetangebote weltweit? Der erläuternde Bericht bleibt hier völlig unklar.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<ul style="list-style-type: none"> - Was ist mit «Antwort» gemeint? Die Antwort des Servers des abgeleiteten Kommunikationsdienstes, den der Kunde besucht hat, oder die Antwort des Kundengeräts auf eine Nachricht von diesem Kommunikationsdienst? - Was ist mit «eindeutig im Bereich der Anbieterin» gemeint? Die Formulierung ist auch hier unverständlich. - Wie soll man sich eine «Antwort von einem anderen Fernmeldedienst» vorstellen? Muss ein Internetprovider die Herkunft sämtlicher auf seinem Netz eintreffenden Datenpakete aufzeichnen und dem Dienst ÜPF auf Anfrage diese Aufzeichnungen herausgeben? Wie soll die gigantische Masse an Daten, die durch ein solches Logging anfällt, durch die Internetprovider gemanaged werden? - Was ist mit «letzter zugriffsrelevanter Aktivitäten» gemeint? Geht es hier um die durch Kunden des Internetproviders aufgerufenen AAKD und andere Internetangebote? Wie soll der Internetprovider wissen, ob eine durch den Kunden aufgerufene IP-Adresse zu einem überwachungspflichtigen AAKD gehört, oder allenfalls zu einem nicht überwachungspflichtigen Dienst? Muss er einfach den ganzen Verkehr aufzeichnen? Wie weit zurück gehen die «zugriffsrelevanten» Aktivitäten? Müssen alle Daten für sechs Monate aufbewahrt werden? - Abgesehen davon: Wo wäre die gesetzliche Grundlage im BüPF für die vorgesehene inhaltliche Überwachung des Internetverkehrs? Das BüPF selber regelt bisher ausschliesslich die Überwachung der Randdaten, nicht aber von Inhaltsdaten, und spätestens dann, wenn Randdaten einen passant auch Auskunft über die vom Kunden abgerufenen Inhalte geben, handelt es sich dabei um Inhaltsdaten, deren Sammlung erst recht gesetzes- und verfassungswidrig wäre, nachdem schon das Sammeln reiner Randdaten als menschenrechtswidrig taxiert wurde.
17.	50a	Artikel streichen	<p>Art. 50a sieht neu vor, dass Anbieter verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Diese Pflicht gilt nicht mehr nur für FDA (Art. 26 BüPF) oder ausnahmsweise für ausgewählte AAKD von hoher wirtschaftlicher Bedeutung (Art. 27 BüPF), sondern soll nun vorgabemässig und ohne Differenzierung auf sämtliche Anbieter mit mehr als 5'000 Teilnehmern angewendet werden, womit wohl fast die gesamte Schweizer AAKD-Branche betroffen ist (kaum ein Produkt ist lebensfähig mit weniger als 5000 Teilnehmern).</p> <p>Dies stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar.</p> <p>Diese Ausweitung ist nicht nur unverhältnismässig, sondern gefährdet aktiv nahezu die gesamte Schweizer IT-Branche: Indem de facto alle Anbieter vorgabemässig gezwungen werden, ihre Verschlüsselungssysteme für Behörden jederzeit entschlüsselbar zu gestalten, entstehen enorme Sicherheitsrisiken, denn</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Verschlüsselung ist wie eine Eierschale: Unversehrt ist sie stark, aber der kleinste Riss führt zu einer erheblichen Schwächung. Die betroffenen Systeme werden durch den vom Verordnungsgeber nun verpflichtend vorgesehenen Einbau von Hintertüren anfälliger für Hackerangriffe, Datenmissbrauch und Spionage. Dies widerspricht Art. 13 BV und dem diesen konkretisierenden Datenschutzgesetz, das den Schutz personenbezogener Daten ausdrücklich durch wirksame technische Massnahmen – insbesondere Verschlüsselung – vorschreibt. Eine durch den Anbieter aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung in jedem Fall.</p> <p>Genau eine solche Schwächung der Verschlüsselung wurde kürzlich vom Europäischen Gerichtshof für Menschenrechte im Fall PODCHASOV gegen Russland (33696/19) als Verstoss gegen Grundrechte gewertet. Art. 50a verstösst somit auch gegen geltendes Völkerrecht.</p> <p>Nebst diesem Verstoss gegen das Völkerrecht wird aber auch das Gebot der Verhältnismässigkeit aus Art. 36 BV nicht eingehalten, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördararbeit steht. Wie bereits bei Art. 16e, Art. 16f und Art. 16g erwähnt, müssen zuerst die einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.</p> <p>Zusätzlich, und wie bereits bei Art. 16d erwähnt, verhindert Art. 50a die effektive Erbringung von VPN-Diensten. Bei solch einem VPN kontrolliert der Betreiber sowohl den Eingangs- als auch den Endpunkt. Da die Kommunikation vom Endpunkt zu einer Webseite aufgrund der vorherrschenden Struktur im allgemeinen Internet nicht End-zu-End-Verschlüsselt erfolgen kann, werden schon kleine VPNs (mit 5000 Nutzern) dazu gezwungen ihre eigene Verschlüsselung zu entfernen und ihre Kunden zu überwachen. Da der Schutz der Privatsphäre der Nutzer*innen von VPNs just den Kernpunkt oder USP der Dienstleistung darstellt, werden Schweizer VPN-Anbieterinnen hierdurch am internationalen Markt übermässig benachteiligt, ja ihres eigentlichen Daseinszwecks beraubt.</p> <p>Wesentlich ist zudem, dass Anbieter von Mail- oder Messaging-Apps zwangsläufig die Nachricht in der App in einer menschenlesbaren Version anzeigen muss, und dass an dieser Stelle die End-zu-End-Verschlüsselung notwendigerweise bereits entfernt ist. Der Wortlaut von Art. 50a lässt entgegen sämtlichen Beteuerungen des Dienstes ÜPF bereits anlässlich der letzten Revision der VÜPF weiterhin offen, ob eine Entfernung der Verschlüsselung auch an dieser Stelle gefordert werden können soll. Angesichts der seit</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			Jahren erkennbaren Tendenz der Schweizer Überwachungsbehörden, die Anwendbarkeit des Überwachungsrechts laufend weiter auszudehnen und sich dabei nur durch Gerichte bremsen zu lassen, ist bei dieser Gelegenheit erneut die Klarstellung zu fordern, wonach die Entfernung von Verschlüsselungen, die erst in der Sphäre des Benutzers angebracht werden (wenngleich auch durch Software der Anbieterin) nicht verlangt werden darf. Dies ist zumindest im erläuternden Bericht zu erwähnen. Der erneute Verzicht wäre nichts anderes als eine Einladung an die Überwachungsbehörden, die Einführung einer offensichtlich illegalen und vom BÜPF keineswegs vorgesehenen «Chatkontrolle» auf dem «Auslegungsweg» vorzunehmen.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Artikel	Antrag	Begründung / Bemerkung	
VD-ÜPF / OME-SCPT / OE-SCPT			
Art. 14 Abs. 3 VD-ÜPF	Streichung	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit 5000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Absatz ist daher ersatzlos zu streichen.	
Art. 14 Abs. 4 VD-ÜPF	Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten.	Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der unterworfenen AAKD massiv. Dies ist wie beschrieben weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.	
Art. 20 Abs. 1 VD-ÜPF	Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.	

Prise de position sur la révision de l'OSCPT

Mai 2025, Centre de Genève pour la Neutralité

Introduction

Le Centre de Genève pour la Neutralité salue les efforts visant à adapter l'application de la loi aux réalités numériques actuelles. Cependant, nous exprimons de profondes préoccupations quant aux propositions actuelles, qui risquent de compromettre la réputation de la Suisse en tant que pays respectueux de la vie privée, tout en menaçant son écosystème numérique naissant et sa neutralité numérique.

Nous considérons notamment que la révision de l'OSCPT est contraire à la volonté populaire, à l'image de l'article 21A¹ de la constitution genevoise adopté par 94% de voies en 2023.

Arguments principaux

1. Excès par rapport aux normes européennes

L'ordonnance proposée va bien au-delà des lois allemande et européenne, risquant une censure par la Cour Européenne des Droits de l'Homme (CEDH). Une telle issue serait nuisible pour la réputation juridique et internationale de la Suisse. Nous recommandons fortement de simplifier l'ordonnance et d'attendre la décision de la CEDH (Glätti et al. c. Suisse) pour introduire les mesures plus radicales, qui risquent d'être dans tous les cas annulées.

2. Impact sur l'écosystème numérique suisse

Une grande partie de l'écosystème numérique suisse repose sur la simplicité de la législation actuelle et sur l'image de la Suisse comme un pays garantissant la confidentialité. Ces sociétés, qui offrent des solutions sécurisées utilisées même par le gouvernement et l'armée suisses, sont essentielles à notre souveraineté numérique. Les obligations d'indentification et de conservation des données secondaires pendant six mois, techniquement complexes et économiquement lourdes, menacent leur viabilité. Quel serait l'intérêt d'acheter des services numériques suisses si ceux-ci étaient soumis à des lois similaires à celles de la Russie ou de la Chine ? Une telle évolution pourrait pousser ces entreprises à délocaliser, affaiblissant ainsi l'autonomie numérique et l'économie helvétique.

3. Fragilisation de la neutralité numérique

La neutralité suisse, patiemment construite au fil des siècles, doit s'étendre au domaine numérique pour rester pertinente. Face aux bouleversements provoqués par le cloud, la blockchain et l'intelligence artificielle, la Suisse doit offrir un refuge sûr pour les utilisateurs de services numériques, à l'abri des conflits mondiaux. Les propositions actuelles, qui favorisent une surveillance accrue et fragilisent la confidentialité, vont à l'encontre de cet objectif. Nous

¹ Art. 21A al. 2 : *L'intégrité numérique inclut notamment le droit d'être protégé contre le traitement abusif des données liées à sa vie numérique, le droit à la sécurité dans l'espace numérique, le droit à une vie hors ligne ainsi que le droit à l'oubli.*

plaids pour des garanties solides de sécurité des données et le soutien aux entreprises éthiques, afin de bâtir un écosystème technologique résilient et attractif.

Recommandations

- **Approche minimaliste** : Limiter les obligations des fournisseurs de services de communication dérivés (FSCD) à ce qui est strictement nécessaire et conforme aux standards européens, en supprimant notamment la conservation obligatoire des données secondaires.
- **Soutien à l'innovation** : Baser les seuils d'application sur des critères économiques (comme le chiffre d'affaires par service) plutôt que sur des seuils arbitraires, pour protéger les PME et encourager l'innovation.
- **Renforcement de la neutralité** : Promouvoir les technologies sécurisées et éthiques, en évitant toute mesure qui affaiblirait le chiffrement ou la confidentialité, afin de consolider la position de la Suisse comme leader numérique neutre.
- **Simplification et prudence** : Nous recommandons de radicalement simplifier l'ordonnance et d'attendre la décision de la CEDH pour introduire les mesures plus radicales, qui risquent d'être rendues caduques.

Vision pour l'avenir

Nous proposons une Suisse numériquement neutre, reposant sur :

- **Respect des droits fondamentaux** : Une législation proportionnée et simplifiée, conforme aux normes internationales et au droit européen.
- **Promotion de l'innovation** : Un soutien aux entreprises technologiques éthiques, renforçant l'écosystème numérique helvétique.
- **Neutralité numérique** : Une infrastructure souveraine et des garanties de confidentialité, faisant de la Suisse un leader mondial des services numériques sécurisés.

Conclusion

La révision de l'OSCPT est une opportunité pour la Suisse de réaffirmer son engagement envers la vie privée, l'innovation et la neutralité numérique. Nous exhortons le Conseil fédéral à adopter une approche prudente et équilibrée, qui protège l'écosystème numérique suisse et renforce sa souveraineté dans un monde numérique en mutation. Le Centre de Genève pour la Neutralité reste disponible pour collaborer à l'élaboration d'un cadre réglementaire durable et respectueux des valeurs helvétiques.

Au nom du comité du Centre de Genève pour la Neutralité,

Nicolas Ramseier, Vice-président



Consultation relative aux révisions partielles de l'OSCPT et de l'OME-SCPT

Formulaire pour la saisie de la prise de position

Date	05.05.2025
Office	Département Fédéral de Justice et Police (DFPJ)
Personne de contact en cas de questions (Nom/tél./courriel)	Simon Janin, 076 268 09 44, s.janin@x80security.com

Merci d'envoyer votre prise de position par courrier électronique à aemterkonsultationen-uepf@isc-ejpd.admin.ch. Un envoi de **votre prise de position en format Word** par courrier électronique facilitera grandement notre travail. D'avance, merci beaucoup.

Remarques générales :

Nous approuvons en principe les révisions partielles de l'OSCPT et de l'OME-SCPT

OUI NON

La révision proposée outrepasse les objectifs déclarés du Conseil fédéral, qui visaient à simplifier le cadre pour les PME tout en maintenant une charge financière modérée. Au contraire, elle élargit la surveillance de manière indiscriminée, imposant des obligations techniques et financières écrasantes aux fournisseurs de services de communication dérivés (FSCD), y compris les PME. Cette approche remet en question la viabilité économique de certaines entreprises suisses emblématiques du respect de la vie privée et piliers de la souveraineté numérique helvétique, et pourrait les pousser à délocaliser.

Les obligations d'indentification et de conservation des données secondaires, notamment pour les FSCD, n'ont d'équivalent nulle part en Europe, où de telles pratiques ont été jugées illégales par la Cour de justice de l'Union européenne (CJUE) pour leur atteinte disproportionnée aux droits fondamentaux. En adoptant des mesures similaires à celles en vigueur en Russie et en Chine, la Suisse risque une censure par le Tribunal européen des droits de l'homme, ce qui entacherait gravement sa réputation internationale. Nous recommandons fortement de radicalement simplifier l'ordonnance et d'attendre les décisions de la Cour européenne avant d'introduire des mesures radicales, qui risquent d'être annulées et de discréditer la Suisse.

De plus, la complexité technique et juridique du texte, avec ses nombreuses références croisées, le rend inaccessible aux PME et même aux experts non spécialisés. Cette opacité crée une insécurité juridique incompatible avec un cadre réglementaire favorable à l'innovation.

Nous rejetons donc la révision et plaidons pour une approche minimaliste, alignée sur les standards européens, qui préserve la confidentialité, soutient l'écosystème numérique et renforce la neutralité numérique suisse.

Nicolas Ramseier, Vice-président du Centre de Genève pour la Neutralité

Remarques par rapport aux différents articles de l'OSCPT

Article	Proposition	Justification / Remarques	
OSCPT / OSCPT / OSCPT			
art. 50a	Supprimer sans remplacement	L'obligation de supprimer le chiffrement, imposée à tous les FSCD avec plus de 5 000 utilisateurs, est disproportionnée et dangereuse. Elle affaiblit la sécurité des systèmes, augmente les risques de cyberattaques et viole l'art. 13 de la Constitution suisse ainsi que la jurisprudence de la CEDH (PODCHASOV c. Russie, 2023). Cette mesure rend les VPN inopérants et compromet les services de messagerie chiffrés, nuisant à la compétitivité suisse.	
art. 60a (HD_62_IP)	Supprimer sans remplacement	La surveillance rétroactive (HD_62_IP) légalise une conservation généralisée des historiques IP, incompatible avec les standards européens (CEDH) et exposant les données à des risques d'intrusion.	
art. 42a & 43a (IR_59_EMAIL_LAST & IR_60_COM_LAST)	Supprimer sans remplacement	Les requêtes IR_59 et IR_60 permettent une surveillance automatisée sans contrôle juridique, équivalant à une surveillance généralisée et en temps réel. Elles imposent des coûts exorbitants et violent l'esprit de la LSCPT.	
art. 16	Supprimer ou revoir dans son intégralité	Le projet de rétention indiscriminée des données secondaires et les obligations d'identification pour les fournisseurs de services de communication (FSCD) éloigne la Suisse des standards européens. Par exemple, elle violerait en Union Européenne la jurisprudence de la CJUE, qui a jugé des mesures similaires comme contraires au droit à l'auto-détermination informationnelle. Le seuil arbitraire de 5 000 utilisateurs pour imposer ces obligations est tout aussi critiquable, ne répondant pas au critère de "significative importance" de la LSCPT et ciblant injustement les PME, startups et associations. Cette mesure freine l'innovation, crée une insécurité juridique et engendre des coûts de conformité exorbitants tout en augmentant les risques de cybersécurité. Avec seulement 1,6 % des ordres de surveillance en 2024 nécessitant ces données, ces obligations sont superflues et devraient être supprimées ou largement révisées pour protéger les droits fondamentaux et la compétitivité suisse.	

SATW
Schweizerische Akademie der
Technischen Wissenschaften
St. Annagasse 18
8001 Zürich
+41 44 226 50 11
info@satw.ch
www.satw.ch

SATW | St. Annagasse 18 | 8001 Zürich

EJPD
Frau Lan Lê und Herr Antonio Abate
Zu Handen Bundesrat Beat Jans

6. Mai 2025

**Vernehmlassungsantwort für die Teilrevisionen zweier Ausführungserlasse
zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)**



Sehr geehrte Frau Lê, Sehr geehrter Herr Abate

Wir danken Ihnen für die Möglichkeit zur Stellungnahme im Zusammenhang mit der Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF).

Nachfolgend finden Sie die Vernehmlassungsantwort von Mitgliedern des Advisory Boards Cybersecurity der SATW mit folgenden Teilen:

1. Einführung und grundsätzliche Bemerkungen
2. Begründung und inhaltliche Kommentare
3. Zusammenfassung
4. Liste der Träger

Wir danken Ihnen für die Kenntnisnahme und die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

A handwritten signature in black ink, appearing to read "B. Dubuis".

Prof. Benoît Dubuis | Präsident SATW

A handwritten signature in black ink, appearing to read "U. Annino".

Umberto Annino | Präsident Advisory Board Cybersecurity SATW

1 Einführung und grundsätzliche Bemerkung

Die Mitglieder des Advisory Board Cybersecurity der Schweizerischen Akademie der Technischen Wissenschaften SATW stehen den vorgeschlagenen Teilrevisionen der Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs kritisch gegenüber. Hiermit fordern wir Sie auf, auf die geplanten Änderungen zu verzichten und die Revisionen ersatzlos zu streichen.

2 Begründung und Inhaltliche Kommentare

Die Mitglieder des Advisory Boards Cybersecurity der SATW erachten den Anspruch der Schweizer Bürger:innen und der hier ansässigen Unternehmen auf Datenschutz, Vertraulichkeit und Sicherheit als ein unverzichtbares Gut. Demgegenüber sehen wir einen erneut ausgeweiteten Anspruch der Strafverfolgungsbehörden nach Zugriff auf private Systeme und Daten über die bestehenden gesetzlichen Regelungen hinaus als minder relevant und in der Umsetzung problematisch an. Mit den in den Ausführungserlassen vorgeschlagenen Revisionen wird die Sicherheit der Schweiz nicht erhöht, sondern im Gegenteil sogar geschwächt.

Aus fachlicher Sicht sind insbesondere die geforderte Entfernung von Verschlüsselungen sowie der geforderte Zutritt zu Rechenzentren inakzeptabel und nicht mit einem Anspruch an ein hohes und langfristig verlässliches Cybersicherheitsniveau vereinbar. Sie schwächen somit sowohl die legitimen Schutzansprüche der Bevölkerung als auch den Wirtschafts- und Produktionsstandort Schweiz.

Die Verschlüsselung von Daten, sei es bei der Übertragung oder bei der Speicherung, dient den legitimen Ansprüchen der Bürger:innen nach Vertraulichkeit, aber zum Beispiel auch dem Schutz von Steuerungsdaten für industrielle Anlagen und kritische Versorgungsinfrastrukturen mit unmittelbarem, ggf. nicht umkehrbarem Schadenspotential für die Schweiz. Ein schwaches Schloss bleibt ein schwaches Schloss und bietet eine signifikante Angriffsfläche, unabhängig davon, wer es aus welchem Grund öffnen möchte. Die Entfernung von Verschlüsselungen bedeutet entsprechend, dass kriminelle und terroristische Akteure sowie ausländische militärische oder wirtschaftliche Nachrichtendienste eine bisher signifikante Hürde weniger überwinden müssen. Mit der vorgeschlagenen Revision schlägt der Bundesrat somit vor, die Schweizer Bürger:innen diesem höheren Risiko, ohne taugliche korrigierende Massnahmen, auszusetzen. Aus unserer Sicht steht dieses Risiko auch im Lichte aktueller geopolitischer Entwicklungen in keinem Verhältnis zu den zusätzlich möglichen, geringfügigen Ermittlungserfolgen, die wesentlich stärker von anderen Faktoren, wie z.B. praxistauglichen Rechtshilfeabkommen, abhängen.

Wir beurteilen demzufolge den Nutzen der vorgeschlagenen Massnahmen als sehr gering bis nicht existent. Wie reale Fälle aus der Vergangenheit zeigen (u.a. Encrochat), nutzen Schwerkriminelle wie auch fremde Nachrichtendienste bereits heute eigene Kommunikationslösungen, die auch durch die geänderte Version der VÜPF nicht erfasst würden. Frei verfügbare open-source Lösungen wie TOR oder PGP würden also z.B. von Kriminellen immer noch genutzt werden, während Schweizer Bürger:innen, Unternehmen und Hochschulen unter Generalverdacht gestellt würden und auf ihr Recht auf Privatsphäre verzichten müssten.

Nicht zuletzt würde die vorgeschlagene Revision der VÜPF auch den Innovationsstandort Schweiz schwächen. Innovative Schweizer Unternehmen oder Forschungseinrichtungen und Unternehmen

mit schützenswerten Geschäftsgeheimnissen und Produktionsprozessen würden zum leichten Ziel fremder Aufklärungsdienste und könnten sich gezwungen sehen, in Staaten mit besserem Datenschutz und verlässlicheren Rahmenbedingungen auszuweichen. Dies hätte unweigerlich einen Abfluss von Fachwissen, aber auch Wertschöpfung aus der Schweiz zur Folge. Die Attraktivität von Neuinvestitionen in der Schweiz in wichtigen Zukunftsmärkten würde in einem ohnehin anspruchsvollen wirtschaftlichen und geopolitischen Umfeld erheblich sinken.

3 Zusammenfassung

Aus Sicht der Mitglieder des Advisory Boards Cybersecurity der SATW lässt sich somit zusammenfassend festhalten:

- Die geforderte Entfernung von Verschlüsselungen stellt eine generelle Schwächung des heute notwendigen Sicherheitsdispositivs dar, die auch kriminellen, terroristischen und staatlichen Akteuren einen einfacheren Zugriff auf die privaten Daten der Bürger:innen und Unternehmen ermöglicht. Ein schwaches Schloss bleibt ein schwaches Schloss.
- Die Erfahrung zeigt, dass schwerkriminelle und fremdstaatliche Akteure bereits heute auf eigene Kommunikationslösungen ausweichen oder frei verfügbare Lösungen mit starker Verschlüsselung verwenden, wie z.B. TOR oder PGP. Die Leidtragenden der vorgeschlagenen Änderungen wären die technisch weniger versierten Bürger:innen, Unternehmen und Hochschulen.
- Die Schweiz würde mit dieser Revision ihren Ruf als Hort der Privatsphäre und des Vertrauensverhältnisses zwischen Staat und Bürger:innen unnötig beschädigen und innovationshemmende Bedingungen schaffen, die dem Wirtschaftsstandort Schweiz schaden und zu einem Know-How-Abfluss im Bereich der datenschutzzentrierten IT-Dienstleistungen sowie in den davon betroffenen Industrien mit schützenswerten Gütern und Informationen führen.

4 Liste der Träger

- Umberto Annino | Microsoft
- Daniel Caduff | Amazon Web Services
- Dr. Stefan Frei | SDX Security
- Martin Leuthold | Switch
- Prof. em. Dr. Hannes Lubich | Verwaltungsrat und Berater
- Dr. Raphael Reischuk | Zühlke Engineering AG
- Daniel Walther | Swatch Group
- Dr. Andreas Wespi | IBM Research Lab



Opendata.ch
4000 Basel

Eidgenössisches Justiz- und Polizeidepartement
Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Basel, 05.05.2025

Vernehmlassungsantwort zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrte Damen und Herren

Gerne nehmen wir die Gelegenheit wahr, im Rahmen der Vernehmlassung zur Verordnung Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) Stellung zu nehmen.

Zweck und Tätigkeitsbereich des Vereins Opendata.ch

[Opendata.ch](#) engagiert sich dafür, Daten, Software und Wissen für das Gemeinwohl zu nutzen. Dazu...

- fördern wir offene, menschenzentrierte Projekte und Infrastruktur ([Hackathons](#), [Prototype Fund](#)),
- stärken wir die Kollaboration im Datenökosystem ([Working Groups](#), [Forum](#), [Hackathons](#)),
- setzen wir uns für förderliche rechtliche und politische Rahmenbedingungen ein,
- informieren und sensibilisieren wir die Öffentlichkeit ([Data Café](#)) und
- unterstützen wir den öffentlichen Sektor dabei, [offener](#), [menschenzentrierter](#) und [innovativer](#) zu werden.

Opendata.ch ist ein gemeinnütziger Verein und wurde 2012 gegründet. Wir sind Teil des internationalen [Open Knowledge Netzwerks](#). Zu den Mitgliedern des Vereins zählen Organisationen des öffentlichen Sektors und der Privatwirtschaft sowie Einzelmitglieder.

Stellungnahme

Vorbemerkung

Die geplante Revision der VÜPF ist ein Frontalangriff auf unsere Grundrechte, die Rechtsstaatlichkeit sowie den IT- und Innovationsstandort Schweiz.

Mit ihrer Umsetzung würde geltendes Recht in einem Ausmass verletzt, das alarmieren muss: Die Revision ist in vielerlei Hinsicht unvereinbar mit dem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), verstösst gegen das Datenschutzgesetz (DSG), steht in klarem Widerspruch zu den verfassungsmässigen Grundrechten und gegen Völkerrecht.

Die vorgesehenen Änderungen führen zu einer massiv ausgeweiteten und flächendeckenden Überwachung. Dies ist mit der Ausrichtung des BÜPF, das eine fein austarierte Interessenabwägung zwischen Freiheit und Privatsphäre einerseits und Sicherheit durch Überwachungsmassnahmen andererseits verfolgt, nicht vereinbar.

Die Auswirkungen auf den Wirtschafts- und Innovationsstandort Schweiz wären zudem verheerend: Die Ausweitung der Überwachung und die damit verbundenen, übermässigen Mitwirkungspflichten machen die Schweiz für IT-Anbieter unattraktiv. Renommierte Unternehmen wie Proton oder Threema, deren Geschäftsmodelle durch die Vorlage direkt ins Visier geraten, würden in ihrer Existenz bedroht. Die ersten Konsequenzen sind bereits sichtbar: Proton hat angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen (siehe [Tages-Anzeiger vom 1. April 2025](#)), Der Chef des Unternehmens erklärte in einem Interview: «Diese Entscheidung ist wirtschaftlicher Selbstmord für die Schweiz» ([watson.ch vom 9. April 2025](#)). Ähnlich äussert sich Threema-Chef Robin Simon: «Der Wirtschaftsstandort würde durch die Revision geschwächt und für Tech-Start-ups unattraktiv.» Aktuell lasse sich Threema alle Optionen offen ([Tages-Anzeiger vom 8. April 2025](#)). Diese Warnzeichen sind ernst zu nehmen und auf diese Revision ist zu verzichten.

Der grundrechtlich garantierte Anspruch auf sichere und vertrauliche Kommunikation darf nicht ausgehöhlt werden. Wenn Anbieter abwandern, bleibt – als wäre dies nicht genug – nicht nur privaten Nutzer:innen der Zugang zu geschützten Kommunikationsmitteln verwehrt, sondern auch besonders schutzbedürftige Gruppen wie Journalist:innen, Whistleblower:innen oder politische Akteur:innen kämen massiv in Bedrägnis ohne vertrauliche und gesicherte Kommunikationswege. Kurz: Die Revision ignoriert Grundrechte und zentrale Schutzbedürfnisse und erweitert stattdessen einseitig die Eingriffsbefugnisse des Staates und dehnt die persönlichen Mitwirkungspflichten ebenso wie den Kreis der Mitwirkungspflichtigen enorm aus.

Hinzu kommt: Die geplanten Regelungen sind technisch unausgereift, unnötig komplex und in Teilen schlicht nicht umsetzbar. Vielmehr wird ein kaum noch durchschaubares Normengeflecht geschaffen, das weder den Mitwirkungspflichtigen noch den Betroffenen ein Mindestmass an Rechtsklarheit bietet, obwohl die Revision präsentiert wird, als handle es sich dabei um Änderungen zur besseren Überblickbarkeit der Rechtslage und zur Schaffung von mehr Rechtssicherheit.

Wir halten es im Übrigen für unzulässig, dermassen einschneidende Ausweitungen von Pflichten auf Verordnungsstufe vorzunehmen; sie sind angesichts der einschneidenden und weitreichenden Konsequenzen zwingend in Gesetzesform zu erlassen. Der Bundesrat überschreitet seine Kompetenzen, wenn er auf dieser Rechtsstufe im grossen Stil verfassungsmässig geschützte Rechte aushebeln will. Aus grundrechtlicher, datenschutzrechtlicher und gesellschaftspolitischer Sicht ist dies inakzeptabel. Die geplanten Änderungen stehen dem erklärten Ziel von mehr Freundlichkeit sowie allgemeinen rechtsstaatlichen Grundsätzen sowie Schutzbedürfnissen Einzelner diametral entgegen.

Wir lehnen die Revision volumnfänglich und in aller Deutlichkeit ab, begründen aber gerne noch im Detail unseren Standpunkt; wir folgen dabei der Argumentation der Digitalen Gesellschaft:

Bemerkungen zu einzelnen Artikeln der VÜPF

Alle Artikel

Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung (Art. 6 Abs. 3 DSG) gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kund:innen auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.

Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.ä. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.

Antrag: Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.

Art. 16b Abs. 1

Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile (Art. 16b Abs. 1 lit. b Ziff. 2 VE-VÜPF) wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Mitwirkungspflichten in Kauf nehmen.

Dazu kommt, dass das Kriterium bezüglich der Überwachungsaufträge nicht vom BÜPF gestützt wird, denn: Die Anzahl von Überwachungsaufträgen ist von der wirtschaftlichen Bedeutung einer FDA völlig losgelöst. Die wirtschaftliche Bedeutung ist aber gemäss Art. 26 Abs. 6 BÜPF ausschlaggebend dafür, ob eine FDA von den vollen Pflichten (teilweise) befreit werden kann. Im Umkehrschluss ist die wirtschaftliche Bedeutsamkeit somit Erfordernis für die Auferlegung von vollen Pflichten. Wenn eine FDA nun aber rein aufgrund einer bestimmten Anzahl von Überwachungsaufträgen nach Art. 16b Abs. 1 lit. b Ziff. 1

VE-VÜPF als vollpflichtige FDA qualifiziert wird, steht dies im Widerspruch zum BÜPF und entbehrt damit einer Rechtsgrundlage.

Dieses bereits in der aktuellen Version der VÜPF vorhandene Problem sollte im Zuge einer Revision nicht bestehen bleiben, sondern muss behoben werden.

Antrag: Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.» Es ist auf die Regelung in Art. 26 Abs. 6 BÜPF abzustellen und eine Einzelfallbetrachtung zur Einstufung vorzunehmen.

Art. 16c Abs. 3

Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als «natürliche» Schutzmechanismen gegen eine übermässige oder missbräuchliche Nutzung solcher Massnahmen durch die Untersuchungsbehörden. Die automatisierte Erteilung von Auskünften ist unverhältnismässig und widerspricht dem Prinzip der Datenminimierung. Die pauschale und undifferenzierte Regel beeinträchtigt zwangsläufig den Grundrechtsschutz.

Der vorgesehene Umsetzungszeitraum von 12 Monaten zur Umsetzung eines dermassen komplexen Systems ist ausserdem völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.

Antrag: Streichung von lit. a «automatisierte Erteilung der Auskünfte» (ebenso in Art. 18 Abs. 2).

Art. 16d

Eine klarere Definition des Begriffs AAKD ist begrüssenswert, doch die neue Auslegung geht nach den Ausführungen im erläuterndem Bericht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdielen wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter etc.) genutzt werden.

Art. 2 lit. c BÜPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft jedoch auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug in die Auslegung unrechtmässig ist – auch hier setzt sich die Revision inakzeptabel über die gesetzlichen Vorgaben des BÜPF hinweg.

Onlinespeicherdielen sind deshalb aus Art. 16d zu streichen.

Zudem anerkennt der erläuternde Bericht zwar, dass VPNs zur Anonymisierung der Nutzer:innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil angebrachte Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Das Bedürfnis, auch künftig VPN-Dienste in Anspruch nehmen zu können, ist zu schützen und darf nicht vereitelt werden. Anbieter von VPNs sind daher ebenfalls aus Art. 16d auszunehmen.

Es ist irritierend, dass die bewusst separat ausgestalteten Kategorien AAKD und FDA einander zunehmend angeglichen werden, und zwar zuungunsten der AAKD, die als Kategorie mit grundsätzlich weniger weitreichenden Pflichten als die FDA konzipiert wurde. Dies missachtet den Willen des Gesetzgebers, den es zu wahren gilt.

Antrag: Streichung von Onlinespeicherdielen und VPN-Anbietern in der Auslegung

Art. 16e, Art. 16f und Art. 16g

Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch komplett entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung mit deutlich erweiterten Pflichten. Entscheidend ist, dass neuerdings das Kriterium von 5'000 Nutzer:innen allein zum Auferlegen massiver Überwachungspflichten ausreicht: Erreicht eine AAKD diese Grösse, fällt sie neu in die Kategorie der AAKD mit reduzierten Pflichten und untersteht somit bereits sehr weitgehenden Mitwirkungspflichten, insbesondere der Identifikationspflicht.

Die Einführung von 5'000 Nutzern:innen als gesondert zu beurteilende Untergrenze verletzt Art. 27 Abs. 3 BÜPF, denn 5'000 Personen sind keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strengereren Überwachungsmassnahmen, gerechtfertigt wären. 5'000 Nutzer:innen werden in der digitalen Welt vielmehr sehr rasch erreicht – die Revision verkennt technische Realitäten.

Zusätzlich führt das Einführen eines Konzernatbestandes in Art. 16f Abs. 3 zu massiven Problemen: Produkte und Dienste müssen nicht mehr für sich allein bestimmte Schwellenwerte erreichen – es genügt, wenn das Mutterunternehmen oder verbundene Gesellschaften diese überschreiten. Insbesondere bei Unternehmen mit Beteiligungsstrukturen führt dies dazu, dass sämtliche Angebote pauschal der höchsten Überwachungsstufe unterstellt werden – unabhängig davon, ob sich einzelne Dienste noch im frühen Entwicklungsstadium befinden oder faktisch kaum genutzt werden. Somit müsste jedes neue Projekt von Beginn an mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden, was Innovation behindert. Zudem missachtet der Konzernatbestand das Verhältnismässigkeitsgebot: Unterschiedliche organisatorische Einheiten mit eigenständigen Angeboten werden unrechtmässig zusammengefasst, obwohl sie individuell zu prüfen wären. Die Anwendung starrer Schwellen auf ganze Konzerne statt auf einzelne Dienste umgeht eine notwendige Einzelfallprüfung.

Eine solche Regelung stünde sodann *im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali*, das die zu seltene Anwendung von Downgrades kritisierte: «Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»

Statt KMU zu entlasten, führt die Revision neu zu einem «*automatischen Upgrade per Verordnung ohne Verfügung* (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.

Eine Analyse der offiziellen VÜPF-Statistik unterstreicht diese offensichtliche Unverhältnismässigkeit. Im Jahr 2023 betrafen 98,97% der total 9'430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,03% für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,74% wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100% des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.

Die neue Vorlage schliesst nun ebenfalls sowohl die Registrierung via normaler E-Mail als auch die komplett anonyme Registrierung (z. B. Signal oder Telegram) aus, da AAKD bereits mit reduzierten Pflichten neu automatisch zwingend die Endnutzer:innen identifizieren müssen. Hiervon betroffen sind nicht nur alle AAKD mit reduzierten Pflichten, sondern auch all deren Wiederverkäufer. Faktisch resultiert das Gesetz somit darin, dass man sich bei keinem Dienst mehr anmelden können soll, ohne den Pass, Führerschein oder die ID entweder direkt oder indirekt zu hinterlegen. Dass Nutzer:innen künftig hierzu gezwungen wären, stellt einen massiven Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 BV) dar und ist unzumutbar.

Ein weiteres Kernproblem, das die automatische Hochstufung mit sich bringt, ist die Rechtsunsicherheit. Die Vorlage will mit klarer definierten Kategorien und Pflichten eine übersichtlichere Situation schaffen, verfehlt dieses Ziel jedoch gänzlich. Bislang fand die Hochstufung per Verfügung statt, wodurch es für die Mitwirkungspflichtigen klar erkennbar war, wann sie unter welche Pflichten fallen. Ausserdem bewirkt diese Praxis eine sinnvolle Einzelfallbetrachtung anstelle pauschaler und unzweckmässiger automatischer Hochstufungen. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den massgebenden Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes kann aber im Zweifelsfall nur schwer zu beantworten sein. Gerade deshalb besteht ein schutzwürdiges Interesse der Anbieter an Klarheit über ihre Pflichten, da sie fortan eventuell die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Diese Umstrukturierung lässt ich nicht mit der Funktionsweise von Verwaltungsverfahren vereinbaren. Die Pflicht zur Abklärung, wann eine Hochstufung vorliegt und was diese für das Unternehmen bedeutet, darf nicht in die Verantwortung der Unternehmen fallen. Der Staat zieht sich hier aus der Verantwortung und schiebt diese den Unternehmen zu,

wodurch diesen zwangsläufig zeitlicher und finanzieller Mehraufwand entsteht. Von einer automatischen Hochstufung von AAKD ist daher abzusehen. Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.

Gegenüber der geltenden VÜPF *erweitert die Revision die Pflichten zur Automatisierung noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragetypen wie z. B. "IR_59" und "IR_60", welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen*. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.

Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 lit. b der geltenden VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grosse[n] Teil ihrer Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. *Damit fallen auch Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz*. Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Auch hiermit werden neue Hürden für Innovation geschaffen. Die Regelung ist unverhältnismässig und nicht sachdienlich.

Auch Non-Profit-Organisationen geraten unter die verschärften Vorgaben. Unter den neuen Kriterien wird aber allein auf die Anzahl der Nutzer:innen abgestellt für die Einstufung als AAKD. Dieses Kriterium greift jedoch zu kurz: Es berücksichtigt insbesondere nicht die wirtschaftliche Tragfähigkeit der Anbieter:innen. Gerade bei Open-Source- und Non-Profit-Lösungen mit grosser Reichweite, aber geringem Budget, führt dies zu einer verheerenden finanziellen Belastung: Anbieter:innen mit solchen Projekten würden gezwungen, umfangreiche Überwachungsmassnahmen einzuführen. Solche Anbieter:innen würden gezielt aus dem Schweizer Markt gedrängt, während gleichzeitig bestehende Monopole wie WhatsApp (96% Marktanteil in der Schweiz) gestärkt würden.

Es muss ausserdem klar festgehalten werden, dass sich das BÜPF und die VÜPF nur auf Anbieter:innen beziehen können, die in der Schweiz tatsächlich tätig sind. Die Erlasse dürfen nicht so ausgelegt werden, dass sie eine extraterritoriale Wirkung entfalten und internationale Dienste wie Signal, WhatsApp oder Microsoft Teams erfasst sind.

Das Kriterium der reinen Nutzer:innenzahl ist ungeeignet und muss gestrichen werden.

Die Regelung schwächt auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade us-amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger:innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer,

End-zu-End-verschlüsselter Kommunikation ist heute wichtiger denn je und fällt in den Bereich grundrechtlich geschützter Ansprüche, die es zu wahren gilt. Diese Ansprüche dürfen nicht aufs Spiel gesetzt werden, um ein knallhartes Überwachungsregime der Kommunikation in der Schweiz durchzusetzen – die Prioritäten werden höchst fragwürdig gesetzt.

Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade illegal ist (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer:innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, diese zu erhebenden Datenmengen sind von enormem Ausmass und bergen folglich massive Risiken für Hackerangriffe.

Des Weiteren ist nicht belegt, dass die Speicherung der betreffenden Daten zu spürbar mehr erfolgreichen Ermittlungen führt. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisbrauch via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfüge, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden. Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren. Diese Handhabe bedeutet einen Verstoss gegen das Legalitätsprinzip und untergräbt legislative Kompetenzen. Ausserdem verfügt die Schweiz bereits über reichlich Mittel zur Aufklärung und Verfolgung von Straftaten, die Behörden können bereits heute auf sicherheitsrelevante Daten zurückgreifen. Unternehmen wie Proton (s. «Positionspapier zur Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)» von Proton) kooperiert seit Jahren mit den Schweizer Strafverfolgungsbehörden und dem Nachrichtendienst des Bundes (NDB). Wenn nun solche Unternehmen aus bereits genannten Gründen zur Abwanderung gezwungen werden, bewirkt die Revision auch hier das genaue Gegenteil ihrer erklärten Ziele: Anstatt der Schaffung besserer Möglichkeiten zur Strafverfolgung würden die Schweizer Behörden wie etwa Fedpol den Zugriff auf wichtige Partner bei der Beschaffung sicherheitsrelevanter Daten verlieren.

Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Souveränität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.

Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das DSG. Der Entwurf bringt nicht, wie der Begleitbericht den Leser:innen weismachen will,

eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit, steht in direktem Gegensatz zum besagten Postulat 19.4031 und bedeutet massive Eingriffe in grundrechtlich geschützte Sphären, sowohl von Unternehmen als auch von Nutzer:innen.

Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen und das bestehende System muss beibehalten werden.

Antrag: Streichung der Artikel und Beibehaltung der bestehenden Kriterien. Alternativ: Änderung des Schwellenwerts für die Hochstufung auf 1 Million Nutzer (aber unter 100 Millionen Umsatz) und individuelle Betrachtung des betroffenen Dienstes zur Bestimmung dieses Schwellenwertes. + Ausnahmen für Pilotprojekte (auch von grossen Firmen) und Non-Profits per se. Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).

Art. 16h

Art. 16h konkretisiert die Kategorie der «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» aus Art. 2 lit. e BÜPF. Die Vorschrift verfehlt ihr Ziel – anstatt Unsicherheiten darüber zu beheben, wer unter diese Kategorie fällt, schafft sie weitere Unklarheiten. Der schwammig formulierte Verordnungstext könnte dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist:innen, Whistleblower:innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber:innen solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer:innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen. Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt. Die Unklarheit bezüglich der Einordnung von TOR-Servern wirft weitere Fragen auf, denn wenn TOR nicht als PZD zu qualifizieren ist, müsste TOR – gleich wie die VPNs – der Kategorie der AAKD zugeordnet werden. Somit stünden Betreiber:innen von TOR-Servern – wie etwa die Digitale Gesellschaft – unter der Identifikationspflicht. Diese ist jedoch, wie dargelegt, nicht umsetzbar.

Es braucht somit entweder die Zusicherung, dass Betreiberinnen von TOR-Nodes nicht dem BÜPF und der VÜPF unterstellt sind oder aber Kategorien von Mitwirkungspflichten, die so gestaltet sind, dass ein:e Betreiber:in eines TOR-Nodes nicht einer Identifikationspflicht unterstellt wird – z. B. indem die Schwelle für das Auferlegen der Identifikationspflicht auf 1 Mio. Nutzer:innen angehoben wird.

Wären Betreiber:innen von TOR-Nodes von der Identifikationspflicht erfasst, würde dies fundamentale Grundrechte wie das Recht auf Privatsphäre und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK), die Meinungs- und Informationsfreiheit (Art. 16 BV, Art. 10 EMRK) gefährden. Ebenso würde das datenschutzrechtliche Prinzip der Datensicherheit (Art. 8 DSG) komplett unterlaufen. Diese Eingriffe in national und international geschützte Rechtsansprüche sind nicht hinzunehmend.

Dieser potentielle Angriff auf die genannten Grundrechte ist hochproblematisch und setzt ein politisches Statement: Die Schweiz bewegt sich weg von Grundrechtsschutz hin zum hochgerüsteten Überwachungsstaat.

Antrag: Es muss sichergestellt werden, dass Technologien wie TOR oder I2P nicht vom Anwendungsbereich der VÜPF erfasst sind.

Art. 16h Abs. 2

Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Endbenutzer:innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 VE-VÜPF: Gemäss diesem Artikel trägt die das WLAN erschliessenden FDA die Verantwortung zur Identifikation der Nutzer:innen. Die Regelung führt also dazu, dass FDA, die einen Vertrag haben mit «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» (PZD), sehr schnell für die Identifikation der Endnutzer:innen ihrer Vertragspartner zuständig sind. Diese Regelung ist unsinnig und schlicht nicht umsetzbar.

Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer:innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24), die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22) oder der Verwendung von IPv6. Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDA unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden.

Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten: FDA resp. Anbieterinnen von öffentlichen WLAN-Zugängen dürfen nur unter einer Identifikationspflicht stehen, wenn die PZD, die den Zugang der FDA nutzt, «professionell betrieben» ist – und zwar nach der aktuellen Auslegungsform (s. Erläuternder Bericht zur (letzten)Totalrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs):

«Mit "professionell betrieben" ist gemeint, dass eine FDA oder eine auf öffentliche WLAN-Zugangspunkte spezialisierte IT-Dienstleisterin den technischen Betrieb des öffentlichen WLAN-Zugangspunktes durchführt, die dies auch noch für andere öffentliche WLAN-Zugangspunkte an anderen Standorten macht. Wenn eine natürliche oder juristische Person an ihrem Internetzugang selbst einen öffentlichen WLAN-Zugangspunkt technisch betreibt und diesen Zugang Dritten zur Verfügung stellt, muss die FDA, die den Internetzugang anbietet, keine Identifikation der Endbenutzenden sicherstellen.»

So wird sichergestellt, dass FDA nicht unmöglich umzusetzenden Pflichten unterstellt werden.

Antrag: Streichung der Ausführung im erläuternden Bericht. Das Kriterium «professionell betrieben» ist nach der bislang geltenden Regelung zu verstehen. Art. 16h Abs. 2 ist ersatzlos zu streichen und im Zusammenhang mit Art. 19 Abs. 2 ist auf die aktuelle Definition von «professionell betrieben» abzustellen.

Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2

Bei Konzernen knüpft die VE-VÜPF nicht mehr an die Umsatz- und Nutzer:innenzahlen des betroffenen Unternehmens an, neu sind die Zahlen des Konzerns ausschlaggebend für eine Hoch- oder Herunterstufung. Die Begründung, dies diene der Vereinfachung, ist unlogisch und irreführend: Unternehmen müssen ihre Zahlen ohnehin produktbezogen ausweisen, die nötigen Daten liegen also längst vor. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.

Antrag: Streichung des «Konzerntatbestand» und Beibehaltung der bestehenden Regelung.

Art. 19 Abs. 1

Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD – erfasst sind die AAKD mit reduzierten und mit vollen Pflichten – widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht. Durch die neuen Schwellenwerte zur Einstufung findet eine beachtliche Ausweitung der Identifikationspflicht statt.

Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des DSG, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch insbesondere der Grundrechtsschutz von Nutzer:innen in der Schweiz massiv beeinträchtigt wird. Die Identifikationspflicht greift immens in das Recht auf informationelle Selbstbestimmung ein und hält einer Grundrechtsprüfung nach Art. 36 BV schon allein aufgrund ihrer Unverhältnismässigkeit nicht stand.

Bezüglich einschneidender Pflichten, die potentiell schwere Grundrechtseingriffe bedeuten – wie es bei Identifikationspflichten zweifellos der Fall ist – muss Rechtsetzung in jedem Fall mit äusserster Sorgfalt und unter strenger Beachtung des Verhältnismässigkeitgebots erfolgen. Ausserdem darf sich eine solche Pflicht nicht über gesetzliche Vorgaben, wie in diesem Fall vom BÜPF vorgegeben, hinwegsetzen.

Durch die breite Auferlegung einer solchen Pflicht werden datenschutzfreundliche Unternehmen bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.

Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Nur so können datenschutzrechtliche Vorgaben und die Rechte Betroffener gewahrt werden.

Antrag: Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation von Teilnehmenden.

Art. 18

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 19 Abs. 2

Das Kriterium «professionell betrieben» ist nach der bestehenden Regelung auszulegen (s. vorstehen). Es sei ausserdem darauf hingewiesen, dass sich aus dieser Regelung eine vertragsrechtliche Problematik zwischen den FDA und den PZD ergeben würde, die nicht tragbar ist.

Antrag: Auslegung des Kriteriums «professionell betrieben» nach der bestehenden Regelung und nicht i. S. v. Art. 16h Abs. 2.

Art. 21 Abs. 1 lit. a

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.

Antrag: Streichung

Art. 22

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.

Antrag: beibehalten

Art. 11 Abs. 4

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.

Antrag: Streichung

Art. 16b

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.

Antrag: Streichung

Art. 31 Abs. 1

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 51 und 52

Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.

Antrag: beibehalten

Art. 60a

Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde laut den Erläuterungen bewusst auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten. Art. 60a ist zu streichen.

Antrag: Streichung des Artikels

Art. 42a und 43a

Die Art. 42a und 43a Die genannten Artikel führen neu die Abfragetypen «IR_59» und «IR_60» ein, über die sensible Daten automatisiert abgefragt werden können. Sie verlangen von Anbietern, dass sie jederzeit Auskunft geben können bezüglich des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Auch für das Auferlegen dieser Pflicht gilt die fragliche Schwelle von 5'000 Nutzer:innen. Erfasst ist somit nahezu die gesamte AAKD-Landschaft der Schweiz.

Das Problem liegt darin, dass die «IR_»-Abfragen zu Informationen nach Art. 42a und 43a neu automatisiert abgerufen werden können – im Gegensatz zu den «HD_»- (historische Daten) und «RT_» (Echtzeitüberwachung) Abfragen, die strengeren Regeln und einer juristischen Kontrolle unterliegen. Bei den «IR_59»- und «IR_60»-Abfragen handelt es sich allerdings um sensible Informationen wie etwa das Abrufen einer IP-Adresse. Solche Informationen mussten bislang zurecht über strengere Abfragetypen eingeholt werden. Es ist nicht nachvollziehbar, warum Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber.

Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser automatisierten Auskünfte ergibt. Unternehmen sind daher nur unzulänglich geschützt vor missbräuchlichen Anfragen und vor Kosten, die ihnen durch die Pflicht, diese Auskünfte automatisch weiterzugeben, entstehen wird.

Künftig könnten so umfangreiche Informationen über die neuen Abfragetypen beschafft werden, die bislang zurecht den strengerden Regeln der rechtlich sichereren Informations-/Überwachungstypen «HD_» und «RT_» unterworfen waren. «IR_59» und «IR_60» ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne den erforderlichen Kontrollen dieser invasiven Überwachungstypen unterworfen zu sein.

Die Entwicklung, dass mittels «IR_»-Abfragen neu auch personenbezogene sensible Nutzungsdaten eingeholt werden können, widerspricht der Logik der unterschiedlichen Abfragetypen und öffnet Tür und Tor für missbräuchliche Abfragen und eine Echtzeitüberwachung von Millionen von Nutzer:innen. Auch hier stehen grundrechtlich geschützte Ansprüche auf dem Spiel, die mit einer solchen Regelung auf nicht nachvollziehbare Weise untergraben und missachtet werden.

Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind. Die AAKD müssten künftig gewisse Datenkategorien systematisch erheben, um dieser Pflicht nachzukommen. Art. 27 Abs. 2 BÜPF erklärt allerdings, dass AAKD «auf Verlangen die *ihr* zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person liefern» müssen. Bei einer dahingehenden Auslegung des Bestimmungen bedeutete dies einen weiteren Verstoss gegen das BÜPF.

Die beiden Artikel sind daher vollumfänglich zu streichen.

Antrag: Streichung der Artikel

Art. 50a

Art. 50a sieht vor, dass Anbieter:innen verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Auch diese Pflicht soll eine Vielzahl neuer Unternehmen erfassen: Betroffen sind nicht mehr nur FDA (Art. 26 BÜPF) und ausnahmsweise AAKD (Art. 27 BÜPF), sondern sämtliche Anbieter:innen mit mehr als 5'000 Nutzer:innen. Im Ergebnis wäre fast die gesamte Schweizer AAKD-Branche betroffen (kaum ein Produkt ist lebensfähig mit weniger als 5'000 Teilnehmer:innen).

Die Ausdehnung dieser Pflicht auf AAKD stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar: Es findet keine Einzelfallprüfung statt und die AAKD werden dieser Pflicht unterworfen, auch wenn sie keineswegs «Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten», was jedoch gesetzliche Vorgabe ist (Art. 27 Abs. 3 BÜPF).

Problematisch ist zudem, dass aufgrund dieser Vorgabe Anbieter:innen ihrer Verschlüsselungen so konfigurieren müssen, dass sie von ihnen aufgehoben werden können – eine durch Anbieter:innen aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung allerdings in jedem Fall. Dies führt zu schwächeren Verschlüsselungen und der Abnahme der Sicherheit von Kommunikationsdiensten.

Daraus ergibt sich eine Grundrechtsproblematik von erheblicher Tragweite: Das Verhältnismässigkeitsgebot aus Art. 36 BV kann nicht eingehalten werden, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer

Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Die Interessenabwägung darf hier nicht zuungunsten der Grundrechtsträger:innen erfolgen, da es sich bei deren Interessen um solche von fundamentalem Gewicht – dem Zugang zu sicherer Kommunikation und damit direkt verbunden dem Recht auf freie Meinungsäußerung – handelt.

Wichtig ist, dass Verschlüsselungen, die auf dem Endgerät der Nutzer:innen erfolgen – also End-zu-End-Verschlüsselungen – nicht unter die Pflicht zur Aufhebung gemäss Art. 50a VE-VÜPF fallen dürfen. Diese Form der Verschlüsselung liegt ausschliesslich in der Sphäre der Nutzer:innen und es wäre untragbar, die Pflicht zur Aufhebung von Verschlüsselungen in dieser Sphäre zu verlangen. Die Anbieter:innen dürfen daher nicht dazu verpflichtet werden, diese Inhalte zu entschlüsseln und zugänglich zu machen. Im Gegensatz dazu betrifft die Transportverschlüsselung «lediglich» die Verbindung zwischen Client und Server und kann von Anbieter:innen kontrolliert werden. Es ist wichtig, dass diese technischen Unterscheidungen und unterschiedlichen Schutzwirkungen und -richtungen bei rechtlichen Umsetzungen beachtet werden. Wir begrüssen die Klarstellung im erläuternden Bericht, dass die End-zu-End-Verschlüsselung vom Anwendungsbereich ausgenommen ist. Es muss jedoch ebenso klar sein, dass das ganze Endgerät von Nutzer:innen aus dem Anwendungsbereich von Art. 50a VE-VÜPF ausgenommen ist.

Es braucht im Übrigen auch eine Klarstellung darüber, dass eine rückwirkende Möglichkeit zur Aufhebung klar ausgeschlossen ist. Eine solche würde de facto eine Vorratsdatenspeicherung verschlüsselter Inhalte und Keys darstellen, die mit dem Prinzip der Datenminimierung (Art. 6 Abs. 3 DSG) und dem Schutz der Privatsphäre (Art. 13 BV) unvereinbar ist.

Antrag: Streichung der «Anbieterin mit reduzierten Pflichten» aus dem Anwendungsbereich sowie eine Klarstellung darüber, dass die Aufhebung von Verschlüsselungen auf dem Endgerät der Nutzer:innen sowie eine rückwirkende Verpflichtung zur Aufhebung ausgeschlossen sind.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Art. 14 Abs. 3 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und wirtschaftlich nicht tragbar, was das Einführen von Fristen obsolet werden lässt. Der Absatz ist daher ersatzlos zu streichen.

Antrag: Streichung

Art. 14 Abs. 4 VD-ÜPF

Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der Unterworfenen AAKD – da auch AAKD mit reduzierten Pflichten erfasst sind – massiv. Dies ist wie bereits ausgeführt weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.

Antrag: Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten»

Art. 20 Abs. 1 VD-ÜPF

Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen, ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.

Antrag: Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»

Schlussbemerkung

Trotz des Umfangs dieser Stellungnahme gilt: Das Ausbleiben von expliziten Bemerkung zu anderen Bestimmungen bedeutet keine Zustimmung. Opendata.ch lehnt, wie oben schon festgehalten, diese Revision volumnfänglich ab.

Freundliche Grüsse



Andreas Kellerhals, Präsident



Florin Hasler, Geschäftsleiter

Crissier, 06.05.2025

Eidgenössisches Justiz- und Polizeidepartement EJPD
Informatik Service Center ISC-EJPD
Eichenweg 3
3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat Jans

Sehr geehrte Damen und Herren

Der Verband SDCA – Swiss Data Center Association dankt für die Gelegenheit Stellung zu nehmen zur geplanten Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF), welche der Bundesrat am 29.01.2025 eröffnet hat.

Die SDCA vertritt Unternehmen im Bereich Rechenzentren und digitale Infrastruktur in der Schweiz – ein Sektor, der auf Rechtssicherheit, stabile Rahmenbedingungen und Vertrauen in den Standort Schweiz angewiesen ist. Wir beobachten mit grosser Sorge, dass die vorgeschlagene Revision zentrale Prinzipien der Verhältnismässigkeit und Gesetzeskonformität verletzt.

Nach eingehender Prüfung kommen wir zum Schluss, dass die Vorlage in ihrer aktuellen Fassung nicht tragbar ist. Wir lehnen die Teilrevision in dieser Form klar ab und fordern deren vollständige Rückweisung. Für detaillierte technische Anmerkungen verweisen wir auf die umfassende Stellungnahme des Verbandes Swico und des Weiteren auf die Stellungnahme von Digitalswitzerland. Nachfolgend erläutern wir unsere zentralen Einwände.

Die Revision ist unverhältnismässig

Die geplanten Änderungen stellen einen tiefgreifenden Eingriff in die Freiheitsrechte von Unternehmen und Individuen dar. Dies betrifft insbesondere die Privatsphäre und den Datenschutz.

So sollen neu auch Anbieter abgeleiteter Kommunikationsdienste (AAKD) schon ab einem Schwellenwert von 5'000 Nutzer:innen mit weitreichenden Pflichten wie Identifikationspflicht, Vorratsdatenspeicherung oder 24/7-Pikettdiensten belegt werden – und das unabhängig von ihrer tatsächlichen wirtschaftlichen Bedeutung oder Sicherheitsrelevanz. Diese Schwelle ist mit den heutigen digitalen Geschäftsmodellen schnell erreicht und betrifft faktisch einen Grossteil der marktaktiven Anbieter, auch viele kleine und mittlere Unternehmen (KMU).

Solche neuen Verpflichtungen stellen nicht nur eine inhaltliche Ausweitung der Überwachung dar, sondern verstossen auch gegen den Willen des Gesetzgebers, der im Bundesgesetz BÜPF explizit zwischen Fernmeldediensten und AAKD unterscheidet und Letztere grundsätzlich von aktiven Überwachungspflichten befreien wollte.

Darüber hinaus sind mehrere der vorgesehenen Pflichten rechtlich bedenklich. Insbesondere die Schwächung oder Umgehung von Verschlüsselungssystemen (Art. 50a E-VÜPF) steht in direktem Widerspruch zum Schutz vertraulicher Kommunikation und schaffen neue Sicherheitslücken.

Gefährdung des Innovations- und Digitalstandort Schweiz

Ein zentraler Erfolgsfaktor des ICT- und Rechenzentrumsstandorts Schweiz ist das internationale Vertrauen in seine liberalen, rechtsstaatlich verankerten Rahmenbedingungen. Die Digitalisierung braucht klare Regeln, aber auch Raum für Innovation und Wachstum.

Mit der vorgeschlagenen Revision würde jedoch ein regulatorisches Klima geschaffen, das Investitionen hemmt, Innovationen blockiert und die Wettbewerbsfähigkeit der Schweiz massiv beeinträchtigt.

Insbesondere technologiegetriebene Anbieter, darunter auch viele aus dem Bereich sicherheitsrelevanter digitaler Dienste, müssen sich heute gut überlegen, wo sie ihre Produkte entwickeln und betreiben. Die geplante Ausweitung der Überwachungspflichten wirkt abschreckend auf international tätige Unternehmen, die hohe Datenschutzstandards erfüllen müssen oder deren Geschäftsmodelle auf dem Schutz der Privatsphäre beruhen.

Ein Abwandern solcher Unternehmen oder der Verzicht auf neue Standorte in der Schweiz hätte direkte Auswirkungen auf Beschäftigung, Know-how, Investitionen und Innovationskraft – gerade in strategisch wichtigen Bereichen wie Cloud-Computing, AI oder digitaler Kommunikation.

Der Standort Schweiz lebt vom Vertrauen in seine Rechtsordnung. Wird dieses Vertrauen durch überbordende Regulierung untergraben, drohen langfristige strukturelle Schäden für die digitale Infrastruktur des Landes.

Falscher Weg ohne demokratische Legitimierung

Besonders schwer wiegt aus unserer Sicht der Versuch, diese tiefgreifenden Neuerungen auf Verordnungsstufe einzuführen, ohne dass eine entsprechende gesetzliche Grundlage vorliegt.

Die Bundesverfassung (Art. 164) schreibt vor, dass wichtige rechtsetzende Bestimmungen auf Gesetzesstufe zu erlassen sind. Dazu gehören insbesondere Grundrechtseingriffe oder neue Pflichten für ganze Branchen. Die vorgesehene Revision überschreitet diesen Rahmen klar.

Eine Ausweitung von Überwachungspflichten dieses Ausmaßes muss zwingend demokratisch legitimiert werden. Wenn der Gesetzgeber solche Massnahmen nicht vorsieht – oder ausdrücklich begrenzt hat –, kann eine Verordnung sie nicht einfach durch die Hintertür einführen. Andernfalls wird das Legalitätsprinzip verletzt, das zu den tragenden Pfeilern des schweizerischen Rechtsstaats zählt.

Fazit und Forderung

Die SDCA lehnt die geplante Teilrevision der VÜPF und VD-ÜPF in ihrer Gesamtheit ab. Die Vorlage ist unverhältnismässig, rechtlich fragwürdig und wirtschaftlich schädlich.

Wir fordern den Bundesrat auf, die Revision zurückzuweisen und eine grundlegende Überarbeitung im Sinne einer verhältnismässigen, gesetzeskonformen und innovationsfreundlichen Lösung in Angriff zu nehmen – im Dialog mit den betroffenen Branchen.

Nur so lässt sich ein wirksames Gleichgewicht zwischen Sicherheit, wirtschaftlicher Entwicklung und Grundrechten gewährleisten. Die Schweiz braucht ein digitales Umfeld, das schützt, aber nicht abschreckt.

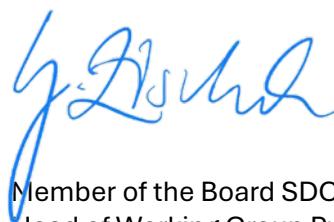
Mit freundlichen Grüßen

Sergio Milesi



President SDCA

Yves Zischek



Member of the Board SDCA
Head of Working Group Public
Affairs & Politics SDCA

Martin Zust



Head of Public Affairs SDCA



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Innosuisse – Agence suisse pour
l'encouragement de l'innovation

CH-3003 Berne, Innosuisse

Adressé par e-mail à l'adresse
ptss-aemterkonsultationen@isc-eipd.admin.ch

Département fédéral de justice et police DFJP

Centre de services informatiques CSI-DFJP

Eichenweg 3

3003 Berne

Notre réf.: coj
Berne, le 5 mai 2025

Consultation sur la révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT)

Madame, Monsieur,

Dans le cadre de la consultation publique sur la révision partielle de deux ordonnances d'exécution de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication, nous nous permettons de soumettre à votre attention nos considérations suivantes :

Innosuisse est l'Agence suisse pour l'encouragement de l'innovation. Sa mission est d'encourager l'innovation fondée sur la science dans l'intérêt de l'économie et de la société suisse. A ce titre, elle soutient les entreprises dans leurs efforts d'innovation, encourage l'entrepreneuriat, facilite le transfert de technologie, et veille à ce que ses actions contribuent au développement durable et à la prospérité nationale.

Dans le cadre du projet mis en consultation, les mesures de surveillance envisagées sont perçues par certaines entreprises, les start-ups en particulier, comme susceptibles de générer une insécurité ou une charge économique significative, entravant leur développement ou leur croissance. Ces préoccupations relèvent d'un enjeu économique impactant la compétitivité et l'attractivité de la place économique suisse.

Dans ce contexte, nous vous invitons à veiller à ce que la mise en œuvre des mesures envisagées ne pénalise pas économiquement les entreprises suisses et/ou leur réputation. Il est crucial d'éviter tout impact négatif susceptible d'affaiblir l'écosystème entrepreneurial ou de nuire à l'attractivité et à la compétitivité de la place économique et technologique suisse. À titre de solution, l'introduction **d'exemptions pour les start-ups et les PME** ou la mise en place d'**indemnités pour couvrir les surcoûts**, notamment en matière d'infrastructure, seraient des mesures appropriées pour prévenir des effets négatifs qui, à terme, risqueraient de fragiliser durablement la position de la Suisse dans le secteur des technologies de l'information et de constituer un frein considérable à l'innovation.

Nous vous remercions de l'attention portée à notre prise de position et restons à votre disposition pour toute question.

Avec nos salutations distinguées

André Kudelski
Président du Conseil d'administration

Dominique Gruhl-Bégin
Directrice



Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Per E-Mail, mit elektronischer Unterschrift

Wallisellen, 5. Mai 2025

Stellungnahme BT Switzerland AG – Teilrevisionen VÜPF und VD-ÜPF

Sehr geehrter Herr Bundesrat,
Sehr geehrte Damen und Herren,

BT Switzerland AG, Filiale der British Telecommunications Group (UK), bietet ausschliesslich Business-to-Business-Dienstleistungen für multinationale Unternehmen mit Hauptsitz in der Schweiz an. Es werden keine Dienstleistungen für Privatpersonen angeboten.

Wir bieten Konnektivitätsdienste, einschliesslich GSIP, sowie Weiterverkauf von Hardware und Software, und professionelle Dienstleistungen (wie Konfiguration oder Systemmanagement im Auftrag unserer Kunden).

Zu unseren Kunden zählen Institutionen aus den Bereichen Bankwesen, Versicherungen und Pharmaindustrie, welche hohe Anforderungen an Vertraulichkeit, Zuverlässigkeit und Sicherheit stellen.

Als Mitglied des Schweizerischen Verbands der Telekommunikation (asut) stimmen wir der Position der ASUT betreffend der VÜPF zu, die Ihnen mitgeteilt wurde. Wir wollten noch unsere Sichtweise als B2B-Anbieter in dieser Stellungnahme einbringen.

Aus dem erläuternden Bericht vom 8. Januar 2025 geht hervor, dass die Überarbeitung als begrenzte Änderung der aktuellen Verpflichtungen gedacht ist, um der aktuellen Sicherheitslage und den technologischen Fortschritten Rechnung zu tragen. Bei genauerer Betrachtung des Textes stellen wir jedoch eine wesentliche Veränderung der aktuellen Situation fest.

Die Änderungen gehen weit über das hinaus, was im Bericht angegeben ist, und unsere Analyse zeigt, dass die neuen Verpflichtungen erhebliche wirtschaftliche Auswirkungen auf die BT Switzerland AG (sowie andere Akteure in einer ähnlichen Situation) haben werden, wobei die konkreten Ergebnisse jedoch voraussichtlich limitiert sein werden. Wir können auch einen Verwaltungsaufwand auf Seiten des Bundes vorhersehen, der erhebliche Kosten verursachen wird. Angesichts der Tatsache, dass sich die derzeitige Verordnung für B2B-Anbieter als effizient erwiesen hat, sollten die wirtschaftlichen Auswirkungen dieser neuen Pflichten überprüft und die Verordnung entsprechend angepasst werden.

Zusätzlich halten wir in unserem B2B Kontext die neuen Verpflichtungen der VÜPF für unverhältnismässig, und die Umsetzung bestimmter Verpflichtungen könnte ein Risiko für die Geheimhaltung der Telekommunikation, die Sicherheit der Systeme unserer Kunden, die eigenen Vertraulichkeitsverpflichtungen unserer Kunden, die vertraglichen Verpflichtungen von BT Switzerland AG sowie ein Risiko des Widerspruchs zu internationalen Vorschriften (z.B., DORA, NIS2), die für unsere Kunden gelten, darstellen.

Dazu befindet der Business Telekommunikationsmarkt sich derzeit im Wandel, und wir investieren derzeit in Innovationen, um unseren Kunden neue (und notwendige) Produkte anbieten zu können. Die wirtschaftlichen Auswirkungen der neuen Verordnung könnten solche Innovationen verzögern.

Unserer Meinung nach sind die neuen Verpflichtungen zu weit gefasst. Wir verstehen zwar, dass die Verordnung prägnant gehalten werden soll, doch werden dabei die Grenzen der Technik ausser Acht gelassen. Es gibt verschiedenen Arten von Anbieter und nicht alle Informationen sind für einen Dienst relevant. Wir sind der Meinung, dass die bisherige Definition des Begriffs FDA mit reduzierten Überwachungspflichten sinnvoll und wirtschaftlich effizient war. Zumindes sollte diese neuen Verpflichtungen angepasst und der Anwendungsbereich jedes Artikels ausdrücklich auf die relevanten Dienste/Technologien beschränkt werden. Einige unserer Vorschläge finden Sie im Anhang zu diesem Schreiben.

Als ein nebenschächerlicher Aspekt möchten wir außerdem darauf hinweisen, dass die verschiedenen Sprachfassungen der Verordnung nicht gleichwertig sind und eine teleologische Analyse erforderlich machen, um den Umfang der Verpflichtungen zu verstehen. Es sollten klarere Fassungen erstellt werden, um die Rechtsklarheit zu gewährleisten.

Aus der Dokumentation zum BÜPF und zur VÜPF, insbesondere aus der Botschaft zum BÜPF und dem Erläuternden Bericht zur VÜPF von 2018, geht hervor, dass die Regierung die Bedeutung der Verhältnismässigkeit und Relevanz der Überwachungsmassnahmen betont und dass es kontraproduktiv wäre, von kleineren Unternehmen der Branche hohe Investitionen zu verlangen. Wir sind der Ansicht, dass die neuen Verpflichtungen im Widerspruch zu diesem letzten Punkt stehen, da sie für einen Zeitraum von mindestens 18 Monaten zu hohe Investitionen und höheren Betriebskosten führen würden.

Wir hoffen, dass der endgültige Text angepasst wird und es Anbietern wie BT Switzerland AG ermöglicht, unseren Kunden weiterhin zuverlässige Dienste anzubieten und Innovation zu fördern.

Für zusätzliche Informationen bitten wir Sie, uns jederzeit zu kontaktieren.

Freundliche Grüsse

BT Switzerland AG

Thomas Meyer
Management

Hermine Lacour
Legal

Anhang – Stellungnahme BT Switzerland AG

Nr/Textstelle/etc. (Alte Regelung)	Nr/Textstelle/etc. (Neue Regelung)	Stellungnahme	Vorschlag/Forderung
N/A	Art. 16a	<p>Dieser Artikel führt zu einem Widerspruch zwischen Art. 2 BÜPF und Art. 3, lit. b, FMG. Wir verstehen, dass die Begriffe unterschiedlich sein können, aber die Definition ist nicht zufriedenstellend: die positiven und negativen Definitionen führen zu Unsicherheiten und einer Grauzone zwischen Abs. 1 und Abs. 2 hinhaus.</p> <p>Unserer Meinung nach sollte dieser Artikel die Definition aus Art. 3, lit. b, FMG ergänzen, ob die Aufzählungen abschliessend oder beispielhaft sind.</p>	<p>„Art. 16a FDA <u>Als FDAGemäss FMG gilt als FDA für den betreffenden Dienst, wer einen Fernmeldedienst erbringt. Die in dieser Verordnung genannten Fernmeldedienste sind:</u></p> <ul style="list-style-type: none"> a. Betrieb eines öffentlichen Fernmeldenetzes; b. direkter Zugangsdienst zu einem öffentlichen Fernmeldenetz (z. B. Internetzugangsdienst) für Dritte; c. öffentlicher Mobilfunkdienst für Dritte; d. öffentlicher Telefondienst für Dritte zusammen mit dem Netzzugang. <p>2 Die Anbieterin gilt nicht als FDA für den betreffenden Dienst, wenn der Dienst ausschliesslich darin besteht, Informationen zu übertragen, insbesondere:</p> <ul style="list-style-type: none"> a. die für die Allgemeinheit bestimmt sind; b. innerhalb eines Gebäudes, einer Liegenschaft, innerhalb von zwei aneinandergrenzenden Liegenschaften oder innerhalb von zwei einander gegenüberliegenden Liegenschaften, die durch eine Strasse, einen Weg, eine WBahnlinie oder einen Wasserlauf getrennt sind; c. innerhalb ein und desselben Unternehmens, zwischen Mutter- und Tochtergesellschaften oder innerhalb eines Konzerns; d. innerhalb von oder zwischen öffentlich-rechtlichen Körperschaften“.
Art. 51	Art. 16b	<p>Die Änderung des Wortlauts in Art. 16 b, 1. lit. b steht im Widerspruch zur Botschaft zum BÜPF und zum Erläuternden Bericht VÜPF von 2018 und schränkt den Begriff der FDA mit reduzierten Pflichten zu stark ein. Die Verwendung des Wortes „bestimmte“ macht den Anwendungsbereich unklar.</p> <p>Darüber hinaus führt 1. zu einer Ausweitung der Pflichten für den Fall, dass die FDA ausreichend Anfragen für ihre Dienste als AAKD erhält.</p> <p>2. führt dazu, dass FDA mit erheblichen Einnahmen außerhalb der Bereitstellung von Telekommunikationsdiensten und für die eine Überwachung irrelevant ist (z. B. Weiterverkauf oder professionelle Dienstleistungen), einbezogen werden. Der bisherige Art. 51 erscheint uns ausgewogener und relevanter.</p> <p>Art. 16 b., 2. bedarf einer Klarstellung, da er zu viele kleine Anbieter ausschließen würde, die Teil grösserer internationaler Unternehmensgruppen sind.</p> <p>Art. 16 b., 4, der keine Neuerung darstellt, ist unverhältnismässig und wirtschaftlich nicht relevant, da die Informationen auf andere Weise verfügbar sind, insbesondere durch die jährlich an das BAKOM übermittelten Statistiken.</p>	<p>„Art. 16b FDA mit reduzierten Pflichten</p> <p>1 Auf Gesuch erklärt der Dienst ÜPF eine FDA für bestimmte Fernmeldedienste zur FDA mit reduzierten Pflichten, wenn sie:</p> <ul style="list-style-type: none"> a. diese Fernmeldedienste nur im Bereich Bildung und Forschung anbietet. b. <u>keine beide der nachstehenden Grössen nicht erreicht:</u> <ol style="list-style-type: none"> 1. Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste; 2. Jahresumsatz in der Schweiz des gesamten Unternehmens mit Fernmeldediensten von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren. <p>Kontrolliert eine Anbieterin im Sinne von Artikel 963 Absatz 2 des Obligationenrechts ein oder mehrere rechnungslegungspflichtige Unternehmen, so sind bei der Bestimmung der Anzahl der Überwachungen und des Jahresumsatzes in der Schweiz mit Fernmeldediensten die Anbieterin und die kontrollierten Unternehmen als Einheit zu betrachten.</p> <p>[...]</p> <p>4 Der Dienst ÜPF kann die durch den Vollzug der Gesetzgebung betreffend die Überwachung des Post- und Fernmeldeverkehrs oder die aufgrund des Vollzugs von Bundesrecht vorhandenen Daten anderer Behörden zur Verifizierung der möglichen Überoder Unterschreitung der Grössen nach diesem Artikel nutzen“.</p>

	Art. 16 c.	Der Anwendungsbereich des Artikels ist unklar und lässt vermuten, dass die Verpflichtungen für bestimmte Dienstleistungen vollständig und für andere vereinfacht gelten können. Das Wort „Bestimmte“ sollte gestrichen werden, um Verwirrung zu vermeiden. Die Anmerkung zu 16 b., 4, gilt auch hier.	„Art. 16c FDA mit vollen Pflichten Eine FDA gilt für bestimmte <u>Fernmeldedienste</u> als FDA mit vollen Pflichten, solange der Dienst ÜPF sie nicht zur FDA mit reduzierten Pflichten erklärt hat. Der Dienst ÜPF erklärt eine FDA mit reduzierten Pflichten für bestimmte <u>Fernmeldedienste</u> zur FDA mit vollen Pflichten, wenn die Voraussetzungen nach Artikel 16b Absatz 1 nicht mehr erfüllt sind“.
N/A	Art. 16 f.	Die Anzahl der Teilnehmenden sollte in Anbetracht des Zwecks des Gesetzes in der Schweiz liegen, da dies sonst einen unverhältnismässigen Aufwand für die AAKD in der Schweiz bedeuten und zu Beeinträchtigungen und Konflikten mit ausländischen Vorschriften führen könnte. Art. 16 f, 3. bedarf einer Klarstellung, da er zu viele kleine Anbieter, die Teil grösserer internationaler Unternehmensgruppen sind, einbeziehen würde.	„Art. 16f AAKD mit reduzierten Pflichten 1 Eine AAKD gilt für alle von ihr angebotenen abgeleiteten Kommunikationsdienste als AAKD mit reduzierten Pflichten, wenn im Durchschnitt der letzten 12 Monate (Stichtag: 30. Juni) die Anzahl der Teilnehmenden <u>in der Schweiz</u> für alle von der Anbieterin angebotenen abgeleiteten Kommunikationsdienste mindestens 5000 betragen hat und sie die Voraussetzungen nach Artikel 16g Absatz 1 nicht erfüllt. [...] 3 Kontrolliert eine Anbieterin im Sinne von Artikel 963 Absatz 2 des Obligationenrechts ein oder mehrere rechnungslegungspflichtige Unternehmen, so sind bei der Bestimmung der Anzahl der Teilnehmenden <u>in der Schweiz</u> und des Jahresumsatzes <u>in der Schweiz</u> die Anbieterin und die kontrollierten Unternehmen als Einheit zu betrachten“.
Art. 22	Art. 16 g.	Wir halten diese Kriterien für irrelevant, da sie für Unternehmen in der Schweiz im Vergleich zu ausländischen Unternehmen mit Nutzern in der Schweiz unangemessene Verpflichtungen mit sich bringen würden. Um eine Angleichung an den Zweck dieser Verordnung zu gewährleisten, erscheint die lokale Anzahl der Nutzer oder die lokalen Einnahmen relevanter.	„Art. 16g AAKD mit vollen Pflichten 1 Der Dienst ÜPF erklärt eine AAKD für alle von ihr angebotenen abgeleiteten Kommunikationsdienste zur AAKD mit vollen Pflichten, wenn: a. im Durchschnitt der letzten 12 Monate (Stichtag: 30. Juni) die Anzahl der Teilnehmenden für alle von der Anbieterin angebotenen abgeleiteten Kommunikationsdienste mindestens 1 Million <u>in der Schweiz</u> betragen hat; oder b. der Jahresumsatz <u>in der Schweiz</u> mit den abgeleiteten Kommunikationsdiensten des gesamten Unternehmens in den beiden vorhergehenden Geschäftsjahren mindestens 100 Millionen Franken betragen hat“.
N/A	Art. 16h	Die Anzahl der Zugriffe auf ein WLAN würde zu viele Unternehmen qualifizieren, die keine Anbieter sind (konzerninterne Kommunikation, Hotels, Universitäten...). Es fehlt eine zeitliche Begrenzung und ein Verweis auf Art. 16a, um konzerninterne Kommunikation auszuschließen.	„Art. 16h Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen 1 Als Person, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellt, gilt, wer einen oder mehrere seiner Zugänge zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellt (z. B. öffentlicher WLAN-Zugang), ohne den Zugangsdienst zu erbringen. 2 Ein öffentlicher WLAN-Zugang gilt als professionell betrieben, wenn kumuliert über einen Tag maximal mehr als 1000 Endbenutzerinnen und -benutzer alle von der gleichen Person gemäss Absatz 1 zur Verfügung gestellten öffentlichen WLAN-Zugänge nutzen können. Die Ausnahmen von Art. 16 let. a, 2, gelten“.
N/A	Art. 42a	Der Geltungsbereich dieses Artikels ist unklar, da er sich auf eine Anwendung bezieht, aber mit den Verpflichtungen der FDA in Zusammenhang steht.	Streichung.
N/A	Art. 43a	Diese neue Verpflichtung führt zu einem unverhältnismässigen Archivierungsaufwand, der erhebliche Investitionen erfordern würde. Bestimmte Informationen können der FDA auch auf andere Weise übermittelt werden, z. B. über Rechnungsdaten (Nichtleistung einer Dienstleistung). Wir beantragen die Streichung dieses Artikels.	Streichung.

N/A	Art. 50a	Der Wortlaut des Artikels ist zu allgemein gehalten und spiegelt nicht die technischen Einschränkungen wider, mit denen die Anbieter konfrontiert sind. Wir schlagen einige Formulierungen vor, um den Anwendungsbereich dieser Bestimmung zu präzisieren. Es ist klar, dass die Anbieter die Überwachung nicht behindern wollen, aber nicht alle Verschlüsselungen können entfernt werden.	<p>„Art. 50a Entfernung von Verschlüsselungen</p> <p><u>Wenn die Anbieterinnen die direkte Kontrolle über die Verschlüsselung und die Entschlüsselung haben, die Verschlüsselung darf kein Hindernis für die Beantwortung eines Auftrags darstellen.</u></p> <p><u>Gemäss den technischen Anforderungen, die Anbieterinnen mit reduzierten Pflichten und die Anbieterinnen mit vollen Pflichten entfernen die von ihnen oder für sie angebrachten Verschlüsselungen, und/oder Sie erfassen und entschlüsseln dafür den Fernmeldeverkehr der überwachten Person an geeigneten Punkten, damit die Überwachungsdaten ohne die vorgenannten Verschlüsselungen geliefert werden. Die Ende-zu-Ende-Verschlüsselungen unter der Kontrolle des Teilnehmers oder zwischen Endkunden sind davon nicht betroffen“.</u></p>
N/A	Art. 60a	Der Wortlaut dieses Artikels ist zu weit gefasst und steht im Widerspruch zu anderen Vorschriften (Rechte der Person, Datenschutz...). Das Erfordernis der Verhältnismäßigkeit fehlt. Darüber hinaus möchten wir darauf hinweisen, dass dies massive Investitionen erfordern und das Risiko für die Cybersicherheit erhöhen würde, da solche Archive eine wertvolle Informationsquelle für Cyberangreifer darstellen würden. Infolgedessen wären massive Investitionen erforderlich, um solche Dateien zu erstellen, zu pflegen und zu sichern. Wir bitten um Löschung dieses Artikels.	Streichung.
N/A	Art. 74c	Der Zeitrahmen für die Anpassung an die neuen Verpflichtungen ist zu kurz, mindestens 18 Monate sind erforderlich.	<p>„Art. 74c Übergangsbestimmung zur Änderung vom XXX</p> <p><u>1 Eine AAKD, die die Größen nach Artikel 16f Absatz 1 oder 16g Absatz 1 überschreitet, muss dies dem Dienst ÜPF innerhalb von 3 Monaten nach Inkrafttreten dieser Änderung schriftlich mitteilen.</u></p> <p><u>2 Die FDA mit vollen Pflichten müssen Auskünfte gemäss den Artikeln 38a, 42a und 43a innerhalb von <u>18</u> Monaten nach Inkrafttreten dieser Änderung erteilen können.</u></p> <p><u>3 Sie müssen die Überwachungen gemäss Artikel 55a innerhalb von <u>24</u> Monaten und diejenigen gemäss Artikel 60a innerhalb von <u>18</u> Monaten nach Inkrafttreten dieser Änderung standardisiert durchführen können“.</u></p>

*Vernehmlassungsantwort zu den Teilrevisionen der VÜPF und der VD-ÜPF
gemäss Schreiben des EJPD vom 29. Januar 2025*

Datum	6.5.2025
Verfasser (Unternehmen)	CH Open Brückenstrasse 73 3005 Bern info@ch-open.ch
Kontaktperson bei Fragen (Name/Tel./E-Mail)	Dr. Matthias Günter, matthias.guenter@ch-open.ch 079 457 13 22

Dieses Dokument geht an:

Eidgenössisches Justiz- und Polizeidepartement EJPD, ptss-aemterkonsultationen@isc-ejpd.admin.ch

Sehr geehrter Herr Bundesrat Jans, sehr geehrte Damen und Herren

Wir beziehen uns auf das am 29. Januar 2025 eröffnete Vernehmlassungsverfahren zu Teilrevisionen von VÜPF und VD-ÜPF und bedanken uns für die Möglichkeit einer Stellungnahme.

Wir lehnen die geplante Teilrevisionen der VÜPF und der VD-ÜPF in aller Deutlichkeit und vollumfänglich ab.

Im Bericht des Bundesrates zur aktuellen Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF und der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) ist zu lesen, dass die Revision im Wesentlichen auf die Anpassung der Verordnungen an die KMU-Freundlichkeit abziele. Ein grosser Teil der vorgeschlagenen Änderungen *verfolgt aber gerade das Gegenteil*.

Die Geschäftsgrundlagen von Schweizer Unternehmen wie Threema, Proton und anderer KMU, die weltweit einen hervorragenden Ruf als Anbieterinnen sicherer Kommunikationsdienste im Internet geniessen, drohen durch die Vorlage zerstört zu werden. Die Sicherheit des Internets in der Schweiz soll mit der Revision der Überwachung jeglichen Internetverkehrs regelrecht untergeordnet werden: «**Sicherheit vor Freiheit» ist das neue Paradigma**. Dieses zieht sich wie ein roter Faden quer durch diese völlig verunglückte Reform. KMU, die aus der Schweiz heraus Internet-Dienste anbieten («abgeleitete Kommunikationsdienste» in der Terminologie des Gesetzes), soll die Schweiz als Standort geradezu vergällt werden. Dies scheint denn auch zu gelingen: **Erste der betroffenen Unternehmen haben bereits angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen** (siehe Tages-Anzeiger vom 1. April 2025).

Ein derartiger Paradigmenwechsel, weg von KMU-Schutz und Überwachung mit Augenmass, hin zu knallharter Überwachung, die alle anderen Interessen unterordnet, wird durch das geltende Gesetz (BÜPF) keineswegs gestützt. Der Paradigmenwechsel widerspricht vielmehr geradezu dem Geist des ursprünglichen BÜPF, das Internetdienste, die in der Schweiz meist von KMU betrieben werden, gerade von der Implementierung teurer Überwachungsmassnahmen schützen wollte, und das eine austarierte Interessenabwägung vorsah zwischen Privatsphäre und Freiheit auf der einen Seite und staatlicher Überwachung auf der anderen Seite.

Entgegen dem im Begleitbericht zum vorgelegten Entwurf erklärten Ziel, die «finanzielle Belastung der KMU gering zu halten», stuft die Vorlage eine grosse Mehrheit der Schweizer Anbieterinnen von Internetdiensten in eine höhere Stufe auf, und zwingt sie neu auch in jenen Bereichen zu einer kostspieligen aktiven Überwachungstätigkeit, wo bisher nur eine KMU-freundliche Duldungspflicht bestand. Dies verschiebt das bisherige Gleichgewicht der Interessen zwischen Strafverfolgung und betroffenen Anbieterinnen in drastischer Weise zulasten der betroffenen Anbieterinnen.

Die vorgeschlagenen Anpassungen bringen ganz erhebliche Risiken für den Innovations- und Wirtschaftsstandort Schweiz mit sich und erfüllen die Kernziele der Revision, die Entlastung von KMU, gerade nicht. Der Ruf der Schweiz als sicherer Hafen für vertrauenswürdige IT-Anbieter droht durch die Revision nachhaltig beschädigt zu werden. Deshalb lehnen wir die Revision vollumfänglich ab.

Auch **die Schweizer Armee** nutzt solche Dienste, wie beispielsweise Threema, und zwar gerade aufgrund des hohen gebotenen Sicherheitsstandards. Die Annahme dieser Revision, welche dieses Sicherheitsniveau gezielt untergraben will, verletzt damit indirekt auch das direkte Interesse der Schweiz an lokal betriebenen Hochsicherheitsanwendungen. Gerade in der heutigen Zeit, in der die Zuverlässigkeit der grossen US-Anbieter in ihrer Abhängigkeit von einer zunehmend erratisch agierenden US-Regierung mehr und mehr in Frage steht, erscheint dies als **inakzeptable Hochrisikostrategie**.

Nicht zuletzt ist mit Nachdruck darauf hinzuweisen, dass die Revision die Überwachung ganz allgemein stark ausweitet. Dies ist mit der durch den Gesetzgeber im BÜPF festgelegten, fein austarierten Interessenabwägung zwischen Freiheit und Privatsphäre der Einwohner der Schweiz einerseits und Sicherheit durch Überwachungsmassnahmen andererseits absolut nicht vereinbar. Die Revision entpuppt sich geradezu als eine Art Wunschkonzert für Überwachungsbehörden. Insbesondere ist künftig auch **eine komplette inhaltliche Überwachung des gesamten Internetverkehrs** der Schweiz vorgesehen. Dies ohne, dass eine solche inhaltliche Überwachung durch die gesetzlichen Grundlagen des BÜPF in irgendeiner Weise gedeckt wäre: Zulässig ist gemäss BÜPF einzig und allein die Überwachung von Randdaten des Fernmeldeverkehrs, und selbst die Zulässigkeit der in diesem Kontext angewendeten anlasslosen Vorratsdatenspeicherung von Randdaten ist bis heute umstritten und Gegenstand von Gerichtsverfahren, ja in der EU bereits höchstrichterlich als menschenrechtswidrig erkannt. Die durch die Verordnungsrevision eingeführte *Inhaltsüberwachung* ist in der Schweiz damit erst recht **offensichtlich illegal und verfassungswidrig**.

Abschliessend sei noch der Hinweis angebracht, dass wir die Gesetzgebungstechnik des Entwurfs für überaus schlecht halten. **Sowohl der Verordnungstext als auch der zugehörige erläuternde Bericht sind über weite Strecken höchst verwirrend und unverständlich formuliert**, unter anderem mit einer Vielzahl von Querverweisen, technischen Fehlern und unklarer Begrifflichkeiten (für ein Beispiel hierfür siehe unten, Bemerkungen zu Art. 43a). Die Texte sind in dieser Form selbst für Fachleute über weite Strecken nicht zu verstehen, geschweige denn als Ganzes zu überblicken. Für KMU, die durch die Revision neu mit erheblich strengerem Pflichten konfrontiert werden, ist eine rechtskonforme Umsetzung dieser Vorlage daher ein schlicht aussichtloses Unterfangen.

Das Legalitätsprinzip gemäss Art. 5 Bundesverfassung fordert vom Gesetzgeber, dass Gesetzestexte für die Adressaten verständlich formuliert sind. Die Texte der Verordnungsrevision genügen dieser Anforderung offensichtlich in keiner Weise. Nur schon aufgrund der völlig fehlenden Verständlichkeit ist die Verfassungsmässigkeit der Revision insgesamt *höchst zweifelhaft*. Wir fordern nur schon deshalb einen Rückzug der vorgelegten Texte, eine komplette Überarbeitung zur Verbesserung der Verständlichkeit und eine erneute Auflage zur Vernehmlassung.

Mit freundlichen Grüßen

Dr. Matthias Günter
Vizepräsident CH Open

Bemerkungen zu einzelnen Artikeln der VÜPF

Nr.	Artikel	Antrag	Begründung / Bemerkung
VÜPF / OSCPT / OSCPT			
0.	Alle Artikel	Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.	<p>Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kunden auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.</p> <p>Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.dgl. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.</p>
1.	16b, Abs. 1	Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.»	Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile, wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Anforderungen in Kauf nehmen.
2.	16c, Abs. 3	Streichung von lit. a «automatisierte Erteilung der Auskünfte (Art. 18 Abs. 2);»	Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Dies untergräbt rechtsstaatliche Prinzipien doppelt: Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>«natürliche» Schutzmechanismen gegen eine überschiessende, missbräuchliche oder zumindest unverhältnismässige Nutzung solcher Massnahmen durch die Untersuchungsbehörden.</p> <p>Der vorgesehene Umsetzungszeitraum von 12 Monaten für die rechtssichere Implementierung eines derart komplexen Systems völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.</p>
3.	Art. 16d	<p>Streichung von Online-speicherdiensten und VPN-Anbietern in der Auslegung</p>	<p>Eine klarere Definition des Begriffs AAKD ist begrüssenswert, doch die neue Auslegung gemäss erläuterndem Bericht geht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdiensten wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter, etc.) genutzt werden.</p> <p>Art. 2 lit. c BüPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug den gesetzlichen Rahmen sprengt. Onlinespeicherdiene sind deshalb aus Art. 16d zu streichen.</p> <p>Zudem anerkennt der erläuternde Bericht, dass VPNs zur Anonymisierung der Nutzer*innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Anbieter von VPNs sind daher ebenfalls aus dem Geltungsbereich von Art. 16d auszunehmen.</p>
4.	Art. 16e, Art. 16f und Art. 16g	<p>Streichung der Artikel und Beibehaltung der bestehenden Kriterien</p> <p>Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).</p>	<p>Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch diametral entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung. Dies daher, weil neu KMU bereits mit mehr als 5'000 Nutzern erfasst werden.</p> <p>Die Einführung von 5000 Nutzern als gesondert zu beurteilende Untergrenze verletzt aus unserer Sicht bereits Art. 27 Abs. 3 BüPF, denn 5000 Personen keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strenger Überwachungsmassnahmen, gerechtfertigt wären. 5000 Nutzer werden in der digitalen Welt vielmehr sehr rasch erreicht.</p> <p>Zusätzlich führt das Einführen eines «Konzernatbestandes» in Art. 16f Abs. 3 zu massiven Problemen, da die Produkte nun nicht mehr für sich alleine eine bestimmte Grösse erreichen müssen, sondern die rele-</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>vanten Zahlen anhand des Umsatzes des Unternehmens, bzw. in Konzernverhältnissen sogar des Konzerns bestimmt werden. Vor allem bei Unternehmen mit Beteiligungsfirmen im Hintergrund fallen nun neu alle Dienstleistungen und Produkte automatisch unter die härteste Stufe, egal ob sie sich erst in einem frühen Entwicklungsstadium befinden. Dies behindert Innovation, da jedes Projekt bereits mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden müsste. Durch diese extreme Einstiegshürde wird der Innovationsstandort Schweiz nachhaltig geschädigt.</p> <p>Gleichzeitig wird auch der Wirkungsbereich der VÜPF stark erweitert. Während heute ein Unternehmen einen grossen Teil seiner Geschäftstätigkeit durch abgeleitete Kommunikationsdienste erbringen muss (Art. 22 Abs. 1 lit. b und Art. 52 Abs. 1 lit. b VÜPF), fällt dieses Kriterium neu weg. Dadurch können künftig auch Unternehmen, deren Geschäftstätigkeit nur am Rande auf abgeleiteten Kommunikationsdiensten basiert, wie Onlineshops, Marktplätze, Auktionsplattformen, Zeitungen, Computerspielhersteller und zahlreiche weitere Unternehmen, unter die VÜPF fallen – allein deshalb, weil ihre Produkte irgendeine Form privater Kommunikation zwischen Nutzer*innen und/oder Drittanbietern ermöglichen.</p> <p>Die vorgeschlagene Regelung stünde sodann im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali, das die zu weite Betroffenheit und die seltene Anwendung von Downgrades kritisierte: «Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»</p> <p>Statt KMU zu entlasten, führt die Revision neu sogar zu einer «automatischen Hochstufung per Verordnung ohne konkretisierende Verfügung (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.</p> <p>Die neue Regelung steht zudem in offensichtlichem Widerspruch zur bisherigen Praxis, denn bis heute wurde gemäss Angaben des Dienst-ÜPF keine einzige AAKD hochgestuft. Auch der Bundesrat stützte sich ausdrücklich auf die geltende Kombination von drei Schranken – einem Unternehmensfokus auf Kommunikationsdienste, einer Umsatzgrenze von 100 Millionen Franken sowie einer grossen Nutzerzahl – als er noch 2023 begründete, die Umsetzung des BÜPF sei gerade wegen der genannten Schranken als KMU-freundlich zu verstehen. Die vorliegende Revision hebt jedoch genau diese Kombination kumulativer Kriterien auf und will die einzelnen Kriterien künftig alternativ anwenden bzw. streicht sie sogar vollständig. Dadurch verlieren die bisherigen Schutzmechanismen ihre Wirkung, und das BÜPF soll neu auf viele KMU Anwendung finden, die früher nicht unter Gesetz und Verordnung fielen.</p> <p>Die Analyse der offiziellen Statistik des Dienstes ÜPF macht die offensichtliche Unverhältnismässigkeit dieses Ansinnens deutlich. Im Jahr 2023 betrafen 98,95 % der total 9'430 Überwachungen allein</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,05 % für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,73 % wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100 % des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.</p> <p>Wesentlich ist insbesondere eine neue Pflicht zur Identifikation der Nutzer: Hiervon betroffen sind nicht nur alle AAKD mit reduzierten oder vollen Pflichten (und damit de facto fast alle AAKD der Schweiz), sondern auch all deren Wiederverkäufer. Im Ergebnis führt die neue Verordnung aus unserer Sicht dazu, dass man sich bei keinem marktrelevanten Dienst mehr anmelden kann, ohne den Pass, Führerschein oder ID zu hinterlegen oder zumindest Daten wie eine Telefonnummer anzugeben, die man ohne Pass oder ID nicht erhalten kann.</p> <p>Die automatische Hochstufung an sich führt bereits zu erheblicher Rechtsunsicherheit bei den betroffenen Unternehmen. Unter dem bestehenden System werden die generell-abstrakten Normen der VÜPF mittels Verfügung auf einen konkreten Einzelfall angewendet. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes ist aber im Zweifelsfall möglicherweise nur schwer zu beantworten. Zweifelsohne besteht hier ein schutzwürdiges Interesse seitens der AAKD daran, zu wissen, ob sie die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Nur das bisherige System entspricht den allgemeinen Grundsätzen des Verwaltungsverfahrens, welches für die Anwendung einer generell-abstrakten Norm eine Konkretisierung durch die Verwaltung voraussetzt. Von einer automatischen Hochstufung von AAKD ist daher aus Gründen der Rechtssicherheit abzusehen. Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.</p> <p>Gegenüber der alten VÜPF erweitert die Revision die Pflichten zur Automatisierung sodann noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragen wie z.B. IR_59 und IR_60, welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen. Genau diese Möglichkeit einer manuellen Intervention ist aber für die Provider kritisch, um Missbräuche zu verhindern, die wiederum die Verträge mit ihren Kunden und das Fernmeldegeheimnis verletzen könnten. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente damit erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 Bst. b der alten VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grosse[n] Teil ihrer Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. Damit fallen insbesondere bereits Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz. Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Dies setzt der Innovation in der Schweiz neue riesige Hürden entgegen.</p> <p>Auch Non-Profit-Organisationen wie die Signal Foundation, die kaum Umsätze erwirtschaften, geraten unter diese verschärften Vorgaben. Während sie bisher unter Duldungspflichten verbleiben konnten, solange sie Art. 22 Abs. 1 VÜPF nicht erfüllten, wird neu allein auf die Anzahl der Nutzer*innen abgestellt, womit z.B. Signal neu als AAKD mit vollen Pflichten erfasst würde. Dies würde dazu führen, dass Signal in der Schweiz entweder zu einem Rückzug aus dem Markt gezwungen wird oder erhebliche rechtliche Konsequenzen riskiert, da Signal keine IP-Adressen speichert und somit gegen Art. 19 RevVÜPF verstößt.</p> <p>Die Regelung ignoriert zudem wirtschaftliche Realitäten: Ein hoher Nutzerkreis bedeutet bei Non-Profits keine finanzielle Tragfähigkeit für umfangreiche Überwachungsmassnahmen. Damit werden Open-Source- und Non-Profit-Lösungen gezielt aus dem Markt gedrängt, während bestehende Monopole wie WhatsApp (96 % Marktanteil in der Schweiz) gestärkt werden. Die neue Regelung ist daher aus ökonomischer Sicht zu verwerfen. Das Kriterium der reinen Nutzerzahl ist ungeeignet und muss gestrichen werden.</p> <p>Nicht zuletzt schwächt die Regelung auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger*innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, Ende-zu-Ende-verschlüsselter Kommunikation ist heute wichtiger denn je.</p> <p>Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade als rechtswidrig gilt (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer*innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, sondern allein diese Anhäufung an Daten malt eine Zielscheibe auf den Rücken von Schweizer Unternehmen und Dienstleistungen für Hackerangriffe aus der ganzen Welt.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Weiters ist zu erwähnen, dass es gar nicht erwiesen ist, dass die Speicherung der fraglichen Daten eine merklich höhere Quote erfolgreicher Ermittlungen durch die Strafverfolgungsbehörden mit sich bringen würde. Im Gegenteil müssen die bereits existierenden Sekundärdaten, die allein durch die Bereitstellung eines Dienstes für den Nutzer entstehen, besser genutzt werden. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisbrauch via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfügt, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden. Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren.</p> <p>Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Souveränität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.</p> <p>Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das Datenschutzgesetz. Der Entwurf bringt nicht, wie der Begleitbericht dem Leser in geradezu in Orwell'scher Manier weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit und steht in direktem Gegensatz zum besagten Postulat 19.4031.</p> <p>Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen, und das bestehende System muss beibehalten werden.</p>
5.	Art. 16h Abs. 2	Streichung der Ausführung im erläuternden Bericht und ein Abstellen der Formulierung auf die gleichzeitige Anzahl Nutzer.	Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Nutzer*innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 Rev.VÜPF, gemäss dem die das WLAN erschliessenden FDA die Verantwortung für die Identifikation der Nutzer der WLANs tragen.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer*innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24) oder die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22). Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDAs unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden. Unter der bestehenden Regelung konnte eine FDA anhand der Lokation (z.B. Bibliothek, Flughafen) eine Einschätzung treffen. Die neue Definition hingegen würde von ihr verlangen, Zugriff auf jedes private Netzwerk zu erhalten, um Hardware und Einstellungen zu prüfen – ein offensichtlich verfassungswidriges und auch praktisch unmögliches Unterfangen. Diese vage Formulierung führt zu anhaltender Rechtsunsicherheit für FDA.</p> <p>Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten.</p> <p>Zudem könnte Art. 16h dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist*innen, Whistleblower*innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer*innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen. Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt.</p>
	Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2	Streichung des «Konzernatbestand» und Beibehaltung der bestehenden Regelung	Die Verordnung nimmt neu nicht mehr die Umsatz- und Nutzerzahlen der betroffenen Unternehmen, sondern die Zahlen des jeweiligen Konzerns als Basis für Up- und Downgrades. Die Begründung zur Einführung dieses «Konzernatbestands», wonach die neue Regelung für die betroffenen Unternehmen zu einer Vereinfachung führe, ist kontraintuitiv, ja offensichtlich falsch und irreführend. In der Praxis sind die betroffenen Unternehmen nämlich schon heute verpflichtet, ihre Buchhaltung nach Produkten aufzugliedern. Somit können die Kennzahlen bereits heute sehr einfach festgestellt werden. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.
6.	Art. 19 Abs. 1	Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation	<p>Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vor sieht.</p> <p>Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des Schweizer Datenschutzgesetzes, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch der Schutz der Schweizer Kundschaft massiv</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
		von Teilnehmenden.	<p>beeinträchtigt wird. Datenschutzfreundliche Unternehmen werden bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.</p> <p>Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Dies wahrt nicht nur den Datenschutz, sondern schützt auch die Wettbewerbsfähigkeit von KMU, stärkt den Innovationsstandort Schweiz und die digitale Souveränität unseres Landes.</p>
7.	Art. 18	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.
8.	Art. 19 Abs. 2	Ersatzlose Streichung zugunsten bestehender Regelung	Eine Überwachung von Kunden durch FDA, ob diese die neuen Vorgaben der VÜPF zu WLANs einhalten (Art. 19 Abs. 2 Rev. VÜPF), und erst recht die dazu gelieferte Erklärung im erläuternden Bericht, wonach die FDA die Identifikation der WLAN-Nutzer vorzunehmen hätten, ist weder gesetzeskonform noch zumutbar (siehe vorstehend). Art. 19 Abs. 2 ist ersatzlos zu streichen.
9.	Art. 21 Abs. 1 lit. a	Streichung	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.
10.	Art. 22	beibehalten	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.
11.	Art. 11 Abs. 4	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.
12.	Art. 16b	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.
13.	Art. 31 Abs. 1	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.
14.	Art. 51 und 52	beibehalten	Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.
15.	Art. 60a	Streichung des Artikels	Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Art. 60a VÜPF (Erläuterung Bundesrat: «...lediglich redaktionelle Änderungen....») sieht vor, dass Fernmeldedienstanbieterinnen über einen rückwirkenden Zeitraum von 6 Monaten alle Ziel-IP-Adressen liefern müssen, welche ihre Kunden besucht haben. Damit wird einerseits das Surfverhalten der gesamten schweizerischen Bevölkerung anlasslos und völlig unverhältnismässig ausspioniert. Andererseits wird die klare Vorgabe des BÜPF umgangen, das nur die Speicherung von Randdaten, aber nicht die Speicherung von Inhaltsdaten vorsieht.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Die geplante Überwachung des Internetverkehrs führt zu einer Überwachung, wer im Internet welche Adressen besucht hat. Dies geht zweifellos über die Schranken der gesetzlichen Regelung hinaus, dies insbesondere nachdem bereits die Aufzeichnung reiner Randdaten höchst umstritten und Gegenstand laufender Gerichtsverfahren ist. Hinzu kommt folgendes: Während bislang die Überwachung einer IP-Adresse nur im Rahmen einer sog. Echtzeit-Überwachung zulässig war, welche entsprechende Bewilligungen durch ein Gericht erforderte, muss neu nur noch ein einfaches Auskunftsbegehren durch die zuständige Behörde genehmigt werden. Die Abfragen erfolgen automatisiert.</p> <p>Art. 60a sieht weiter vor, dass bei nicht exakt zuordenbaren IP-Adressen die kompletten Listen aller Nutzerinnen und Nutzer zu liefern ist. IP-Adressen sind ein rares Gut. Alle FDA teilen diese den Nutzenden im Millisekunden-Takt zu. Da die Zeitstempel der Systemanbieter nicht immer übereinstimmen, sind diese IP-Adressen nicht immer eindeutig einem Nutzenden zuzuordnen. Neu müssen Provider nun komplettene Listen aller Nutzenden liefern. Dies bringt Zehntausende in den Fokus von Überwachungsbehörden, was auf eine Art Rasterfahndung nach Delikten über grosse Teile der Bevölkerung hinausläuft. Entdecken Strafverfolger dabei zufälligerweise etwas, können sie umgehend Strafverfahren einleiten.</p> <p>Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde sodann gemäss Bericht gezielt auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten.</p> <p>Art. 60a ist zu streichen.</p>
16.	Art. 42a und Art. 43a	Streichung des Artikels	<p>Sowohl Art. 42a als auch Art. 43a fordern die Abrufbarkeit des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Nicht nur gilt auch hier wieder die Limite von 5'000 Nutzern, was somit fast die gesamte AAKD-Landschaft der Schweiz flächendeckend umfasst, sondern solche Abfragen sollen nun auch durch eine einfach «IR_» Abfrage gemacht werden können, welche im Gegensatz zu den «HD_»-Abfragen und den «RT_»-Überwachungen ohne weitere juristische Aufsicht automatisiert abgerufen werden können, obwohl es sich auch hier um das Abrufen einer IP-Adresse in der Vergangenheit handelt, genau wie bei den «HD_» abfragen, welche deutlich strenger reglementiert sind. Es ist nicht nachvollziehbar und verletzt aus unserer Sicht die gesetzliche Grundlage des BÜPF, dass Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber.</p> <p>Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser Automatisierten Auskünfte ergibt. Durch das Fehlen solcher Limiten könnte daher z.B. alle 5 Minuten eine solche Anfrage automatisiert gestellt werden. Zunächst können sich dadurch lärmende Kosten für die betroffenen AAKD ergeben. Sodann können die Anfragen an ein automatisiertes Auskunftssystem gestellt werden, und es können auf diese Weise viele der Informationen welche ursprünglich über die juristisch</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>sichereren HD_ und RT_ Auskunfts-/Überwachungstypen liefern, neu über den rechtlich unsicheren IR_- Typ eingeholt werden. IR_59 und IR_60 ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne dass sie den benötigten Kontrollen dieser invasiven Überwachungsarten unterliegen würden.</p> <p>Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind, wie dies das BÜPF vorsieht.</p> <p>Die beiden Artikel sind daher vollumfänglich zu streichen.</p> <p>Diese neue Regelung und der zugehörige erläuternde Bericht sind im Übrigen eklatante Beispiele für die eingangs bemängelte überaus verwirrende und unverständliche Darstellung von Verordnungstext und erläuterndem Bericht.</p> <p>Im erläuternden Bericht steht auf S. 39 wörtlich:</p> <p><i>«In Absatz 1 sind die zu liefernden Angaben geregelt. Gemäss Buchstabe a ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin der oder dem Teilnehmenden einen solchen zugeteilt hat. Der «eindeutige Dienstidentifikator» gemäss Buchstabe b bezeichnet den Fernmelde- oder abgeleiteten Kommunikationsdienst, auf den sich die Antwort bezieht, eindeutig im Bereich der Anbieterin. In Buchstabe c werden die zu liefernden Angaben über den Ursprung der Verbindung bei der letzten zugriffsrelevanten Aktivität aufgezählt. Diese Angaben können für die Identifikation der Benutzerinnen und Benutzer nützlich sein.»</i></p> <p>Der Leser bzw. die Leserin urteile selber über die Verständlichkeit.</p> <p>Folgende Begriffe sind auch für den fachkundigen Leser nicht nachvollziehbar, bzw. es stellen sich folgende Verständnisfragen:</p> <ul style="list-style-type: none"> - Eindeutiger Identifikator: Was ist gemeint? Ist die Kundennummer des Internetproviders gemeint? Oder jene des genutzten dritten Fernmeldedienstes oder abgeleiteten Kommunikationsdienstes? Wie soll der Internetprovider überhaupt an diese Daten herankommen? - Eindeutiger Dienstidentifikator: Muss der Internetprovider eine Liste aller möglichen durch seine Kunden im Internet genutzten Kommunikationsdienste führen und aufzeichnen, muss er zudem aufzeichnen welcher Kunde welchen Dienst wann genau genutzt hat? Woher hat er diese Liste? Wie kann er herausfinden, ob ein Kunde gerade einen bestimmten Dienst nutzt? Gilt dies auch für ausländische Dienste? Nur für AAKD, für ausländische Fernmeldedienste, oder für alle Internetangebote weltweit? Der erläuternde Bericht bleibt hier völlig unklar.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<ul style="list-style-type: none"> - Was ist mit «Antwort» gemeint? Die Antwort des Servers des abgeleiteten Kommunikationsdienstes, den der Kunde besucht hat, oder die Antwort des Kundengeräts auf eine Nachricht von diesem Kommunikationsdienst? - Was ist mit «eindeutig im Bereich der Anbieterin» gemeint? Die Formulierung ist auch hier unverständlich. - Wie soll man sich eine «Antwort von einem anderen Fernmelddienst» vorstellen? Muss ein Internetprovider die Herkunft sämtlicher auf seinem Netz eintreffenden Datenpakete aufzeichnen und dem Dienst ÜPF auf Anfrage diese Aufzeichnungen herausgeben? Wie soll die gigantische Masse an Daten, die durch ein solches Logging anfällt, durch die Internetprovider gemanaged werden? - Was ist mit «letzter zugriffsrelevanter Aktivitäten» gemeint? Geht es hier um die durch Kunden des Internetproviders aufgerufenen AAKD und andere Internetangebote? Wie soll der Internetprovider wissen, ob eine durch den Kunden aufgerufene IP-Adresse zu einem überwachungspflichtigen AAKD gehört, oder allenfalls zu einem nicht überwachungspflichtigen Dienst? Muss er einfach den ganzen Verkehr aufzeichnen? Wie weit zurück gehen die «zugriffsrelevanten» Aktivitäten? Müssen alle Daten für sechs Monate aufbewahrt werden? - Abgesehen davon: Wo wäre die gesetzliche Grundlage im BüPF für die vorgesehene inhaltliche Überwachung des Internetverkehrs? Das BüPF selber regelt bisher ausschliesslich die Überwachung der Randdaten, nicht aber von Inhaltsdaten, und spätestens dann, wenn Randdaten einen passant auch Auskunft über die vom Kunden abgerufenen Inhalte geben, handelt es sich dabei um Inhaltsdaten, deren Sammlung erst recht gesetzes- und verfassungswidrig wäre, nachdem schon das Sammeln reiner Randdaten als menschenrechtswidrig taxiert wurde.
17.	50a	Artikel streichen	<p>Art. 50a sieht neu vor, dass Anbieter verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Diese Pflicht gilt nicht mehr nur für FDA (Art. 26 BüPF) oder ausnahmsweise für ausgewählte AAKD von hoher wirtschaftlicher Bedeutung (Art. 27 BüPF), sondern soll nun vorgabemässig und ohne Differenzierung auf sämtliche Anbieter mit mehr als 5'000 Teilnehmern angewendet werden, womit wohl fast die gesamte Schweizer AAKD-Branche betroffen ist (kaum ein Produkt ist lebensfähig mit weniger als 5000 Teilnehmern).</p> <p>Dies stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar.</p> <p>Diese Ausweitung ist nicht nur unverhältnismässig, sondern gefährdet aktiv nahezu die gesamte Schweizer IT-Branche: Indem de facto alle Anbieter vorgabemässig gezwungen werden, ihre Verschlüsselungssysteme für Behörden jederzeit entschlüsselbar zu gestalten, entstehen enorme Sicherheitsrisiken, denn</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Verschlüsselung ist wie eine Eierschale: Unversehrt ist sie stark, aber der kleinste Riss führt zu einer erheblichen Schwächung. Die betroffenen Systeme werden durch den vom Verordnungsgeber nun verpflichtend vorgesehenen Einbau von Hintertüren anfälliger für Hackerangriffe, Datenmissbrauch und Spionage. Dies widerspricht Art. 13 BV und dem diesen konkretisierenden Datenschutzgesetz, das den Schutz personenbezogener Daten ausdrücklich durch wirksame technische Massnahmen – insbesondere Verschlüsselung – vorschreibt. Eine durch den Anbieter aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung in jedem Fall.</p> <p>Genau eine solche Schwächung der Verschlüsselung wurde kürzlich vom Europäischen Gerichtshof für Menschenrechte im Fall PODCHASOV gegen Russland (33696/19) als Verstoss gegen Grundrechte gewertet. Art. 50a verstösst somit auch gegen geltendes Völkerrecht.</p> <p>Nebst diesem Verstoss gegen das Völkerrecht wird aber auch das Gebot der Verhältnismässigkeit aus Art. 36 BV nicht eingehalten, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Wie bereits bei Art. 16e, Art. 16f und Art. 16g erwähnt, müssen zuerst die einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.</p> <p>Zusätzlich, und wie bereits bei Art. 16d erwähnt, verhindert Art. 50a die effektive Erbringung von VPN-Diensten. Bei solch einem VPN kontrolliert der Betreiber sowohl den Eingangs- als auch den Endpunkt. Da die Kommunikation vom Endpunkt zu einer Webseite aufgrund der vorherrschenden Struktur im allgemeinen Internet nicht End-zu-End-Verschlüsselt erfolgen kann, werden schon kleine VPNs (mit 5000 Nutzern) dazu gezwungen ihre eigene Verschlüsselung zu entfernen und ihre Kunden zu überwachen. Da der Schutz der Privatsphäre der Nutzer*innen von VPNs just den Kernpunkt oder USP der Dienstleistung darstellt, werden Schweizer VPN-Anbieterinnen hierdurch am internationalen Markt übermässig benachteiligt, ja ihres eigentlichen Daseinszwecks beraubt.</p> <p>Wesentlich ist zudem, dass Anbieter von Mail- oder Messaging-Apps zwangsläufig die Nachricht in der App in einer menschenlesbaren Version anzeigen muss, und dass an dieser Stelle die End-zu-End-Verschlüsselung notwendigerweise bereits entfernt ist. Der Wortlaut von Art. 50a lässt entgegen sämtlichen Beteuerungen des Dienstes ÜPF bereits anlässlich der letzten Revision der VÜPF weiterhin offen, ob eine Entfernung der Verschlüsselung auch an dieser Stelle gefordert werden können soll. Angesichts der seit</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			Jahren erkennbaren Tendenz der Schweizer Überwachungsbehörden, die Anwendbarkeit des Überwachungsrechts laufend weiter auszudehnen und sich dabei nur durch Gerichte bremsen zu lassen, ist bei dieser Gelegenheit erneut die Klarstellung zu fordern, wonach die Entfernung von Verschlüsselungen, die erst in der Sphäre des Benutzers angebracht werden (wenngleich auch durch Software der Anbieterin) nicht verlangt werden darf. Dies ist zumindest im erläuternden Bericht zu erwähnen. Der erneute Verzicht wäre nichts anderes als eine Einladung an die Überwachungsbehörden, die Einführung einer offensichtlich illegalen und vom BÜPF keineswegs vorgesehenen «Chatkontrolle» auf dem «Auslegungsweg» vorzunehmen.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Artikel	Antrag	Begründung / Bemerkung	
VD-ÜPF / OME-SCPT / OE-SCPT			
Art. 14 Abs. 3 VD-ÜPF	Streichung	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit 5000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Absatz ist daher ersatzlos zu streichen.	
Art. 14 Abs. 4 VD-ÜPF	Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten.	Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der unterworfenen AAKD massiv. Dies ist wie beschrieben weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.	
Art. 20 Abs. 1 VD-ÜPF	Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.	

Eidgenössisches Justiz- und Polizeidepartement
Bundeshaus West
3003 Bern

Ausschliesslich per E-Mail an:
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Zürich, 06.05.2025

Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat Jans
Sehr geehrte Damen und Herren

Gerne nehmen wir die Möglichkeit wahr, innerhalb der festgesetzten Frist Stellung zur Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) zu nehmen.

Swico ist der Wirtschaftsverband der Digitalindustrie und vertritt die Interessen etablierter Unternehmen sowie Start-ups in Politik, Wirtschaft und Gesellschaft. Swico zählt über 750 Mitglieder aus der ICT- und Internetbranche. Diese Unternehmen beschäftigen 56'000 Mitarbeitende und erwirtschaften jährlich einen Umsatz von 40 Milliarden Franken.

Zusammenfassung:

Die vorgeschlagene Revision ist in weiten Teilen weder verhältnismässig noch gesetzeskonform, stellt einen unverhältnismässigen Eingriff in die Freiheitsrechte dar, bringt sicherheitspolitisch keinen Mehrwert, schwächt den Wirtschafts- und Innovationsstandort Schweiz und verursacht unnötige Mehrkosten und Bürokratie für die betroffenen Unternehmen.

Swico lehnt die Teilrevision der beiden Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehr (VÜPF, VD-ÜPF) entschieden ab. Wir fordern eine Rückweisung und eine umfassende, verhältnismässige und gesetzeskonforme Überarbeitung der beiden Vorlagen. In diesen Prozess sind die Wirtschaftsvertreter aktiv miteinzubeziehen. Zusammengefasst wollen wir folgende zentrale Kritikpunkte an der Vernehmlassungsvorlage besonders hervorheben:

1. Die erweiterte Betrachtung auf Basis des Gesamtumsatzes eines Unternehmens sowie bei den Schwellenwerten bei den Anbietern abgeleiteter Kommunikationsdienste (AAKD) betreffend die Teilnehmer wird die Anzahl Unternehmen, welche einer reduzierten oder

- vollständigen Pflicht unterliegen, deutlich erhöhen. Diese Ausweitung betrachtet Swico als unverhältnismässig.
2. Bei der Kategorisierung der Mitwirkungspflichtigen ist auf die Bedeutung der einzelnen Dienste abzustellen.
 3. AAKD sind – wie bis anhin – grundsätzlich von aktiven Überwachungspflichten zu befreien. Insbesondere die Pflicht zur Vorratsdatenspeicherung lehnen wir ab.
 4. Nur AAKD mit Diensten "von besonderer wirtschaftlicher Bedeutung" sind allenfalls zusätzliche Pflichten aufzuerlegen. Die Beurteilung, ob diese Qualifikation erreicht ist, hat sich auf den jeweiligen Dienst zu beziehen und darf nicht abhängig sein von allfälligen weiteren Aktivitäten des Anbieters. Das Abstellen auf den (Konzern-)Umsatz eines Unternehmens widerspricht den Vorgaben des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF).
 5. Faktisch werden die meisten AAKD (mit mehr als 5'000 Teilnehmenden) mit signifikanten neuen Pflichten belegt. Diese Praxisänderung bedarf einer Gesetzesänderung. Die Einführung entsprechender, neuer Pflichten auf dem Verordnungsweg verletzt Art. 164 der Bundesverfassung, wonach die wichtigen rechtsetzenden Bestimmungen auf Gesetzesstufe zu erlassen sind. Diese Pflichten-Erweiterung ist zudem inhaltlich in keiner Weise gerechtfertigt.
 6. Die zusätzlichen Pflichten wirken sich klar negativ auf den Innovations- und Wirtschaftsstandort Schweiz aus. Dies zumal Technologieanbieter, die im Verordnungsentwurf formulierten, umfassenden Überwachungspflichten bei der Sitz-Wahl und Investitionsentscheiden kritisch beurteilen. Die Schweiz gelangt im Vergleich zu anderen Standorten ins Hintertreffen.

1 Allgemeine Würdigung

Swico engagiert sich für die Sicherheit im digitalen Raum. In diesem konkreten Fall äussern wir jedoch beträchtliche Zweifel und Kritik. Aus den folgenden Gründen fordert Swico eine Rückweisung und eine umfassende, verhältnismässige und gesetzeskonforme Überarbeitung der beiden Verordnungen:

Die Revision ist unverhältnismässig und bringt keinen Sicherheitsgewinn

Die geplante Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) ist sicherheitspolitisch motiviert. Solch weitreichende Eingriffe in Grundrechte müssen jedoch verhältnismässig sein und somit ein legitimes öffentliches Interesse verfolgen, geeignet und erforderlich sein sowie zugunsten des öffentlichen Wohls ausfallen. Swico setzt sich für Sicherheit im digitalen Raum und eine wirksame Strafverfolgung ein. In diesem konkreten Fall gehen jedoch die vorgeschlagenen Änderungen deutlich über das hinaus, was für den Schutz der Gesellschaft zwingend nötig ist. Was übrig bleibt, ist ein starker Eingriff in die Freiheitsrechte jedes Einzelnen zugunsten eines politisch motivierten Sicherheitsbedürfnisses, das in dieser Form nicht zu rechtfertigen ist.

Gerne möchten wir anmerken, dass uns kein Nachweis vorliegt, dass die aktuellen Mittel und Kompetenzen der Strafuntersuchungsbehörden nicht mehr ausreichen würden, damit sie ihrer Aufgabenerfüllung nachkommen können.

Erweiterter Geltungsbereich für FDA und AAKD missachtet den Willen des Gesetzgebers

Der grösste Kritikpunkt an dieser Teilrevision ist die neu definierte Kategorisierung verbunden mit ausgeweiteten Mitwirkungspflichten für Fernmeldedienstanbieter (FDA) und AAKD. Als besonders kritisch erachten wir, dass mit dieser Vorlage aufgrund der tiefen Schwellenwerte für die Hoch- und Herunterstufung ein deutlich erweiterter Kreis an Unternehmen als AAKD eingestuft wird, der einer deutlich umfassenderen Regulierung und erweiterten Pflichten unterworfen wird. Es ist irritierend, werden die bewusst separat ausgestalteten Kategorien AAKD und FDA zunehmend einander angeglichen, und zwar zu Ungunsten der AAKD, die per Gesetz (Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs) gezielt als Kategorie mit grundsätzlich weniger weitreichenden Pflichten als die FDA konzipiert wurde. Dies missachtet den Willen des Gesetzgebers, den es zu wahren gilt.

Der Verordnungsentwurf zur VÜPF geht über die Bestimmungen des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) und dessen Auslegung durch den Bundesrat und Gerichte hinaus. Als Beispiel ist die Identifikationspflicht zu nennen, die die Gerichte ausdrücklich nicht vorsehen. Oder die vorgesehene Schwächung der Verschlüsselungen in Art. 50a, die bereits in anderen Fällen vom Gerichtshof für Menschenrechte als Verletzung der Grundrechte eingestuft wurde.

In welchem Missverhältnis die Konzeption des BÜPF mit jener der beabsichtigten VÜPF steht, zeigt auch die neue Kategorisierung der AAKD: Das BÜPF sieht vor, dass nur AAKD von grosser wirtschaftlicher Bedeutung oder mit einer grossen Benutzerschaft aktive Überwachungspflichten auferlegt werden sollen (Art. 22 Abs. 4, Art. 27 Abs. 3 BÜPF). Gemäss E-VÜPF sind AAKD aber bereits ab 5'000 Nutzerinnen und Nutzern massiven aktiven Überwachungspflichten ausgesetzt (insb. Benutzeridentifikation gemäss Art. 19 E-VÜPF, Vorratsdatenspeicherung gemäss Art. 21 E-VÜPF und Sicherstellen der Überwachungsbereitschaft gemäss Art. 31 E-VÜPF).

Datenschutz und Cybersicherheit nicht unter dem Deckmantel der Sicherheit aushöhlen

Die vorgesehenen Änderungen hin zu einer massiv ausgeweiteten Überwachung sind unverhältnismässig und stehen nicht mehr im Einklang mit Freiheit und Privatsphäre, welche im BÜPF fein austariert sind. Der grundrechtlich garantierte Anspruch auf sichere und vertrauliche Kommunikation wird mit der einseitigen Fokussierung auf überwachungsrelevante Aspekte ausgehöhlt. Indem de facto alle Anbieter verpflichtet werden, ihre Verschlüsselungssysteme für Behörden jederzeit entschlüsselbar zu gestalten, entstehen enorme Sicherheitsrisiken, die neue Schlupflöcher für Hackerangriffe, Datenmissbrauch und Spionage darstellen. Unseres Erachtens macht die Verpflichtung zur Sammlung von Randdaten Schweizer Unternehmen zu lukrativen Zielen krimineller Akteure.

Im schlimmsten Fall werden damit neue Risiken geschaffen, die Cybersicherheit und Datenschutz aushöhlen und den Interessen des Datenschutzes und unserer verfassungsmässigen Grundrechte widersprechen. Zum Datenschutz gehört auch das Prinzip der Datenminimierung. Dieses zentrale Prinzip sehen wir mit der starken Ausweitung der Pflichten als besonders verletzt.

Den Wirtschaftsstandort Schweiz nicht gefährden

Neben gesellschaftspolitischen Überlegungen sehen wir unseren Wirtschafts- und Innovationsstandort Schweiz in Gefahr.

Der Wirtschaftsstandort Schweiz steht derzeit aufgrund der internationalen Entwicklungen, namentlich der Infragestellung der regelbasierten Ordnung, unter grossem Wettbewerbsdruck. Vor diesem Hintergrund erachtet Swico es als absolut fahrlässig und unangebracht, den Technologiestandort Schweiz zu schwächen. Würde die Revision in der vorliegenden Form umgesetzt, würde aber genau dies passieren. Denn die betroffenen Dienste im Bereich der Datensicherheit leben vom Vertrauen und von der Rechtssicherheit.

Die Ausweitung der Überwachung und die damit verbundenen, übermässigen Mitwirkungspflichten machen die Schweiz für IT-Anbieter unattraktiv. Renommierte und innovative Unternehmen, die den Datenschutz ihrer Kundinnen und Kunden in den Fokus stellen, erfahren durch die Ausweitung der unverhältnismässigen Pflichten nicht nur einen finanziellen Schaden, sondern auch einen erwachsenden Vertrauens- und Reputationsverlust in digitale Lösungen. Die vorgeschlagenen Umsetzungsmassnahmen würden zu einer Schwächung des Wirtschafts- und Innovationsstandortes Schweiz führen.

Mit einer Ausweitung der fernmelderechtlichen Überwachungspflichten, wie sie die Vernehmlassungsvorlage vorsieht, werden die günstigen Rahmenbedingungen für Dienstleister in der Schweiz akut gefährdet. Der technische, administrative und infrastrukturelle Mehraufwand wäre besonders für KMU enorm und liesse sich nicht mit entsprechenden Vorteilen für den Strafvollzug und die Sicherheit der Bevölkerung rechtfertigen. Wir sind der festen Überzeugung, dass eine schlankere Regulierung mit weniger erfassten Unternehmen und risikobasierten Pflichten mindestens vergleichbaren Nutzen für die Strafvollzugsbehörden bringt, allerdings ohne einen wirtschaftlichen Kollateralschaden.

Fazit: Rückweisung und eine verhältnismässige sowie gesetzeskonforme Überarbeitung der Vorlage

Aus den aufgeführten Gründen lehnt Swico die vorgeschlagene Revision entschieden ab. Swico ist der Ansicht, dass die Vorlage gründlich überarbeitet werden muss. Zwingend ist dabei eine gesetzeskonforme Umsetzung. Die vorgeschlagene Ausweitung der Überwachungsbefugnisse auf Basis einer Verordnung ist vom Gesetzgeber so nicht gewollt. Eine dermassen breit angelegte Ausweitung von Pflichten auf Verordnungsstufe ist nicht haltbar. Solch einschneidende Änderungen sind auf Gesetzesebene zu erlassen, damit Schweizerinnen und Schweizer auch die Möglichkeit haben, darüber abzustimmen. Art. 164 der Bundesverfassung wird durch E-VÜPF verletzt. Swico anerkennt die Sicherheitsbedürfnisse von Staat und Bevölkerung. Grundrechtseingriffe müssen aber auch im digitalen Raum verhältnismässig sein. Schliesslich würde der vorliegende Entwurf den Technologiestandort Schweiz und seinen innovativen Unternehmen im Bereich der Datensicherheit nachhaltig schaden. Dies in einem Moment, in dem Vertrauen, Vorhersehbarkeit, Rechtssicherheit zentral wie nie zuvor sind.

2 Bemerkungen zu einzelnen Artikeln der E-VÜPF

Vorbemerkung: Den Grundsatz der Datenminimierung über alle Artikel hinweg verfolgen

Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung (Art. 6 Abs. 3 DSG) gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch ist das Prinzip der Datenminimierung zu verfolgen. Es darf nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kundinnen und Kunden auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.

Pikettdienst

Art. 11 Abs. 1

Gemäss E-VÜPF sollen alle Anbieterinnen mit vollen Pflichten (FDA und AAKD) einen Pikettdienst zur Verfügung stellen, der jederzeit erreichbar ist. Das bedeutet gemäss der neuen Konzeption der Kategorisierung von AAKD, dass ein Unternehmen, das einen inhaltlich nicht hoch relevanten, abgeleiteten Kommunikationsdienst (AKD) oder Fernmeldedienst erbringt (z.B. eine Sharing-Plattform für Kunden; Chat-Feature), aber konzernweit über einen Umsatz von mehr als CHF 100 Mio. erwirtschaftet, einen 24/7/365-Pikettdienst für Anfragen des Dienstes ÜPF betreiben muss. Auch kleinere FDA sind von dieser neuen Vorgabe betroffen, z.B. lokale Internet-Access-Anbieter, die in eine grössere Gemeindestruktur eingebunden sind.

Die neue Pflicht ist mit enormen zusätzlichen Kosten verbunden, zumal die Arbeitnehmenden für ihren Pikett-Einsatz vergütet werden müssen. Diesen Kosten steht ein nicht verhältnismässiger Nutzen gegenüber. Falls der Bundesrat trotzdem an der Implementierung eines solchen Pikettdienstes festhalten will, sind die Mitwirkungspflichtigen im Rahmen der Verordnung über die Finanzierung der Überwachung des Post- und Fernmeldeverkehrs (FV-ÜPF; SR 780.115.1) zusätzlich angemessen zu entschädigen.

Forderung Swico: Beibehaltung der bisherigen Regelung. Keine Pflicht zum Betrieb eines Pikettdienstes für AAKD. Falls trotzdem eine solche Pflicht eingeführt werden sollte, ist sie angemessen zu vergüten.

Definition von FDA

Art. 16a

Swico begrüßt die Klarstellung in Art. 16a Abs. 2 lit. a, dass die Übertragung von Informationen, die für die Allgemeinheit bestimmt sind, nicht als Erbringung eines Fernmeldedienstes gelten.

FDA mit reduzierten Pflichten

Art. 16b Abs. 1

Swico beurteilt die in der E-VÜPF definierten Unterscheidungskriterien, die über das Ausmass der Auskunfts- und Überwachungspflichten entscheiden, kritisch. Diese entsprechen in Teilen nicht den gesetzlichen Vorgaben des BÜPF und sind weder sachgerecht noch verhältnismässig.

Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft und ein erweiterter Kreis von FDA mit reduzierten Pflichten wird in eine FDA mit vollen Pflichten eingestuft.

Umsatzkriterium: Art. 16b Abs. 1 lit. b Ziff. 2 setzt als Kriterium auf den Umsatz der gesamten Unternehmung (sogar des gesamten Konzerns) anstelle nur der relevanten Teile oder Dienste (Art. 16b Abs. 1 lit. b Ziff. 2 E-VÜPF). Damit unterliegen Unternehmen mit einem jährlichen Gesamtumsatz von 100 Millionen Franken stets den vollen Überwachungspflichten für alle Dienste, obwohl gemäss dem erläuternden Bericht (S. 10) die Dienste differenziert betrachtet werden sollen. Damit findet die Bedeutung des jeweils angebotenen Dienstes keine Berücksichtigung, obwohl dies gemäss Art. 26 Abs. 6 BÜPF vorgesehen ist.

Die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten (konzernweit über CHF 100 Mio. Umsatz), wird so aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Mitwirkungspflichten in Kauf nehmen.

Kriterium der Anzahl Überwachungsaufträge: Auch wenn die relevante Anzahl Überwachungsaufträge bei 10 belassen wird (bisher Art. 51 VÜPF), so führt die Kombinierung der Anzahl Überwachungsaufträge mit anderen Diensten (z.B. AKD) dazu, dass der Schwellenwert schneller erreicht wird als unter geltendem Recht.

Forderung Swico: Anpassung des Textes in Art. 16b Abs. 1: «Auf Gesuch erklärt der Dienst ÜPF eine FDA für einen von ihr angebotenen Fernmeldedienst zur FDA mit reduzierten Pflichten, wenn dieser Dienst:
(a) als Fernmeldedienst im Bereich der Bildung und Forschung qualifiziert oder
(b) die beiden nachstehenden Grössen erreicht:
1. Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni);
2. Jahresumsatz in der Schweiz von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.»

Konzerntatbestand

Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2

Neu werden die Zahlen des jeweiligen Konzerns als Basis für die Hoch- und Herunterstufung herangezogen. Die neue Regelung soll gemäss erläuterndem Bericht für betroffene Unternehmen zu Erleichterungen führen. Die Begründung zur Einführung dieses «Konzerntatbestands» ist nicht haltbar. In der Praxis sind die betroffenen Unternehmen nämlich schon heute verpflichtet, ihre Buchhaltung nach Produkten aufzugliedern. Somit können die Kennzahlen bereits heute sehr einfach festgestellt werden.

Forderung Swico: Streichung des «Konzerntatbestand» und Beibehaltung der bestehenden Regelung.

Umsetzung der automatisierten Abfrage**Art. 16c Abs. 3, Art. 18 Abs. 2 Umsetzung der automatisierten Abfrage**

Wird eine FDA mit reduzierten Pflichten zu einer FDA mit vollen Pflichten eingestuft, so ist der vorgesehene Umsetzungszeitraum von 12 Monaten für die rechtssichere Implementierung eines derart komplexen Systems nicht zureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel.

Forderung Swico: Anpassungsfrist in Art. 16c Abs. 3 lit. a ist deutlich zu erhöhen.

Definition der Anbieter abgeleiteter Kommunikationsdienste: persönliche Speicher und VPN entfernen**Art. 16d**

Eine klarere Definition des Begriffs AAKD begrüssen wir. Jedoch geht die neue Auslegung nach den Ausführungen im erläuternden Bericht weit über den gesetzlichen Zweck hinaus. Der erläuternde Bericht nennt Onlinespeicherdiene wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter etc.) genutzt werden, als AAKD.

Wir sind der Ansicht, dass persönliche Speicher nicht Teil der Betrachtung sein sollten. Denn in Art. 2 lit. c BÜPF sind AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen» definiert. Das trifft auf persönliche Cloud-Speicher nicht zu. Erneut setzt man sich gegen die gesetzlichen Vorgaben des BÜPF hinweg. Onlinespeicherdiene sind deshalb aus Art. 16d zu streichen.

Zudem anerkennt der erläuternde Bericht zwar, dass VPNs zur Anonymisierung der Nutzerinnen und Nutzer dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil angebrachte Verschlüsselungen zu entfernen sind. Anbieter von VPNs sind daher ebenfalls aus Art. 16d auszunehmen. In der Botschaft vom 27. Februar 2013 zur Totalrevision de BÜPF hielt der Bundesrat fest, dass Anbieter von Verschlüsselungsprodukten keine AAKD sein sollen. Somit sind VPN-Anbieter von der Definition der AAKD explizit auszunehmen.

Forderung Swico: Online-Speicherdiene und VPN-Dienste sind von der Definition des AKD explizit auszunehmen.

Nichteinführung des Dreistufenmodells bei AAKDs**Art 16e, 16f und 16g**

Die vorgeschlagene Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Die Revision geht jedoch in die gegenteilige Richtung. Sie setzt die grosse Mehrheit der KMU, die AKD betreiben, einer überaus strengen Regelung aus, obwohl die BÜPF in Art. 26 Abs. 6 die wirtschaftliche Bedeutung eines Dienstes berücksichtigt.

Die Einführung von 5'000 Nutzern als gesondert zu beurteilende Untergrenze in Art. 16f Abs. 1 E-VÜPF verletzt Art. 22 Abs. 4 und Art. 27 Abs. 3 BÜPF, denn 5'000 Personen sind keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strenger Überwachungsmassnahmen, gerechtfertigt wären. 5'000 Nutzer werden in der digitalen

Welt vielmehr sehr rasch erreicht. Art. 22 und Art. 27 BÜPF verlangen zudem, dass nicht der Anbieter von besonderer wirtschaftlicher Bedeutung sein muss, sondern der Dienst.

Zusätzlich führt das Einführen eines Konzernatbestandes in Art. 16f Abs. 3 zu massiven Problemen, da die Produkte nun nicht mehr für sich allein eine bestimmte Grösse erreichen müssen. Vor allem bei Unternehmen mit Beteiligungsfirmen im Hintergrund fallen nun neu alle Dienstleistungen und Produkte automatisch unter die härteste Stufe, unabhängig von ihrem Entwicklungsstadium. Dies behindert Innovation und schwächt den Wirtschaftsstandort Schweiz.

Statt KMU zu entlasten, führt die Revision neu zu einem «automatischen» Hochstufung per Verordnung ohne Verfügung (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.

Die automatische Hochstufung wie sie in den Artikeln 16ff vorgesehen ist, führt zu erheblicher Rechtsunsicherheit. Unter dem bestehenden System werden die generell-abstrakten Normen der VÜPF mittels Verfügung auf einen konkreten Einzelfall angewendet. Unter dem revidierten System entfällt dieser Schritt und eine AAKD wird automatisch hochgestuft, sobald sie den Schwellenwert erreicht. Von einer automatischen Hochstufung von AAKD ist aus Gründen der Rechtssicherheit abzusehen. Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.

Gegenüber der aktuellen VÜPF erweitert die vorgeschlagene Revision die Pflichten zur Automatisierung noch einmal deutlich auf neu alle AAKD mit vollen Pflichten und sie schafft mehrere neue problematische Abfragen, wie z.B. IR_59 (Art. 42a E-VÜPF) und IR_60 (Art. 43a E-VÜPF), welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen. Genau diese Möglichkeit einer manuellen Intervention ist aber für die Provider kritisch, um Missbräuche zu verhindern, die wiederum die Verträge mit ihren Kunden und das Fernmeldegeheimnis verletzen könnten. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente damit erheblich und damit auch das Risiko für die Wahrung der Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.

Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 Bst. b der aktuellen VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grossen[n] Teil ihrer Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. Damit fallen auch Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz. Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Dies setzt der Innovation in der Schweiz neue, riesige Hürden entgegen.

Durch die von der E-VÜPF ausgeweitete Vorratsdatenspeicherung wächst das Risiko für die Verletzung der Sicherheit und der Privatsphäre der Nutzerinnen und Nutzer dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, sondern allein diese Anhäufung an Daten malt eine Zielscheibe auf den Rücken von Schweizer Unternehmen und Dienstleistungen für Hackerangriffe aus der ganzen Welt. Weiter ist zu erwähnen, dass es gar nicht erwiesen ist, dass die Speicherung der fraglichen Daten eine merklich höhere Quote erfolgreicher Ermittlungen durch die Strafverfolgungsbehörden mit sich bringen würde. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Massnahmen mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden. Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes und nicht durch eine reine Verordnung zu implementieren.

Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung sowie das Datenschutzgesetz. Der Entwurf bringt keine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, behindert Innovation in der Schweiz und schwächt die innere Sicherheit.

Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen, und das bestehende System muss beibehalten werden.

Forderung Swico: Streichung der Artikel 16e, 16f und 16g sowie Beibehaltung der bestehenden Kriterien. Beibehaltung der Art. 22, 51 und 52. Zudem soll es eine Ausnahme für Pilotprojekte (auch von grossen Firmen) und Non-Profits per se geben.

Eventualiter Die Schwellenwerte sind stark zu erhöhen und auf Ebene der "Dienste" anzusetzen, damit die VÜPF die Anforderungen des BÜPF betreffend "grosse wirtschaftliche Bedeutung" bzw. "grosse Benutzerschaft" einhält.

- Streichung des Konzernatbestandes in Art. 16f Abs. 3 und Art. 16g Abs. 2.
- Streichung der automatisierten Auskünfte in Art. 16g Abs. 3 lit. b Ziff. 1 und Abschaffung der Verpflichtung der AAKD zur Speicherung in Art. 16g Abs. 3 lit. a Ziff. 2 von Randalten zu Zwecken rückwirkender Überwachung.

Erleichterungen für Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen

Art. 16h Abs. 2

Art. 16h Abs. 2 E-VÜPF definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Nutzerinnen und Nutzer den Zugang nutzen können. Der Erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität)». Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 E-VÜPF, gemäss dem die das WLAN erschliessenden FDA die Verantwortung für die Nutzer der WLANs tragen.

Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzerinnen und Nutzer zulassen kann, etwa durch die Nutzung mehrerer Subnetze oder die Aggregation von IP-Adressbereichen. Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDAs unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates, offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden. Unter der bestehenden Regelung konnte eine FDA anhand der Lokation (z.B. Bibliothek, Flughafen) eine Einschätzung treffen. Die neue Definition hingegen würde von ihr verlangen, Zugriff auf jedes private Netzwerk zu erhalten, um Hardware und Einstellungen zu prüfen – ein offensichtlich verfassungswidriges und auch praktisch unmögliches Unterfangen. Diese vage Formulierung führt zu anhaltender Rechtsunsicherheit für FDA.

Forderung Swico:

- Streichung der Ausführung im Erläuternden Bericht. Das Kriterium «professionell betrieben» ist nach der bislang geltenden Regelung zu verstehen.
- Art. 16h Abs. 2 ist ersatzlos zu streichen und im Zusammenhang mit Art. 19 Abs. 2 ist auf die aktuelle Definition von «professionell betrieben» abzustellen.

Streichung der Identifikationspflichten für AAKDs**Art. 19**

Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD (auch mit reduzierten Pflichten), widerspricht direkt der Regelung des BÜPF, die eine solche Pflicht nur für sehr wenige AAKD vorsieht (Art. 22/27 BÜPF). Eine Überwachung von Kunden durch FDA, ob erstere die neuen Vorgaben der VÜPF zu WLANS einhalten (Art. 19 Abs. 2 E-VÜPF), ist weder gesetzeskonform noch zumutbar.

Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des Schweizer Datenschutzgesetzes, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch der Schutz der Schweizer Kundschaft massiv beeinträchtigt wird. Datenschutzfreundliche Unternehmen werden bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.

Forderung Swico: Streichung «AAKD mit reduzierten Pflichten» in Art. 19 Abs. 1 und Beibehaltung des aktuellen Art. 19 Abs. 2 VÜPF.

Reduktion der Auskunftspflichten für AAKDs**Art. 18 Abs. 3**

Wie bereits zu Art. 16e bis 16f dargelegt, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Die Konzeption des BÜPF sieht vor, dass nur AAKD mit Diensten von besonderer wirtschaftlicher Bedeutung aktive Überwachungspflichten auferlegt werden sollen. An diesem Konzept gilt es festzuhalten.

Forderung Swico: Streichen. Das bisherige Konzept ist beizubehalten.

Identitätsnachweis**Art. 20a Abs. 1**

Swico empfiehlt, die e-ID gemäss BGEID als gültigen Identitätsnachweis mitaufzunehmen.

Streichung der Aufbewahrungspflichten für AAKDs mit reduzierten Pflichten**Art. 21 Abs. 1 lit. a**

Wie bereits bei Art. 16e bis 16f dargelegt, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. Die Konzeption des BÜPF sieht vor, dass nur AAKD mit Diensten von besonderer wirtschaftlicher Bedeutung aktiven Überwachungspflichten auferlegt werden sollen. An diesem Konzept gilt es festzuhalten.

Die Anpassung von Art. 21 Abs. 6 E-VÜPF ist konzeptionell falsch. Anbieter von Telefonie- und Multimedialiendiensten sind per Definition FDA, vgl. Anhang zur VÜPF, Ziff. 8 und 9.

Klassische OTT-Anbieter von Videokonferenz-Lösungen sind keine Multimedialiendienste. Sie werden erst dann zum Multimedialiendienst, wenn sie zusammen mit einem Telefondienst angeboten werden.

Forderung Swico:

- AAKD mit reduzierten Pflichten sind aus Art. 21 Abs. 1 lit. a zu streichen.
- Zudem ist Art. 21 Abs. 6 gänzlich zu streichen.

Erweiterte Auskunft bei juristischen Personen**Art. 27 Abs. 2**

Gemäss der heutigen Regelung ist die flexible Suchfunktion für Namen von natürlichen Personen möglich. Diese flexible Suchfunktion wurde eingeführt, um ein in der Praxis auftretendes Problem bei der Eingabe von Personennamen zu beheben. Insbesondere bei etwas komplizierteren, nicht geläufigen Namen werden teilweise fehlerhafte bzw. nicht ganz korrekte Eingaben getätigt.

Die nun vorgeschlagene Erweiterung auf juristische Personen lässt sich nicht rechtfertigen. Erstens sind den FDA im Bereich der juristischen Personen keine ähnlichen, regelmässig auftretenden Probleme bei der Sucheingabe bekannt und auch in den Erläuterungen wird hierzu nichts ausgeführt. Im Gegensatz zur Personensuche stehen den Strafverfolgungsbehörden bei der Firmensuche ausserdem öffentlich zugängliche Tools zur Verfügung. Den Strafverfolgungsbehörden kann zugemutet werden, eine entsprechende Kontrolle bzw. Suche bei Bedarf selbst durchzuführen. Eine Abwäzung auf Mitwirkungspflichtige ist vor diesem Hintergrund unnötig und unverhältnismässig. Die Implementierung von neuen technischen Funktionen sind bei allen betroffenen Anbietern mit einem nicht unerheblichen Entwicklungsaufwand und entsprechenden Kosten verbunden.

Forderung Swico: Beibehaltung des aktuellen Art. 27 Abs. 2**Nachweis der Auskunfts- und Überwachungsbereitschaft für AAKD mit reduzierten Pflichten****Art. 31 Abs. 1**

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. Die Konzeption des BÜPF sieht vor, dass nur AAKD mit

Diensten von besonderer wirtschaftlicher Bedeutung aktiven Überwachungspflichten auferlegt werden sollen. An diesem Konzept gilt es festzuhalten.

Forderung Swico: AAKD mit reduzierten Pflichten sind von allen Pflichten nach Art. 31 E-VÜPF zu befreien.

Aufhebung der Toleranzabweichung für Mitwirkungspflichtige

Art. 38 Abs. 2

Der Wortlaut von Art. 38 Abs. 2 VÜPF wird materiell nicht angepasst und auch gemäss den Erläuterungen soll bei diesem Auskunftstyp inhaltlich nichts geändert werden. In denselben Erläuterungen wird jedoch ergänzend angemerkt, dass die beauftragten Mitwirkungspflichtigen bei der Suche und Identifikation der Benutzer, der Urheberschaft oder der Herkunft mögliche Toleranzabweichungen der Systemuhren zu berücksichtigen haben.

Eine solche Berücksichtigung stellt eine materielle Änderung dar, die Seitens der FDA in dieser Form jedoch nicht umgesetzt werden kann. Die Herkunft und Details zur Urheberschaft der Daten sind bei der Übermittlung des Auftrags an die Mitwirkungspflichtigen jedoch nicht vorgesehen. Ihnen ist die Herkunft der Daten, die dem Auftrag zu Grunde liegen, die dort vorhandene technische Infrastruktur und die für die Synchronisation der Zeit verwendeten Methoden und Funktionen somit nicht bekannt. Ohne diese Informationen ist eine Einschätzung von Toleranzabweichungen der Systemuhren bei den FDA jedoch nicht möglich.

Änderung: Die Anmerkungen in den Erläuterungen zu Art. 28 Abs. 2 sind zu streichen.

Neue Auskunftstypen für E-Mail-Dienste und Zugriff auf FDA und AAKD

Art. 42a und Art. 43a

Die Art. 42a und 43a führen neu die Abfragetypen «IR_59_EMAIL_LAST» und «IR_60_COM_LAST» ein, über die sensible Daten automatisiert abgefragt werden können. Sie verlangen von Anbietern, dass sie jederzeit Auskunft geben können bezüglich des letzten Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Auch für das Auferlegen dieser Pflicht gilt die fragliche Schwelle von 5'000 Nutzerinnen und Nutzer (AAKD mit reduzierten Pflichten). Erfasst ist somit nahezu die gesamte AAKD-Landschaft der Schweiz.

Das Problem liegt (abgesehen von grundsätzlichen Fragen der Zulässigkeit einer solchen Pflicht) darin, dass die «IR_»-Abfragen zu Informationen nach Art. 42a und 43a neu automatisiert abgerufen werden können – im Gegensatz zu den «HD_»- (historische Daten) und «RT_» (Echtzeitüberwachung) Abfragen, die strengeren Regeln und einer juristischen Kontrolle unterliegen. Bei den «IR_59»- und «IR_60»-Abfragen handelt es sich allerdings um sensible Informationen, wie etwa das Abrufen einer IP-Adresse. Solche Informationen mussten bislang zurecht über strengere Abfragetypen eingeholt werden.

Künftig könnten so umfangreiche Informationen über die neuen Abfragetypen beschafft werden, die bislang den strengereren Regeln der rechtlich sichereren Informations-/Überwachungstypen «HD_» und «RT_» unterworfen waren. «IR_59» und «IR_60» ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne den erforderlichen Kontrollen dieser invasiven Überwachungstypen unterworfen zu sein.

Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind. Die AAKD müssten künftig gewisse Datenkategorien systematisch erheben, um dieser Pflicht nachzukommen.

Forderung Swico: Streichung Art. 42a und 43a, alternativ die Erwähnungen der Protokolle, IP-Adressen und des Ports des Clients streichen

Verschlüsselungen

Art. 50a

Art. 50a sieht vor, dass Anbieterinnen und Anbieter verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Auch diese Pflicht soll eine Vielzahl neuer Unternehmen erfassen: Betroffen sind nicht mehr nur FDA (Art. 26 BÜPF) und ausnahmsweise AAKD (Art. 27 BÜPF), sondern sämtliche Anbieterinnen und Anbieter mit mehr als 5'000 Nutzerinnen und Nutzer. Im Ergebnis wäre fast die gesamte Schweizer AAKD-Branche betroffen.

Die Ausdehnung dieser Pflicht auf AAKD stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar: Es findet keine Einzelfallprüfung statt und die AAKD werden dieser Pflicht unterworfen, auch wenn sie keineswegs Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten (Art. 27 Abs. 3 BÜPF).

Problematisch ist zudem, dass aufgrund dieser Vorgabe Anbieterinnen und Anbieter ihrer Verschlüsselungen so konfigurieren müssen, dass sie von ihnen aufgehoben werden können – eine durch Anbieterinnen und Anbieter aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung allerdings in jedem Fall. Dies führt zu schwächeren Verschlüsselungen und der Abnahme der Sicherheit von Kommunikationsdiensten.

Forderung Swico Streichung des Art. 50a

Echtzeitüberwachung von Randdaten

Art. 55a

Die Mitwirkungspflichtigen müssen neu einen Teil der in Echtzeit aufgezeichneten Inhaltsdaten wieder aussortieren. Welche Daten bzw. IP-Pakete entfernt bzw. geliefert werden müssen, wird dabei von der anordnenden Strafverfolgungsbehörde bestimmt. Diese vorgesehene Aussonderungspflicht durch die Mitwirkungspflichtigen ist problematisch und entspricht nicht der gesetzlich vorgegebene Aufgabenteilung.

Gemäss Art. 17 Bst. g BÜPF gehört es nämlich zu den Aufgaben des Dienstes ÜPF auf Ersuchen der anordnenden Behörde eine allfällige Sortierung vorzunehmen und bestimmte Daten aus dem Datenfluss herauszufiltern. Diese Aufgabe fällt somit und entgegen der in Art. 55a E-VÜPF vorgeschlagenen Regelung dem Dienst ÜPF und nicht den Mitwirkungspflichtigen zu. Eine Abwälzung auf die Mitwirkungspflichtigen lehnen wir ab.

Forderung Swico: Streichung Art. 55a

Rückwirkende Überwachung

Art. 60a

Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde laut den Erläuterungen bewusst auch falschpositive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten.

Forderung Swico: Art. 60a streichen.

Übergangsfristen

Art. 74a

Bei den Auskünften gemäss Art. 38a, 42a und 43a handelt es sich um neue, komplexe Auskunftstypen, die von Grund auf neu entwickelt, implementiert und erfolgreich getestet werden müssen. Sollte Art. 42a und 43a wider Erwarten nicht gestrichen werden, so ist in Art. 74c E-VÜPF veranschlagte Umsetzungsfrist von 6 Monaten klarerweise zu kurz bemessen. Eine Übergangsfrist von 18 Monaten wäre vor diesem Hintergrund angemessen. Sollte Art. 60a E-VÜPF und Art. 55 E-VÜPF wider Erwarten nicht gestrichen werden, so gilt es auch darauf hinzuweisen, dass die benötigte minimale Umsetzungsfrist 18 Monate beträgt, da die beiden Überwachungstypen in Zusammenarbeit mit externen Lieferanten von Grund auf neu entwickelt werden müssten.

Forderung Swico: Für die Umsetzung der Artikel 38a, 42a und 43a sowie falls Art. 55a und 60a wider Erwarten nicht gestrichen werden, benötigt es eine Übergangsfrist von 18 Monaten.

3 Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Art. 14 Abs. 3 VD-ÜPF

Wie bereits bei Art. 16e bis 16f E-VÜPF angesprochen, ist ein aktives Tätigwerden für alle AAKD (auch für solche mit mehr als 5'000 Nutzerinnen) unverhältnismässig und wirtschaftlich nicht tragbar, was das Einführen von Fristen obsolet werden lässt.

Forderung Swico: Keine Anpassung der aktuellen Bestimmung.

Art. 14 Abs. 4 VD-ÜPF

Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der unterworfenen AAKD – da auch AAKD mit reduzierten Pflichten erfasst sind – massiv. Dies ist wie bereits ausgeführt, weder durch das BÜPF gedeckt, noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.

Forderung Swico: Änderung von «AAKD mit minimalen Pflichten» zu «AAKD ohne volle Pflichten»

Art. 20 Abs. 1 VD-ÜPF

Wie bereits bei Art. 16e bis 16f E-VÜPF angesprochen, ist ein aktives Tätigwerden für alle AAKD (auch für solche mit mehr als 5'000 Nutzerinnen und Nutzer) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.

Forderung Swico: Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»

Wir bedanken uns für die Berücksichtigung unserer Anliegen und stehen für Rückfragen gerne zu Verfügung.

Freundliche Grüsse
Swico



Dr. Jon Fanzun
CEO



Simon Ruesch
Head Legal & Public Affairs
Mitglied der Geschäftsleitung

An das
Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundeshaus West
3003 Bern

per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

6. Mai 2025

—

**Stellungnahme der Orange Business Switzerland AG im Vernehmlassungsverfahren zu den
Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs
(VÜPF, VD-ÜPF)**

Sehr geehrter Herr Bundesrat,
Sehr geehrte Damen und Herren,

Wir nehmen Bezug auf die am 29. Januar 2025 eröffnete Vernehmlassung zur Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) und danken Ihnen für die Einladung zur Stellungnahme.

Über Orange Business Switzerland AG

Die Orange Business Switzerland AG, Beethovenstrasse 48, 8002 Zürich, bietet als Teil der französischen Orange-Gruppe IT- und Telekommunikationsdienste für multinationale Unternehmen an. Dabei ist Orange Business Switzerland AG ausschliesslich im Business-to-Business (B2B) Segment für globale Unternehmen mit Hauptsitz in der Schweiz tätig.

Als Netzwerk- und Digitalintegratorin bietet die Orange Business Switzerland AG in der Schweiz Fernmeldedienste in Bereich durchgängig gesicherter digitaler Infrastruktur an, ist aber auch als Wiederverkäuferin von Hard- und Softwarelösungen sowie im Bereich Consulting insbesondere im Bereich Cybersicherheit tätig. Gerade Consultingleistungen und die Modernisierung von Kundenanbindungen mit modernster Hardware, sowie Netzwerkmanagementdienste werden in den letzten Jahren vermehrt nachgefragt.



Business Services

Zu unseren Kunden gehören neben multinationalen Unternehmen aus den Bereichen Finanz- und Versicherungswesen, Medizin, Chemie sowie Lebens- und Genussmittel auch Behörden und internationale Organisationen, die für ihre weltweit vernetzten Tätigkeiten höchste Anforderungen an Zuverlässigkeit und Sicherheit stellen.

Die Orange Business Switzerland AG ist seit langem aktives Mitglied des Schweizerischen Verbands der Telekommunikation (asut) und stimmt der Ihnen zugegangenen Stellungnahme der asut im Vernehmlassungsverfahren zu den Teilrevisionen der VÜPF und VD-ÜPF vollinhaltlich zu.

Angesichts der Tragweite der angestrebten Änderungen und der Schwierigkeiten, die wir damit sehen, möchten wir auf einige Aspekte aber auch noch gesondert eingehen und nutzen daher die Gelegenheit zur Stellungnahme.

Bisherige Rechtssicherheit durch die Regelung in Art 51 VÜPF

Art 26 (6) BÜPF gibt dem Bundesrat die Möglichkeit, Anbieterinnen von Fernmeldediensten (FDA) von bestimmten gesetzlichen Pflichten zu befreien.

Die Orange Business Switzerland AG hat es sehr begrüßt, dass der Bundesrat mit der Verordnung vom 15. November 2017 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) von dieser Möglichkeit Gebrauch gemacht und im Art. 51 VÜPF vorgesehen hat, FDA unter bestimmten Voraussetzungen das Recht auf reduzierte Überwachungspflichten zu gewähren.

Damit wurde eine rechtssichere Lösung geschaffen, die Unternehmen seither Planungssicherheit gewährleistet hat. Die Schweiz war hier federführend und die klare, einfache, sachgerechte Schweizer Regelung wurde in anderen Ländern wiederholt als Beispiel für Rechtssicherheit, sowie Verwaltungsvereinfachung und Verhältnismässigkeit gepriesen.

Der Umfang der reduzierten Überwachungspflichten ist sehr klar umrissen und ein entsprechender Antrag, als FDA mit reduzierte Überwachungspflichten eingestuft zu werden, kann bisher beim Dienst ÜPF einfach eingereicht werden, wobei nachgewiesen werden muss, dass Überwachungsaufträge zu weniger als 10 verschiedenen Zielen der Überwachung in den letzten 12 Monaten eingingen bzw. der in der Schweiz erwirtschaftete Jahresumsatz mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten der letzten zwei Geschäftsjahren unter der Schwelle von 100 Mio Franken lag.

Veränderte Umsatzschwellen bringen keine Vereinfachung

Diese klare Regelung soll nun laut den erläuternden Bericht vom 8. Januar 2025¹ zu Artikel 16 Buchstabe b Ziffer 2 vereinfacht werden, indem nicht mehr auf den Jahresumsatz in der Schweiz mit Fernmelddiensten und abgeleiteten Kommunikationsdiensten abgestellt wird (s. bisheriger Art. 51 Abs. 1 Bst. b Ziff. 2 VÜPF), sondern auf den gesamte Unternehmensumsatz in der Schweiz, "da es sich in der Praxis gezeigt hat, dass der gesamte Unternehmensumsatz viel einfacher ermittelt und belegt werden kann."

Eine Vereinfachung durch ein geplantes Abzielen auf den gesamten Unternehmensumsatz in der Schweiz erschliesst sich uns nicht. Seit 1998 werden im Rahmen der Fernmeldestatistik Daten erhoben und veröffentlicht. Nach Artikel 59 Absatz 2 des Fernmeldegesetzes vom 30. April 1997 (FMG; SR 784.10) haben Anbieterinnen von Fernmelddiensten dem BAKOM regelmässig die zur Erstellung einer amtlichen Fernmeldestatistik erforderlichen Angaben einzureichen. Teil dieser Angaben sind auch der Jahresumsatz in der Schweiz mit Fernmelddiensten.

Eine Änderung der bisherigen Regelung erscheint uns darüber hinaus auch nicht sachgerecht, denn sie entspricht nicht dem Wesen dem der Verordnung VÜPF zugrundeliegenden Gesetzes BÜPF. Das BÜPF gibt in seinem § 1 klar vor, dass es sich beim sachlichen Geltungsbereich um die Überwachung des Post- und Fernmeldeverkehrs handelt.

Nachdem das BÜPF als sachlichen Geltungsbereich die Überwachung des Post- und Fernmeldeverkehrs festlegt, müssen sich die Regelungen der VÜPF als nachgeordneter Verordnung auf denselben sachlichen Geltungsbereich beziehen. Ein Abzielen auf den gesamten Unternehmensumsatz in der Schweiz würde gleichsam eine Ausdehnung des Geltungsbereichs der VÜPF auf alle Tätigkeitsbereiche eines Unternehmens in der Schweiz zur Folge haben, auch auf solche, die nicht dem Post- und Fernmeldeverkehr zugeordnet werden können. Das kann vom Verordnungsgeber nicht gewollt sein.

Sachgerecht erschiene insofern, für Anbieterinnen von Fernmelddiensten auch weiterhin und wie bisher in Art 51 VÜPF nur den Jahresumsatz in der Schweiz mit Fernmelddiensten und abgeleiteten Kommunikationsdiensten in Betracht zu ziehen.

¹ https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2022/21/cons_1/doc_7/de/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2022-21-cons_1-doc_7-de-pdf-a.pdf

Wir beantragen daher, die neue Regelung des Artikel 16 Buchstabe b Ziffer 2 der (künftigen) VÜPF angelehnt an die bisherige Regelung in Art 51 (geltende) VÜPF folgendermassen zu formulieren:

Art 16

- 1 Auf Gesuch erklärt der Dienst ÜPF eine FDA für bestimmte Fernmelddienste zur FDA mit reduzierten Pflichten, wenn sie:
 - a. diese Fernmelddienste nur im Bereich Bildung und Forschung anbietet.
 - b. **keine eine** der nachstehenden Grössen **nicht** erreicht:
 1. Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmelddienste und abgeleiteten Kommunikationsdienste;
 2. Jahresumsatz in der Schweiz ~~des gesamten Unternehmens~~ mit Fernmelddiensten und abgeleiteten Kommunikationsdiensten von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.
- 2 Kontrolliert eine Anbieterin im Sinne von Artikel 963 Absatz 2 des Obligationenrechts ein oder mehrere rechnungslegungspflichtige Unternehmen, so sind bei der Bestimmung der Anzahl der Überwachungen und des Jahresumsatzes mit Fernmelddiensten und abgeleiteten Kommunikationsdiensten die Anbieterin und die kontrollierten Unternehmen als Einheit zu betrachten.
- 3 Eine FDA mit reduzierten Pflichten ist verpflichtet, dem Dienst ÜPF schriftlich Meldung zu erstatten und entsprechende Belege einzureichen, wenn:
 - a. sie die betreffenden Fernmelddienste nicht mehr ausschliesslich im Bereich Bildung und Forschung anbietet;
 - b. ihr Jahresumsatz mit Fernmelddiensten und abgeleiteten Kommunikationsdiensten die Grösse nach Absatz 1 Buchstabe b Ziffer 2 erreicht hat; die Mitteilung muss innerhalb von drei Monaten nach dem Abschluss des Geschäftsjahres erfolgen.
- 4 Der Dienst ÜPF kann die durch den Vollzug der Gesetzgebung betreffend die Überwachung des Post- und Fernmeldeverkehrs oder die aufgrund des Vollzugs von Bundesrecht vorhandenen Daten anderer Behörden zur Verifizierung der möglichen Über- oder Unterschreitung der Grössen nach diesem Artikel nutzen.

Durch die geplante Erweiterung des Kreises der Verpflichteten steigen die Kosten, die Strafverfolgung profitiert nicht

Besonders bemerkenswert an der bisherige Regelung war im internationalen Vergleich, dass damit eine Balance zwischen den für die Strafverfolgung relevantesten Datenquellen bei monetär vertretbarem Aufwand für die Bundeskasse gefunden wurde.



Business Services

Wie auch die vor kurzem veröffentlichte Statistik des Dienstes ÜPF² zeigt, sind zwar die absoluten Zahlen der verschiedenen Überwachungsmassnahmen im vergangenen Jahr gestiegen, relativ gesehen sind aber nach wie vor nur einige wenige grosse Fernmeldediensteanbieterinnen für den überwiegenden Teil der Massnahmen und somit die Mithilfe bei der Aufklärung von schweren Straftaten essentiell.

Alle anderen Mitwirkungspflichtigen haben demgegenüber nur sehr wenige Überwachungsmassnahmen zu vertreten.

Eine – wie nunmehr durch die veränderte Regelung geplante – weitgehende Verpflichtung vieler anderer, kleinerer Unternehmen durch die Veränderung des relevanten Umsatzes scheint weder aus Gründen der verbesserten Strafverfolgung, noch aus Gründen der Wirtschaftlichkeit sinnvoll. Investitionen in hoher 6 bis 7-stelliger Zahl auf Seiten der Unternehmen und ein gesteigerter Aufwand für Entschädigungen seitens des Bundes wären die Folge – ohne sicherheitsrelevantem Mehrgewinn.

Wir bitten Sie daher, bei der geplanten Neuregelung nicht über das Ziel hinauszuschiessen und den Text noch einmal sorgfältig zu prüfen, im Hinblick auf die Gesetz- und Verhältnismässigkeit der geplanten Vereinfachung, aber auch im Hinblick auf die zu erwartenden Kosten und dem erwarteten geringen Zugewinn für die Strafverfolgung.

Freundliche Grüsse

i.A. Dr. Margit Brandl

Senior Regulatory Counsel

für die Orange Business Switzerland AG

² <https://www.li.admin.ch/de/stats>

**Vernehmlassungsantwort zu den Teilrevisionen der VÜPF und der VD-ÜPF
gemäss Schreiben des EJPD vom 29. Januar 2025**

Datum	05. Mai 2025
Verfasser (Unternehmen)	Alfred Künzler, Init7 (Schweiz) AG
Kontaktperson bei Fragen (Name/Tel./E-Mail)	Alfred Künzler, (kuenzler at init7 dot net)

Dieses Dokument geht an:

Eidgenössisches Justiz- und Polizeidepartement EJPD, ptss-aemterkonsultationen@isc-eipd.admin.ch

Sehr geehrter Herr Bundesrat Jans, sehr geehrte Damen und Herren

Wir beziehen uns auf das am 29. Januar 2025 eröffnete Vernehmlassungsverfahren zu Teilrevisionen von VÜPF und VD-ÜPF und bedanken uns für die Möglichkeit einer Stellungnahme.

Wir lehnen die geplante Teilrevisionen der VÜPF und der VD-ÜPF in aller Deutlichkeit und vollumfänglich ab.

Im Bericht des Bundesrates zur aktuellen Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF und der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) ist zu lesen, dass die Revision im Wesentlichen auf die Anpassung der Verordnungen an die KMU-Freundlichkeit abziele. Ein grosser Teil der vorgeschlagenen Änderungen verfolgt aber gerade das Gegenteil.

Die Geschäftsgrundlagen von Schweizer Unternehmen wie Threema, Proton und anderer KMU, die weltweit einen hervorragenden Ruf als Anbieterinnen sicherer Kommunikationsdienste im Internet geniessen, drohen durch die Vorlage zerstört zu werden. Die Sicherheit des Internets in der Schweiz soll mit der Revision der Überwachung jeglichen Internetverkehrs regelrecht untergeordnet werden: **«Sicherheit vor Freiheit» ist das neue Paradigma.** Dieses zieht sich wie ein roter Faden quer durch diese völlig verunglückte Reform. KMU, die aus der Schweiz heraus Internet-Dienste anbieten («abgeleitete Kommunikationsdienste» in der Terminologie des Gesetzes), soll die Schweiz als Standort geradezu vergällt werden. Dies scheint denn auch zu gelingen: **Erste der betroffenen Unternehmen haben bereits angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen** (siehe Tages-Anzeiger vom 1. April 2025).

Ein derartiger Paradigmenwechsel, weg von KMU-Schutz und Überwachung mit Augenmass, hin zu knallharter Überwachung, die alle anderen Interessen unterordnet, wird durch das geltende Gesetz (BÜPF) keineswegs gestützt. Der Paradigmenwechsel widerspricht vielmehr geradezu dem Geist des ursprünglichen BÜPF, das Internetdienste, die in der Schweiz meist von KMU betrieben werden, gerade von der Implementierung teurer Überwachungsmassnahmen schützen wollte, und das eine austarierte Interessenabwägung vorsah zwischen Privatsphäre und Freiheit auf der einen Seite und staatlicher Überwachung auf der anderen Seite.

Entgegen dem im Begleitbericht zum vorgelegten Entwurf erklärten Ziel, die «finanzielle Belastung der KMU gering zu halten», stuft die Vorlage eine grosse Mehrheit der Schweizer Anbieterinnen von Internetdiensten in eine höhere Stufe auf, und zwingt sie neu auch in jenen Bereichen zu einer kostspieligen aktiven Überwachungstätigkeit, wo bisher nur eine KMU-freundliche Duldungspflicht bestand. Dies verschiebt das bisherige Gleichgewicht der Interessen zwischen Strafverfolgung und betroffenen Anbieterinnen in drastischer Weise zugunsten der betroffenen Anbieterinnen. Die vorgeschlagenen Anpassungen bringen ganz erhebliche Risiken für den Innovations- und Wirtschaftsstandort Schweiz mit sich und erfüllen die Kernziele der Revision, die Entlastung von KMU, gerade nicht. Der Ruf der Schweiz als sicherer Hafen für vertrauenswürdige IT-Anbieter droht durch die Revision nachhaltig beschädigt zu werden. Deshalb lehnen wir die Revision vollumfänglich ab.

Auch die Schweizer Armee nutzt solche Dienste, wie beispielsweise Threema, und zwar gerade aufgrund des hohen gebotenen Sicherheitsstandards. Die Annahme dieser Revision, welche dieses Sicherheitsniveau gezielt untergraben will, verletzt damit indirekt auch das direkte Interesse der Schweiz an lokal betriebenen Hochsicherheitsanwendungen. Gerade in der heutigen Zeit, in der die Zuverlässigkeit der grossen US-Anbieter in ihrer Abhängigkeit von einer zunehmend erratisch agierenden US-Regierung mehr und mehr in Frage steht, erscheint dies als **inakzeptable Hochrisikostrategie**.

Nicht zuletzt ist mit Nachdruck darauf hinzuweisen, dass die Revision die Überwachung ganz allgemein stark ausweitet. Dies ist mit der durch den Gesetzgeber im BÜPF festgelegten, fein austarierten Interessenabwägung zwischen Freiheit und Privatsphäre der Einwohner der Schweiz einerseits und Sicherheit durch Überwachungsmassnahmen andererseits absolut nicht vereinbar. Die Revision entpuppt sich geradezu als eine Art Wunschkonzert für Überwachungsbehörden. Insbesondere ist künftig auch eine **komplette inhaltliche Überwachung des gesamten Internetverkehrs** der Schweiz vorgesehen. Dies ohne dass eine solche inhaltliche Überwachung durch die gesetzlichen Grundlagen des BÜPF in irgendeiner Weise gedeckt wäre: Zulässig ist gemäss BÜPF einzig und allein die Überwachung von Randdaten des Fernmeldeverkehrs, und selbst die Zulässigkeit der in diesem Kontext angewendeten anlasslosen Vorratsdatenspeicherung von Randdaten ist bis heute umstritten und Gegenstand von Gerichtsverfahren, ja in der EU bereits höchstrichterlich als menschenrechtswidrig erkannt. Die durch die Verordnungsrevision eingeführte Inhaltsüberwachung ist in der Schweiz damit erst recht **offensichtlich illegal und verfassungswidrig**.

Abschliessend sei noch der Hinweis angebracht, dass wir die Gesetzgebungstechnik des Entwurfs für überaus schlecht halten. **Sowohl der Verordnungstext als auch der zugehörige erläuternde Bericht sind über weite Strecken höchst verwirrend und unverständlich formuliert**, unter anderem mit einer Vielzahl von Querverweisen, technischen Fehlern und unklarer Begrifflichkeit (für ein Beispiel hierfür siehe unten, Bemerkungen zu Art. 43a). Die Texte sind in dieser Form selbst für Fachleute über weite Strecken nicht zu verstehen, geschweige denn als Ganzes zu überblicken. Für KMU, die durch die Revision neu mit erheblich strengerem Pflichten konfrontiert werden, ist eine rechtskonforme Umsetzung dieser Vorlage daher ein schlicht aussichtsloses Unterfangen.

Das Legalitätsprinzip gemäss Art. 5 Bundesverfassung fordert vom Gesetzgeber, dass Gesetzesstexte für die Adressaten verständlich formuliert sind. Die Texte der Verordnungsrevision genügen dieser Anforderung offensichtlich in keiner Weise. Nur schon aufgrund der völlig fehlenden Verständlichkeit ist die Verfassungsmässigkeit der Revision insgesamt höchst zweifelhaft. Wir fordern nur schon deshalb einen Rückzug der vorgelegten Texte, eine komplette Überarbeitung zur Verbesserung der Verständlichkeit und eine erneute Auflage zur Vernehmlassung.

Mit freundlichen Grüßen

Init7 (Schweiz) AG

Alfred Künzler

Bemerkungen zu einzelnen Artikeln der VÜPF

Nr.	Artikel	Antrag	Begründung / Bemerkung
VÜPF / OSCPT / OSCPT			
0.	Alle Artikel	Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.	<p>Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kunden auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.</p> <p>Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.dgl. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.</p>
1.	16b, Abs. 1	<p>Aufhebung der Formulierung von lit. b Ziff. 1 und 2:</p> <p>«Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmelddienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.»</p>	Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile, wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Anforderungen in Kauf nehmen.
2.	16c, Abs. 3	<p>Streichung von lit. a «automatisierte Erteilung der Auskünfte (Art. 18 Abs. 2);»</p>	<p>Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Dies untergräbt rechtsstaatliche Prinzipien doppelt: Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als «natürliche» Schutzmechanismen gegen eine überschiessende, missbräuchliche oder zumindest unverhältnismässige Nutzung solcher Massnahmen durch die Untersuchungsbehörden.</p> <p>Der vorgesehene Umsetzungszeitraum von 12 Monaten für die rechtssichere Implementierung eines derart komplexen Systems völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
3.	Art. 16d	Streichung von Onlinespeicherdiensten und VPN-Anbietern in der Auslegung	<p>Eine klarere Definition des Begriffs AAKD ist begrüssenswert, doch die neue Auslegung gemäss erläuterndem Bericht geht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdiensten wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter, etc.) genutzt werden.</p> <p>Art. 2 lit. c BüPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug den gesetzlichen Rahmen sprengt. Onlinespeicherdienste sind deshalb aus Art. 16d zu streichen.</p> <p>Zudem anerkennt der erläuternde Bericht, dass VPNs zur Anonymisierung der Nutzer*innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Anbieter von VPNs sind daher ebenfalls aus dem Geltungsbereich von Art. 16d auszunehmen.</p>
4.	Art. 16e, Art. 16f und Art. 16g	<p>Streichung der Artikel und Beibehaltung der bestehenden Kriterien</p> <p>Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).</p>	<p>Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch diametral entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung. Dies daher, weil neu KMU bereits mit mehr als 5'000 Nutzern erfasst werden.</p> <p>Die Einführung von 5000 Nutzern als gesondert zu beurteilende Untergrenze verletzt aus unserer Sicht bereits Art. 27 Abs. 3 BüPF, denn 5000 Personen keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strenger Überwachungsmassnahmen, gerechtfertigt wären. 5000 Nutzer werden in der digitalen Welt vielmehr sehr rasch erreicht.</p> <p>Zusätzlich führt das Einführen eines «Konzernatbestandes» in Art. 16f Abs. 3 zu massiven Problemen, da die Produkte nun nicht mehr für sich alleine eine bestimmte Grösse erreichen müssen, sondern die relevanten Zahlen anhand des Umsatzes des Unternehmens, bzw. in Konzernverhältnissen sogar des Konzerns bestimmt werden. Vor allem bei Unternehmen mit Beteiligungsfirmen im Hintergrund fallen nun neu alle Dienstleistungen und Produkte automatisch unter die härteste Stufe, egal ob sie sich erst in einem frühen Entwicklungsstadium befinden. Dies behindert Innovation, da jedes Projekt bereits mit volumänglichen Überwachungspflichten geplant und eingeführt werden müsste. Durch diese extreme Einstiegshürde wird der Innovationsstandort Schweiz nachhaltig geschädigt.</p> <p>Gleichzeitig wird auch der Wirkungsbereich der VÜPF stark erweitert. Während heute ein Unternehmen einen grosse[n] Teil seiner Geschäftstätigkeit durch abgeleitete Kommunikationsdienste erbringen muss (Art. 22 Abs. 1 lit. b und Art. 52 Abs. 1 lit. b</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>VÜPF), fällt dieses Kriterium neu weg. Dadurch können künftig auch Unternehmen, deren Geschäftstätigkeit nur am Rande auf abgeleiteten Kommunikationsdiensten basiert, wie Onlineshops, Marktplätze, Auktionsplattformen, Zeitungen, Computerspielhersteller und zahlreiche weitere Unternehmen, unter die VÜPF fallen – allein deshalb, weil ihre Produkte irgendeine Form privater Kommunikation zwischen Nutzer*innen und/oder Drittanbietern ermöglichen.</p> <p>Die vorgeschlagene Regelung stünde sodann im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali, das die zu weite Betroffenheit und die seltene Anwendung von Downgrades kritisierte: «Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»</p> <p>Statt KMU zu entlasten, führt die Revision neu sogar zu einer «automatischen Hochstufung per Verordnung ohne konkretisierende Verfügung (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.</p> <p>Die neue Regelung steht zudem in offensichtlichem Widerspruch zur bisherigen Praxis, denn bis heute wurde gemäss Angaben des Dienst-ÜPF keine einzige AAKD hochgestuft. Auch der Bundesrat stützte sich ausdrücklich auf die geltende Kombination von drei Schranken – einem Unternehmensfokus auf Kommunikationsdienste, einer Umsatzgrenze von 100 Millionen Franken sowie einer grossen Nutzerzahl – als er noch 2023 begründete, die Umsetzung des BÜPF sei gerade wegen der genannten Schranken als KMU-freundlich zu verstehen. Die vorliegende Revision hebt jedoch genau diese Kombination kumulativer Kriterien auf und will die einzelnen Kriterien künftig alternativ anwenden bzw. streicht sie sogar vollständig. Dadurch verlieren die bisherigen Schutzmechanismen ihre Wirkung, und das BÜPF soll neu auf viele KMU Anwendung finden, die früher nicht unter Gesetz und Verordnung fielen.</p> <p>Die Analyse der offiziellen Statistik des Dienstes ÜPF macht die offensichtliche Unverhältnismässigkeit dieses Ansinnens deutlich. Im Jahr 2023 betrafen 98,95 % der total 9430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,05 % für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,73 % wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100 % des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.</p> <p>Wesentlich ist insbesondere eine neue Pflicht zur Identifikation der Nutzer: Hiervon betroffen sind nicht nur alle AAKD mit</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>reduzierten oder vollen Pflichten (und damit de facto fast alle AAKD der Schweiz), sondern auch all deren Wiederverkäufer. Im Ergebnis führt die neue Verordnung aus unserer Sicht dazu, dass man sich bei keinem marktrelevanten Dienst mehr anmelden kann, ohne den Pass, Führerschein oder ID zu hinterlegen oder zumindest Daten wie eine Telefonnummer anzugeben, die man ohne Pass oder ID nicht erhalten kann.</p> <p>Die automatische Hochstufung an sich führt bereits zu erheblicher Rechtsunsicherheit bei den betroffenen Unternehmen. Unter dem bestehenden System werden die generell-abstrakten Normen der VÜPF mittels Verfügung auf einen konkreten Einzelfall angewendet. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes ist aber im Zweifelsfall möglicherweise nur schwer zu beantworten. Zweifelsohne besteht hier ein schutzwürdiges Interesse seitens der AAKD daran, zu wissen, ob sie die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Nur das bisherige System entspricht den allgemeinen Grundsätzen des Verwaltungsverfahrens, welches für die Anwendung einer generell-abstrakten Norm eine Konkretisierung durch die Verwaltung voraussetzt. Von einer automatischen Hochstufung von AAKD ist daher aus Gründen der Rechtssicherheit abzusehen. Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.</p> <p>Gegenüber der alten VÜPF erweitert die Revision die Pflichten zur Automatisierung sodann noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragen wie z.B. IR_59 und IR_60, welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen. Genau diese Möglichkeit einer manuellen Intervention ist aber für die Provider kritisch, um Missbräuche zu verhindern, die wiederum die Verträge mit ihren Kunden und das Fernmeldegeheimnis verletzen könnten. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente damit erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.</p> <p>Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 Bst. b der alten VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grosse[n] Teil ihrer Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten.</p> <p>Damit fallen insbesondere bereits Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz. Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Dies setzt der Innovation in der Schweiz neue riesige Hürden entgegen.</p> <p>Auch Non-Profit-Organisationen wie die Signal Foundation, die kaum Umsätze erwirtschaften, geraten unter diese verschärften Vorgaben. Während sie bisher unter Duldungspflichten verbleiben konnten, solange sie Art. 22 Abs. 1 VÜPF nicht erfüllten, wird neu allein auf die Anzahl der Nutzer*innen abgestellt, womit z.B. Signal neu als AAKD mit vollen Pflichten erfasst würde. Dies würde dazu führen, dass Signal in der Schweiz entweder zu einem Rückzug aus dem Markt gezwungen wird oder erhebliche rechtliche Konsequenzen riskiert, da Signal keine IP-Adressen speichert und somit gegen Art. 19 RevVÜPF verstößt.</p> <p>Die Regelung ignoriert zudem wirtschaftliche Realitäten: Ein hoher Nutzerkreis bedeutet bei Non-Profits keine finanzielle Tragfähigkeit für umfangreiche Überwachungsmassnahmen. Damit werden Open-Source- und Non-Profit-Lösungen gezielt aus dem Markt gedrängt, während bestehende Monopole wie WhatsApp (96 % Marktanteil in der Schweiz) gestärkt werden. Die neue Regelung ist daher aus ökonomischer Sicht zu verwerfen. Das Kriterium der reinen Nutzerzahl ist ungeeignet und muss gestrichen werden.</p> <p>Nicht zuletzt schwächt die Regelung auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger*innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, Ende-zu-Ende-verschlüsselter Kommunikation ist heute wichtiger denn je.</p> <p>Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade als rechtswidrig gilt (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer*innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, sondern allein diese Anhäufung an Daten malt eine Zielscheibe auf den Rücken von Schweizer Unternehmen und Dienstleistungen für Hackerangriffe aus der ganzen Welt.</p> <p>Weiters ist zu erwähnen, dass es gar nicht erwiesen ist, dass die Speicherung der fraglichen Daten eine merklich höhere Quote erfolgreicher Ermittlungen durch die Strafverfolgungsbehörden mit sich bringen würde. Im Gegenteil müssen die bereits existierenden Sekundärdaten, die allein durch die Bereitstellung eines Dienstes für den Nutzer entstehen, besser genutzt werden.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisbrauch via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen verfügt, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden. Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren.</p> <p>Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Souveränität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.</p> <p>Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das Datenschutzgesetz. Der Entwurf bringt nicht, wie der Begleitbericht dem Leser in geradezu in Orwell'scher Manier weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit und steht in direktem Gegensatz zum besagten Postulat 19.4031.</p> <p>Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen, und das bestehende System muss beibehalten werden.</p>
5.	Art. 16h Abs. 2	Streichung der Ausführung im erläuternden Bericht und ein Abstellen der Formulierung auf die gleichzeitige Anzahl Nutzer.	<p>Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Nutzer*innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 RevVÜPF, gemäss dem die das WLAN erschliessenden FDA die Verantwortung für die Identifikation der Nutzer der WLANs tragen.</p> <p>Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer*innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24) oder die Aggregation von IP-Adressbereichen</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>(z.B. 192.168.0.0/22). Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDAs unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden. Unter der bestehenden Regelung konnte eine FDA anhand der Lokation (z.B. Bibliothek, Flughafen) eine Einschätzung treffen. Die neue Definition hingegen würde von ihr verlangen, Zugriff auf jedes private Netzwerk zu erhalten, um Hardware und Einstellungen zu prüfen – ein offensichtlich verfassungswidriges und auch praktisch unmögliches Unterfangen. Diese vage Formulierung führt zu anhaltender Rechtsunsicherheit für FDA.</p> <p>Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten.</p> <p>Zudem könnte Art. 16h dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist*innen, Whistleblower*innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer*innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen. Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt.</p>
	Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2	Streichung des «Konzerntatbestand» und Beibehaltung der bestehenden Regelung	<p>Die Verordnung nimmt neu nicht mehr die Umsatz- und Nutzerzahlen der betroffenen Unternehmen, sondern die Zahlen des jeweiligen Konzerns als Basis für Up- und Downgrades. Die Begründung zur Einführung dieses «Konzerntatbestands», wonach die neue Regelung für die betroffenen Unternehmen zu einer Vereinfachung führe, ist kontraintuitiv, ja offensichtlich falsch und irreführend. In der Praxis sind die betroffenen Unternehmen nämlich schon heute verpflichtet, ihre Buchhaltung nach Produkten aufzugliedern. Somit können die Kennzahlen bereits heute sehr einfach festgestellt werden. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.</p>
6.	Art. 19 Abs. 1	Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation von Teilnehmenden.	<p>Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht.</p> <p>Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des Schweizer Datenschutzgesetzes, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch der Schutz der Schweizer Kundschaft massiv beeinträchtigt wird. Datenschutzfreundliche Unternehmen werden bestraft, da ihr Geschäftsmodell</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.</p> <p>Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Dies wahrt nicht nur den Datenschutz, sondern schützt auch die Wettbewerbsfähigkeit von KMU, stärkt den Innovationsstandort Schweiz und die digitale Souveränität unseres Landes.</p>
7.	Art. 18	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.
8.	Art. 19 Abs. 2	Ersatzlose Streichung zugunsten bestehender Regelung	Eine Überwachung von Kunden durch FDA, ob diese die neuen Vorgaben der VÜPF zu WLANs einhalten (Art. 19 Abs. 2 RevVÜPF), und erst recht die dazu gelieferte Erklärung im erläuternden Bericht, wonach die FDA die Identifikation der WLAN-Nutzer vorzunehmen hätten, ist weder gesetzeskonform noch zumutbar (siehe vorstehend). Art. 19 Abs. 2 ist ersatzlos zu streichen.
9.	Art. 21 Abs. 1 lit. a	Streichung	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.
10.	Art. 22	beibehalten	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.
11.	Art. 11 Abs. 4	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.
12.	Art. 16b	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.
13.	Art. 31 Abs. 1	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.
14.	Art. 51 und 52	beibehalten	Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.
15.	Art. 60a	Streichung des Artikels	<p>Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen.</p> <p>Art. 60a VÜPF (Erläuterung Bundesrat: «...lediglich redaktionelle Änderungen....») sieht vor, dass Fernmeldedienstanbieterinnen über einen rückwirkenden Zeitraum von 6 Monaten alle Ziel-IP-Adressen liefern müssen, welche ihre Kunden besucht haben. Damit wird einerseits das Surfverhalten der gesamten schweizerischen Bevölkerung anlasslos und völlig unverhältnismässig ausspioniert. Andererseits wird die klare Vorgabe des BÜPF umgangen, das nur die Speicherung von</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Randdaten, aber nicht die Speicherung von Inhaltsdaten vorsieht.</p> <p>Die geplante Überwachung des Internetverkehrs führt zu einer Überwachung, wer im Internet welche Adressen besucht hat. Dies geht zweifellos über die Schranken der gesetzlichen Regelung hinaus, dies insbesondere nachdem bereits die Aufzeichnung reiner Randdaten höchst umstritten und Gegenstand laufender Gerichtsverfahren ist. Hinzu kommt folgendes: Während bislang die Überwachung einer IP-Adresse nur im Rahmen einer sog. Echtzeit-Überwachung zulässig war, welche entsprechende Bewilligungen durch ein Gericht erforderte, muss neu nur noch ein einfaches Auskunfts-begehrten durch die zuständige Behörde genehmigt werden. Die Abfragen erfolgen automatisiert.</p> <p>Art. 60a sieht weiter vor, dass bei nicht exakt zuordnbaren IP-Adressen die kompletten Listen aller Nutzerinnen und Nutzer zu liefern ist. IP-Adressen sind ein rares Gut. Alle FDA teilen diese den Nutzenden im Millisekunden-Takt zu. Da die Zeitstempel der Systemanbieter nicht immer übereinstimmen, sind diese IP-Adressen nicht immer eindeutig einem Nutzenden zuzuordnen. Neu müssen Provider nun komplettte Listen aller Nutzenden liefern. Dies bringt Zehntausende in den Fokus von Überwachungsbehörden, was auf eine Art Rasterfahndung nach Delikten über grosse Teile der Bevölkerung hinausläuft. Entdecken Strafverfolger dabei zufälligerweise etwas, können sie umgehend Strafverfahren einleiten.</p> <p>Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde sodann gemäss Bericht gezielt auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten.</p> <p>Art. 60a ist zu streichen.</p>
16.	Art. 42a und Art. 43a	Streichung des Artikels	<p>Sowohl Art. 42a als auch Art. 43a fordern die Abrufbarkeit des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Nicht nur gilt auch hier wieder die Limite von 5'000 Nutzern, was somit fast die gesamte AAKD-Landschaft der Schweiz flächendeckend umfasst, sondern solche Abfragen sollen nun auch durch eine einfach «IR_» Abfrage gemacht werden können, welche im Gegensatz zu den «HD_»-Abfragen und den «RT_»-Überwachungen ohne weitere juristische Aufsicht automatisiert abgerufen werden können, obwohl es sich auch hier um das Abrufen einer IP-Adresse in der Vergangenheit handelt, genau wie bei den «HD_» abfragen, welche deutlich strenger reglementiert sind. Es ist nicht nachvollziehbar und verletzt aus unserer Sicht die gesetzliche Grundlage des BÜPF, dass Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber.</p> <p>Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser Automatisierten Auskünfte ergibt. Durch das Fehlen solcher Limiten könnte daher z.B. alle 5 Minuten eine solche Anfrage automatisiert gestellt werden.</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Zunächst können sich dadurch lähmende Kosten für die betroffenen AAKD ergeben. Sodann können die Anfragen an ein automatisiertes Auskunftssystem gestellt werden, und es können auf diese Weise viele der Informationen welche ursprünglich über die juristisch sichereren HD_ und RT_Auskunfts-/Überwachungstypen liegen, neu über den rechtlich unsicheren IR_-Typ eingeholt werden. IR_59 und IR_60 ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne dass sie den benötigten Kontrollen dieser invasiven Überwachungsarten unterliegen würden.</p> <p>Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind, wie dies das BÜPF vorsieht.</p> <p>Die beiden Artikel sind daher vollumfänglich zu streichen.</p> <p>Diese neue Regelung und der zugehörige erläuternde Bericht sind im Übrigen eklatante Beispiele für die eingangs bemängelte überaus verwirrende und unverständliche Darstellung von Verordnungstext und erläuterndem Bericht.</p> <p>Im erläuternden Bericht steht auf S. 39 wörtlich:</p> <p><i>«In Absatz 1 sind die zu liefernden Angaben geregelt. Gemäss Buchstabe a ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin der oder dem Teilnehmenden einen solchen zugeteilt hat. Der «eindeutige Dienstidentifikator» gemäss Buchstabe b bezeichnet den Fernmelde- oder abgeleiteten Kommunikationsdienst, auf den sich die Antwort bezieht, eindeutig im Bereich der Anbieterin. In Buchstabe c werden die zu liefernden Angaben über den Ursprung der Verbindung bei der letzten zugriffsrelevanten Aktivität aufgezählt. Diese Angaben können für die Identifikation der Benutzerinnen und Benutzer nützlich sein.»</i></p> <p>Der Leser bzw. die Leserin urteile selber über die Verständlichkeit.</p> <p>Folgende Begriffe sind auch für den fachkundigen Leser nicht nachvollziehbar, bzw. es stellen sich folgende Verständnisfragen:</p> <ul style="list-style-type: none"> • Eindeutiger Identifikator: Was ist gemeint? Ist die Kundennummer des Internetproviders gemeint? Oder jene des genutzten dritten Fernmeldedienstes oder abgeleiteten Kommunikationsdienstes? Wie soll der Internetprovider überhaupt an diese Daten herankommen? • Eindeutiger Dienstidentifikator: Muss der Internetprovider eine Liste aller möglichen durch seine Kunden im Internet genutzten Kommunikationsdienste führen und aufzeichnen, muss er zudem aufzeichnen welcher Kunde welchen Dienst wann genau genutzt hat? Woher hat er diese Liste? Wie kann er herausfinden, ob ein Kunde gerade einen bestimmten Dienst nutzt? Gilt

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>dies auch für ausländische Dienste? Nur für AAKD, für ausländische Fernmeldedienste, oder für alle Internetangebote weltweit? Der erläuternde Bericht bleibt hier völlig unklar.</p> <ul style="list-style-type: none"> • Was ist mit «Antwort» gemeint? Die Antwort des Servers des abgeleiteten Kommunikationsdienstes, den der Kunde besucht hat, oder die Antwort des Kundengeräts auf eine Nachricht von diesem Kommunikationsdienst? • Was ist mit «eindeutig im Bereich der Anbieterin» gemeint? Die Formulierung ist auch hier unverständlich. • Wie soll man sich eine «Antwort von einem anderen Fernmeldedienst» vorstellen? Muss ein Internetprovider die Herkunft sämtlicher auf seinem Netz eintreffenden Datenpakete aufzeichnen und dem Dienst ÜPF auf Anfrage diese Aufzeichnungen herausgeben? Wie soll die gigantische Masse an Daten, die durch ein solches Logging anfällt, durch die Internetprovider gemanaged werden? • Was ist mit «letzter zugriffsrelevanter Aktivitäten» gemeint? Geht es hier um die durch Kunden des Internetproviders aufgerufenen AAKD und andere Internetangebote? Wie soll der Internetprovider wissen, ob eine durch den Kunden aufgerufene IP-Adresse zu einem überwachungspflichtigen AAKD gehört, oder allenfalls zu einem nicht überwachungspflichtigen Dienst? Muss er einfach den ganzen Verkehr aufzeichnen? Wie weit zurück gehen die «zugriffsrelevanten» Aktivitäten? Müssen alle Daten für sechs Monate aufbewahrt werden? • Abgesehen davon: Wo wäre die gesetzliche Grundlage im BÜPF für die vorgesehene inhaltliche Überwachung des Internetverkehrs? Das BÜPF selber regelt bisher ausschliesslich die Überwachung der Randdaten, nicht aber von Inhaltsdaten, und spätestens dann, wenn Randdaten en passant auch Auskunft über die vom Kunden abgerufenen Inhalte geben, handelt es sich dabei um Inhaltsdaten, deren Sammlung erst recht gesetzes- und verfassungswidrig wäre, nachdem schon das Sammeln reiner Randdaten als menschenrechtswidrig taxiert wurde.
17.	50a	Artikel streichen	<p>Art. 50a sieht neu vor, dass Anbieter verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Diese Pflicht gilt nicht mehr nur für FDA (Art. 26 BÜPF) oder ausnahmsweise für ausgewählte AAKD von hoher wirtschaftlicher Bedeutung (Art. 27 BÜPF), sondern soll nun vorgabemässig und ohne Differenzierung auf sämtliche Anbieter mit mehr als 5'000 Teilnehmern angewendet werden, womit wohl fast die gesamte Schweizer AAKD-Branche betroffen ist (kaum ein Produkt ist lebensfähig mit weniger als 5000 Teilnehmern).</p> <p>Dies stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar.</p> <p>Diese Ausweitung ist nicht nur unverhältnismässig, sondern</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>gefährdet aktiv nahezu die gesamte Schweizer IT-Branche: Indem de facto alle Anbieter vorgabemässig gezwungen werden, ihre Verschlüsselungssysteme für Behörden jederzeit entschlüsselbar zu gestalten, entstehen enorme Sicherheitsrisiken, denn Verschlüsselung ist wie eine Eierschale: Unversehrt ist sie stark, aber der kleinste Riss führt zu einer erheblichen Schwächung. Die betroffenen Systeme werden durch den vom Verordnungsgeber nun verpflichtend vorgesehenen Einbau von Hintertüren anfälliger für Hackerangriffe, Datenmissbrauch und Spionage. Dies widerspricht Art. 13 BV und dem diesen konkretisierenden Datenschutzgesetz, das den Schutz personenbezogener Daten ausdrücklich durch wirksame technische Massnahmen – insbesondere Verschlüsselung – vorschreibt. Eine durch den Anbieter aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung in jedem Fall.</p> <p>Genau eine solche Schwächung der Verschlüsselung wurde kürzlich vom Europäischen Gerichtshof für Menschenrechte im Fall PODCHASOV gegen Russland (33696/19) als Verstoss gegen Grundrechte gewertet. Art. 50a verstösst somit auch gegen geltendes Völkerrecht.</p> <p>Nebst diesem Verstoss gegen das Völkerrecht wird aber auch das Gebot der Verhältnismässigkeit aus Art. 36 BV nicht eingehalten, weil das Resultat – die Schwächung der Verschlüsselung des bei-nahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Wie bereits bei Art. 16e, Art. 16f und Art. 16g erwähnt, müssen zuerst die einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.</p> <p>Zusätzlich, und wie bereits bei Art. 16d erwähnt, verhindert Art. 50a die effektive Erbringung von VPN-Diensten. Bei solch einem VPN kontrolliert der Betreiber sowohl den Eingangs- als auch den Endpunkt. Da die Kommunikation vom Endpunkt zu einer Webseite aufgrund der vorherrschenden Struktur im allgemeinen Internet nicht End-zu-End-Verschlüsselt erfolgen kann, werden schon kleine VPNs (mit 5000 Nutzern) dazu gezwungen ihre eigene Verschlüsselung zu entfernen und ihre Kun-den zu überwachen. Da der Schutz der Privatsphäre der Nutzer*innen von VPNs just den Kernpunkt oder USP der Dienstleistung darstellt, werden Schweizer VPN-Anbieterinnen hierdurch am internationalen Markt übermässig benachteiligt, ja ihres eigentlichen Daseinszwecks beraubt.</p> <p>Wesentlich ist zudem, dass Anbieter von Mail- oder Messaging-Apps zwangsläufig die Nachricht in der App in einer menschenlesbaren Version anzeigen muss, und dass an dieser Stelle die End-zu-End-Verschlüsselung notwendigerweise bereits entfernt ist. Der Wortlaut von Art. 50a lässt entgegen sämtlichen Beteuerungen des Dienstes ÜPF bereits anlässlich der letzten Revision der VÜPF weiterhin offen, ob eine Entfernung der Verschlüsselung auch an dieser Stelle gefordert werden können soll. Angesichts der seit Jahren erkennbaren Tendenz der</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			Schweizer Überwachungsbehörden, die Anwendbarkeit des Überwachungsrechts laufend weiter auszudehnen und sich dabei nur durch Gerichte bremsen zu lassen, ist bei dieser Gelegenheit erneut die Klarstellung zu fordern, wonach die Entfernung von Verschlüsselungen, die erst in der Sphäre des Benutzers angebracht werden (wenn-gleich auch durch Software der Anbieterin) nicht verlangt werden darf. Dies ist zumindest im erläuternden Bericht zu erwähnen. Der erneute Verzicht wäre nichts anderes als eine Einladung an die Überwachungsbehörden, die Einführung einer offensichtlich illegalen und vom BÜPF keineswegs vorgesehenen «Chatkontrolle» auf dem «Auslegungsweg» vorzunehmen.

Bemerkungen zu einzelnen Artikeln der VÜPF

Artikel	Antrag	Begründung / Bemerkung
VD-ÜPF / OME-SCPT / OE-SCPT		
Art. 14 Abs. 3 VD-ÜPF	Streichung	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit 5000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Absatz ist daher ersatzlos zu streichen.
Art. 14 Abs. 4 VD-ÜPF	Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten.»	Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der Unterworfenen AAKD massiv. Dies ist wie beschrieben weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.
Art. 20 Abs. 1 VD-ÜPF	Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.

Stefan Thöni, Parkstrasse 7, 6312 Steinhausen

Eidgenössisches Justiz-
und Polizeidepartement
Bundeshaus West
3003 Bern

5. Mai 2025

Vernehmlassung zu den Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit, unsere Vernehmlassungsantwort zu den Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs einreichen zu dürfen.

Generelles

Wir lehnen die geplante Ausweitung der Überwachungspflichten für Anbieter abgeleiteter Kommunikationsdienste ab. Damit soll offensichtlich das Threema-Urteil des Bundesgerichts umgeworfen und Messengerdiensten zusätzliche Überwachungspflichten aufgelegt werden.

Wir fordern insbesondere, dass vor den geplanten Teilrevisionen eine Überwachungsgesamtrechnung angestellt wird, die aufzeigt, wo und wie Menschen in der Schweiz genau überwacht werden oder überwacht werden können, und welche Freiräume noch bestehen.

Die Überwachung der Internetkommunikation ist bereits heute ausufernd und schränkt die Freiheit zahlloser unbescholtener Menschen unverhältnismässig ein. Gerade im Hinblick auf den weltweiten Vormarsch des Faschismus muss die Internetüberwachung jetzt reduziert werden, bevor die auf Vorrat gespeicherten Überwachungsdaten von einem au-

toritären Regime dafür missbraucht werden, Menschen grundlos in Gulags zu deportieren.

Einzelkommentare

Art. 12 VÜPF

In Absatz 2 sollten zusätzlich die Anzahl der betroffenen Menschen, der Umfang der überwachten Gespräche und Daten in die Statistik aufgenommen werden.

Art. 13 VÜPF

In Absatz 1 sollte zusätzlich die Anzahl der betroffenen Menschen in die Statistik aufgenommen werden.

Absatz 3 sollte dahingehend geändert werden, dass eine Aufschlüsselung je Kanton erfolgt.

Art. 16a VE-VÜPF

In Absatz 2 sollten neben Unternehmen und Konzernen auch Vereine und Verbände aufgenommen werden, welche interne Fernmelde- oder abgeleitete Kommunikationsdienste betreiben. Dabei geht es vornehmlich um abgeleitete Kommunikationsdienste via den Verweis aus Art. 16d Abs. 2 VE-VÜPF.

Falls nicht alle Vereine und Verbände von Überwachungspflichten befreit werden, so müssen zum Schutz der Demokratie doch zumindest die politischen Akteure, namentlich politische Parteien und Organisationen der Zivilgesellschaft ausgenommen werden (Siehe Art. 5 Abs. 5 NDG).

Art. 16b VE-VÜPF

Bei Absatz 1 Buchstabe b sollten keine Kenngrößen verwendet werden, die von Entscheidungen der überwachenden Behörden abhängen, sondern nur solche, welche die Anbieterin durch ihr Geschäftsgebaren selbst bestimmen kann, wie z.B. die Anzahl Kunden oder Teilnehmerinnen. Nur so kann verhindert werden, dass die Anbieterin plötzlich ohne ihr Zutun nicht mehr FDA mit reduzierten Pflichten ist.

Art. 16h VE-VÜPF

Bei Absatz 2 sollte deutlich gemacht werden, dass die Anzahl Endbenutzer*innen gemeint ist, welche den WLAN-Zugang gleichzeitig nutzen können (Kapazität) und nicht etwa die über einen längeren Zeitraum kumuliert möglichen Endbenutzer*innen. Letztere könnte eine nicht professionelle Betreiber*in gar nicht wissen oder limitieren, da sie gerade nicht verpflichtet ist, die Endbenutzer*innen zu identifizieren.

Art. 50a VE-VÜPF

Das Entfernen der von Anbieter*innen angebrachten Verschlüsselung ist bei Anwendung von asymmetrischer Verschlüsselung mit einem öffentlichen Schlüssel (engl. Public Key) des Nutzers nicht möglich.

Daher kann dieser Artikel dahingehend verstanden werden, dass asymmetrische Verschlüsselung durch Anbieter*innen verboten wird oder Inhaltsdaten der Vorratsdatenspeicherung unterworfen werden, was den Zweck der asymmetrischen Verschlüsselung untergraben würde.

Der Artikel muss daher dahingehend geändert werden, dass Verschlüsselung nur dann durch die Anbieter*in entfernt werden muss, wenn sie ohnehin über den Schlüssel verfügt.

Freundliche Grüsse

Stefan Thöni

Monsieur le Conseiller fédéral
Jans Beat
Chef du Département fédéral de justice et
police (DFJP)
Palais fédéral ouest
3003 Berne

Lausanne, le 6 mai 2025

RÉVISION PARTIELLE DE DEUX ORDONNANCES D'EXÉCUTION DE LA SURVEILLANCE DE LA CORRESPONDANCE PAR POSTE ET TÉLÉCOMMUNICATION (OSCPT ET OME-SCPT)

Monsieur le Conseiller fédéral,

La Chambre vaudoise du commerce et de l'industrie (CVCI) a pris note de la consultation relative à la révision partielle de deux ordonnances d'exécution de la surveillance de la correspondance par poste et télécommunication (OSCPT et OME-SCPT).

La CVCI est préoccupée par le fait que les propositions visant à étendre massivement la surveillance étatique tout en réduisant le contrôle judiciaire menacent les droits fondamentaux des citoyens suisses ainsi que ceux de nos clients à l'échelle internationale.

La CVCI constate que le nombre d'entreprises et de services concernés par les différentes obligations est extrêmement important et fait craindre la mise en œuvre d'un système s'apparentant à une surveillance généralisée en Suisse. Parmi ces dernières, de nombreuses voix s'élèvent contre cette réforme, comme Protonmail et Threema qui estiment que cette révision va trop loin. Ces entreprises soulignent que pour livrer des données automatiquement, le cryptage des métadonnées doit être supprimé, ce qui prétérira encore plus leur confidentialité. Ces dernières années, la Suisse et le Canton de Vaud se sont engagés fortement pour le développement d'un territoire de la confiance numérique via des initiatives comme la Trust Valley et nous estimons que cette révision vient mettre en difficulté cet écosystème en pleine croissance. La proposition est rédigée en des termes si généraux qu'elle pourrait s'appliquer à pratiquement toutes les entreprises technologiques suisses et risquer de nuire à la compétitivité du secteur technologique suisse à un moment où celui-ci connaît une opportunité de croissance sans précédent en Europe.

La Suisse s'est forgée au cours d'un siècle une réputation mondiale en matière de stabilité, de protection de la sphère privée et de sécurité. Cela a grandement profité à de nombreux secteurs de l'économie suisse au cours du siècle dernier et continue d'être l'un des principaux avantages concurrentiels de la Suisse. Dans ce contexte, il est pour le moins étonnant qu'une ordonnance d'exécution outrepasse le silence de la loi. Cette automatisation de l'accès à nos données, qui paraît explicitement dans la dernière révision de l'OSCPT, soulève des interrogations quant à la protection de la sphère privée.

Nous estimons que certaines propositions, telles que la conservation obligatoire des métadonnées appliquée de manière générale, éloignent la Suisse des normes européennes au risque de nuire de manière permanente à la réputation de la Suisse en matière de confiance, de sécurité et de protection de la vie privée, au détriment d'un large éventail d'industries actuelles et futures.

En conséquence, la CVCI demande le retrait du projet de modification mis en consultation et demande une redéfinition des catégories de fournisseurs concernés, une modification des différentes obligations et appelle à un dialogue avec les milieux concernés dans les meilleurs délais.

En vous remerciant de la suite que vous donnerez à la présente, je vous prie de croire, Monsieur le Conseiller fédéral, à l'expression de mes salutations respectueuses.

Chambre vaudoise du commerce et de l'industrie



Romaine Nidegger

Responsable du service politique



Julien Guex

Responsable Innovation

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Herrn Bundesrat Beat Jans
Bundeshaus West
3003 Bern

Colt Technology Services AG
Bahnhofplatz 1
8001 Zürich

Christian Weber
Tel: + 49 (0) 69 / 5 66 06 - 6591
Fax: + 49 (0) 69 / 5 66 06 - 1200
E-Mail: christian.weber@colt.net

www.colt.net

Frankfurt, 06.05.2025

Nur per e-mail: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Vernehmlassung betreffend die Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF);

Stellungnahme der Colt Technology Services AG

Sehr geehrter Herr Bundesrat,
Sehr geehrte Damen und Herren,

die Colt Technology Services AG (*im folgenden „Colt“*) ist eine Anbieterin von Fernmeldediensten („FDA“) im Sinne der Art. 4 FMG sowie Art. 2 Bst. b BÜPF und seit 1997 in der Schweiz vertreten. Colt ist Teil der international operierenden Colt Technology Services Limited. Zunächst als klassisches Telekommunikationsunternehmen im Vereinigten Königreich gegründet, bietet unser Unternehmen aktuell Netzwerk- und Telefonieservices ausschliesslich für Geschäftskunden in einer Vielzahl von Ländern an, in der Schweiz mit einem Schwerpunkt in den Branchen Banken und Versicherungen sowie Pharmazie und Chemie.

Colt ist darüber hinaus Mitglied der asut. Der im Rahmen dieser Vernehmlassung abgegebenen Stellungnahme des Verbandes schliessen wir uns daher vollumfänglich an.

Wir bedanken uns für die Gelegenheit zur Äusserung und möchten eingangs zunächst festhalten, dass wir die derzeit bestehenden Regelungen zur Überwachung des Post- und Fernmeldeverkehrs für geeignet halten, den Verordnungszweck zu erfüllen und das BÜPF in einer Weise zu konkretisieren, dass für die FDA ein höchstmögliche Mass an rechtlicher Sicherheit und Klarheit hinsichtlich ihrer Verpflichtungen erzielt wird. Wesentliche Änderungen halten wir somit weder für geboten noch zumutbar.

Im einzelnen:

Nicht gerechtfertigte Aufwandssteigerung

Vor allem die Vielzahl der im Entwurf enthaltenen Änderungen, insbesondere die Einführung neuer Überwachungs- und Auskunftstypen, wird in ihrer Kombination zu erheblichem

monetärem und personellem Aufwand bei den FDA führen, der unseres Erachtens im Missverhältnis zu den potentiell zu erzielenden Vorteilen steht.

Unnötige Änderung der Regelung zu den FDA mit reduzierten Überwachungspflichten

Die aktuelle Statistik des Dienstes Überwachung Post- und Fernmeldeverkehr ÜPF zeigt, dass die Gesamtzahl der Überwachungs- und Auskunftsmassnahmen im Jahr 2024 gegenüber dem Vorjahr signifikant angestiegen ist, insbesondere bei (*einfachen und komplexen*) Auskünften. Gleichzeitig ist auffällig, dass lediglich auf die vier grössten Unternehmen der Telekommunikationsbranche nahezu alle Massnahmen entfallen (*Überwachungen: 99%, Auskünfte: 94%*). Aus diesem Grund hat sich der Verordnungsgeber auf Vorbringen der kleineren Telekommunikationsunternehmen vor einigen Jahren dafür entschieden, in Art. 51 VÜPF den Kreis der Mitwirkungspflichtigen zu erweitern und den Typ „*FDA mit reduzierten Überwachungspflichten*“ einzuführen. Diese Regelung hat sich bewährt, und sie trägt dem Kriterium der Verhältnismässigkeit Rechnung, da nur diejenigen FDA vollumfänglich in Anspruch genommen werden, auf die ohnehin das Gros der Massnahmen entfällt.

Durch einige der in Art. 16a und 16b eVÜPF vorgeschlagenen Änderungen ergibt sich zudem ein Widerspruch zu bestehenden bzw. vorrangigen gesetzlichen Regelungen:

- Art. 16a eVÜPF erweitert den Begriff der Anbieterin von Fernmeldediensten ggü. Art. 2 FMG und Art. 3 lit. d FMG anstatt ihn wie geboten zu konkretisieren bzw. zu harmonisieren – dies führt zu grösserer Rechtsunsicherheit.
- Art. 16b Abs. 1 eVÜPF schränkt Art. 51 VÜPF zunächst dahingehend ein, dass statt kumulativen Vorliegens der Voraussetzungen des Abs. 1 lit. b Nr. 1 und 2 VÜPF (*Anzahl Überwachungsaufträge und Zwei-Jahres-Umsatz*) nun die Überschreitung **nur eines** der beiden Schwellwerte ausreicht, um nicht mehr als FDA mit reduzierten Überwachungspflichten eingestuft zu werden. Lautet die bestehende Regelung noch „*Auf Gesuch einer FDA erklärt der Dienst ÜPF diese als FDA mit reduzierten Überwachungspflichten [...], wenn sie beide der nachstehenden Grössen nicht erreicht: [...]*“ soll dafür gem eVÜPF zukünftig genügen, dass die FDA **keine** der nachstehenden Grössen erreicht.
- Eine weitere Verschlechterung stellt die beabsichtigte Änderung der Bezugsgrösse des Jahresumsatzes in Art. 16b Abs. 1 lit. a Nr. 2 eVÜPF dar – indem zukünftig auf den Jahresumsatz des **gesamten** Unternehmens statt auf den Jahresumsatz mit **Fernmeldediensten** und abgeleiteten Kommunikationsdiensten abgestellt werden soll. Zum einen wird hier eine sprachliche Unschärfe erzeugt (*bezeichnet „Unternehmen“ den Gesamtkonzern?*), wodurch der Verordnungsgeber ohne entsprechende Kompetenz potentiell Umsätze ausserhalb seines geographischen Zuständigkeitsbereichs zugrundelegen würde, zum anderen kann der Gesamtumsatz in erheblichem Umfang Anteile aus völlig anderen Geschäftsfeldern enthalten, die sachlich dem Regelungsgegenstand der Verordnung fremd sind.

Auch und vor allem ergibt sich durch die in Art. 16a und 16b eVÜPF vorgeschlagenen Änderungen keine Verbesserung der Strafverfolgung.

Wir halten die vorgeschlagenen Änderungen aus den oben dargestellten Erwägungen heraus für unverhältnismässig.

Wir schlagen daher vor, die bestehende Regelung unverändert beizubehalten, mindestens aber durch entsprechende Anpassung hinsichtlich der vorstehenden Ausführungen zu überarbeiten.

Diese Stellungnahme enthält keine Geschäfts- und Fabrikationsgeheimnisse und kann den übrigen Beteiligten des Vernehmlassungsverfahrens sowie interessierten Dritten ohne Einschränkungen zugänglich gemacht werden.

Wir bedanken uns für eine Berücksichtigung unseres Vorbringens und verbleiben

Mit freundlichen Grüßen
Colt Technology Services AG



i. V. Christian Weber
Rechtsanwalt (Syndikusrechtsanwalt)
Senior Advisor Regulatory Affairs
Central & Eastern Europe

/ Stellungnahme

Vernehmlassung: Verordnungen über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

6. Mai 2025

Sehr geehrter Herr Bundesrat Beat Jans, sehr geehrte Damen und Herren

Wir danken für die Möglichkeit zur Stellungnahme zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF).

AlgorithmWatch CH ist eine gemeinnützige Nichtregierungsorganisation mit Sitz in Zürich. Wir setzen uns dafür ein, dass Algorithmen und Künstliche Intelligenz (KI) Gerechtigkeit, Demokratie, Menschenrechte und Nachhaltigkeit stärken, statt sie zu schwächen.

Gerne nehmen wir zur Teilrevision dieser zweier Ausführungserlasse wie folgt Stellung. Der Verzicht auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Artikeln kann nicht als Zustimmung von AlgorithmWatch CH gewertet werden. Für die Stellungnahme zu einzelnen Artikeln verweisen wir auf die Stellungnahme der Digitalen Gesellschaft.

Allgemeine Anmerkungen

Die geplante Revision der VÜPF ist nicht vereinbar mit unseren Grundrechten, der Rechtsstaatlichkeit sowie dem IT- und Innovationsstandort Schweiz.

Mit ihrer Umsetzung würde geltendes Recht in beträchtlichem Ausmass verletzt: Die Revision ist in vielerlei Hinsicht unvereinbar mit dem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), verstösst gegen das Datenschutzgesetz (DSG), steht in klarem Widerspruch zu den verfassungsmässigen Grundrechten und verstösst gegen Völkerrecht.

Die vorgesehenen Änderungen führen zu einer massiv ausgeweiteten Überwachung – ganz grundsätzlich und flächendeckend. Dies ist mit der Ausrichtung des BÜPF, das eine fein austarierte Interessenabwägung zwischen Freiheit und Privatsphäre einerseits und Sicherheit durch Überwachungsmassnahmen andererseits verfolgt, nicht vereinbar.

Auch die Auswirkungen auf den Wirtschafts- und Innovationsstandort Schweiz wären verheerend: Die Ausweitung der Überwachung und die damit verbundenen, übermässigen Mitwirkungspflichten machen die Schweiz für IT-Anbieter äusserst unattraktiv.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und die Berücksichtigung unserer Anmerkungen.



Dr. Angela Müller

Geschäftsleiterin AlgorithmWatch CH



Dr. Andreas Peya, RA und Syndikus-RA
Leiter Regulierung Zentral- und Osteuropa

Verizon Deutschland GmbH
Rebstöcker Str. 59
D-60326 Frankfurt am Main

T +49 69 97268-6002
E Andreas.Peya@de.verizon.com

6. Mai 2025

Verizon Deutschland GmbH, Rebstöcker Str. 59, D-60326 Frankfurt/M

PER EMAIL: ptss-aemterkonsultationen@isc-ejpd.admin.ch
 Eidgenössisches Justiz- und
 Polizeidepartement EJPD
 Bundeshaus West

CH-3003 Bern

Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Stellungnahme der Verizon Switzerland AG

Sehr geehrter Herr Bundesrat,
sehr geehrte Damen und Herren,

Wir nehmen Bezug auf die am 29. Januar 2025 eröffnete Vernehmlassung zur «Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)» und danken Ihnen für die Einladung zur Stellungnahme.

Für die Verizon Switzerland AG, Förrlibuckstrasse 150, 8005 Zürich, machen wir von der Gelegenheit zur Stellungnahme gerne wie folgt Gebrauch:

Geschäftsfeld der Verizon Switzerland AG

Die Verizon Switzerland AG ist im Unternehmenssegment tätig und betreut multinationale Kunden mit Hauptsitz in der Schweiz, insbesondere im Banken-, Finanz- und Pharmabereich, aber auch bekannte Schweizer Mittelstandskunden in der Industrie. Ebenso zählen in der Schweiz ansässige (Sport-)Verbände und supranationale Organisationen zu unserem Kundenstamm.

Orientiert an der individuellen Nachfrage unserer Kunden liefern wir massgeschneiderte Kommunikationslösungen für die Bedürfnisse dieser Kundengruppen. Anders als im Massenmarkt (der sich überwiegend an Konsumenten richtet) üblich, formulieren unsere Kunden ihren Bedarf an Kommunikationslösungen im Rahmen von Ausschreibungen. Dies beinhaltet Netzwerklösungen inkl. Sprachtelefonie, Cloud-Dienstleistungen und Sicherheitslösungen, die auf die internationalen Ansprüche von multinational tätigen Unternehmen ausgerichtet sind.

Unsere Kunden legen grossen Wert auf eine persönliche Betreuung und eine umfassende Expertise im Bereich der Telekommunikation. Damit stellen wir sicher, dass die Kundschaft optimal von der Digitalisierung profitiert und ihre Geschäftsziele effizient erreicht. Die

Verizon Deutschland GmbH, Sitz der Gesellschaft: Dortmund, Handelsregister: Amtsgericht Dortmund, HRB 14952

Geschäftsführer: Detlef Eppig

USt-Ident-Nr./VAT-ID-No.: DE 814082641

Bankverbindung:

Bank of America, Konto-Nr. 17323012, BLZ 50010900

IBAN: DE15 5001 0900 0017 3230 12, BIC: BOFADEFX



Verbindung von globaler Technologie mit lokaler Präsenz und Verständnis des Schweizer Marktes macht die Verizon Switzerland AG zu einem Anbieter für Unternehmen mit hohen Ansprüchen an eine verlässliche Kommunikationsinfrastruktur. Wir sind seit der Marktoffnung im Schweizer Markt aktiv und Mitglied des Schweizerischen Verbands der Telekommunikation (asut), welcher die Interessen der Telekommunikations-, Netzwerk- und Datacenter-Branche vertritt. Vor diesem Hintergrund haben wir an der asut Stellungnahme mitgewirkt und verweisen inhaltlich voll auf diese.

Aufgrund des besonderen Bedarfs der von uns betreuten Kundengruppe aus dem Unternehmenssegment weisen wir noch einmal gesondert auf folgende Aspekte hin:

Bisherige Regelung erfüllt alle Anforderungen

Der VÜPF Verordnungstext heute in Art. 51 (FDA mit reduzierten Überwachungspflichten) sowie Art. 52 (AAKD mit weitergehenden Überwachungspflichten) stellt eine bewährte und rechtssichere Regelung zur Ermittlung des Umfangs der Pflichten von betroffenen Unternehmen dar. Verizon Switzerland AG hat diese Regelung von Anfang an befürwortet und seinerzeit die Einführung aus gutem Grund unterstützt.

Als Paneuropäisch tätiger Anbieter können wir aus unserer eigenen Erfahrung bestätigen, dass die Schweiz durch diese absolut klare und rechtssichere Regelung bislang europaweit eine Führungsrolle eingenommen hat, was die zuverlässige Bestimmung des Umfangs sowie der Ausnahmen von den gesetzlichen Verpflichtungen angeht. Angesichts eines dynamischen Wettbewerbsumfelds ist es von erheblichem Mehrwert, seine eigenen Betriebskosten genau bestimmen und zukünftige Investitionen sinnvoll in innovative Produkte und Dienste im Sinne der Kunden lenken zu können.

Vor diesem Hintergrund bedauern wir sehr, dass diese Führungsrolle der Schweiz durch die Ausweitung des Umfangs in der laufenden Vernehmlassung durch Art. 16b (FDA mit reduzierten Pflichten) nun ohne Not riskiert werden soll.

Wenngleich die sprachlichen Änderungen auf den ersten Blick marginal erscheinen mögen, wären die Auswirkungen doch gravierend. So erscheint uns nicht einleuchtend, wieso nunmehr zukünftig nicht mehr nur der Jahresumsatz mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten in der Schweiz zur Beurteilung herangezogen werden soll. Das bedeutet für im Unternehmenssegment tätige Anbieter, dass ein für die Strafverfolgung nicht relevanter Jahresumsatz mit Dienstleistungen – die gerade keine Fernmeldedienste und abgeleiteten Kommunikationsdienste darstellen – urplötzlich eine Unternehmensbetroffenheit entstehen kann. Dies gilt etwa für den Bereich des stark zunehmenden reinen Netzwerkmanagements, bei Beratungsleistungen (bspw. im Bereich Cybersecurity), oder bei zusätzlichem Verkauf von Fernmeldetechnik wie Routern, Switches und anderem Equipment der neuesten Generation bei gleichzeitigem Rückgang der Vermarktung von klassischen Fernmeldediensten wie der Sprachtelefonie.

Die im Rahmen des vorliegenden Entwurfs erwogene zukünftige Verpflichtung für Investitionen in die Überwachbarkeit von Fernmeldediensten würde sich dann auf Unternehmensumsätze mit Dienstleistungen stützen, die gerade keine Fernmeldedienste sind. Alleine dieses Beispiel zeigt, dass die angestrebte Neuregelung im Vergleich zur



Vorgängerregelung Willkür aufweist. Denn sie kann neben der Rechtsunsicherheit hohe Anfangsinvestitionen auf Seite der betroffenen Unternehmen verursachen ohne einen Mehrwert für die Strafverfolgung zu generieren. Die von der Teilrevision angestrebte Vereinfachung wird nicht erreicht und verkehrt sich ins Gegenteil.

Unverhältnismässigkeit der Ausweitung betroffener Unternehmen

Die Statistik des Bundes zur Fernmeldeüberwachung für die vorangegangenen Jahre belegt überdies, dass die angefallenen Auskünfte und Überwachungen zu 94% (Auskünfte) bzw. 99% (Überwachungen) auf lediglich vier Unternehmen, die bereits bislang und auch zukünftig umfassend den Pflichten der VÜPF unterliegen (werden).

Die geplante erweiterte Betrachtung des (nicht mehr nur TK-relevanten) Gesamtumsatzes und die neuen Schwellenwerte bei den AAKD bezüglich der Teilnehmeranzahl werden die Zahl der Unternehmen mit teilweisen oder vollständigen Pflichten erheblich steigern. Diese Unternehmen müssten dann finanzielle Ressourcen in die Implementierung und den Betrieb entsprechender Prozesse und Systeme investieren.

Angesichts der voraussichtlichen Anzahl zusätzlicher Auskünfte und Überwachungen erscheint dieser Aufwand unverhältnismässig, da dem kaum ein entsprechender Mehrwert bzw. Erkenntnisgewinn gegenübersteht. Zudem ist zu berücksichtigen, dass eine Zunahme der Unternehmen mit vollen Pflichten auch einen erhöhten Kontroll- und Überwachungsaufwand für den Dienst ÜPF zur Folge hätte.

Abschliessend möchten wir festhalten, dass die E-VÜPF-Gesetzgebung die bislang ausgewogene und rechtssichere Regelung gerade für kleinere Marktteilnehmer, zu denen auch die Unternehmenskundenanbieter wie die Verizon Switzerland AG zu zählen sind, nachhaltig verschlechtern würde.

Die aufkommende Frage der eigenen Unternehmensbetroffenheit führt zu Wettbewerbsnachteilen und Rechtsunsicherheit, wodurch der Digitalstandort Schweiz ohne Not geschwächt wird. Mit den angedachten Änderungen entsteht im Übrigen zugleich ein erhöhter Kontroll- und Überwachungsaufwand für den Dienst ÜPF mit signifikanten Kostenfolgen für den Bund.

Demgegenüber ist durch die angedachten Änderungen jedoch kein Zusatznutzen für die Strafverfolgung zu erwarten, was durch die Erfahrungen aus der Heranziehung der bisherigen Statistiken belegt wird.

Verizon beantragt deshalb,

die Formulierungen in den Art. 16b und 16g, jeweils in Abs. 1 bei den Umsätzen der jeweiligen Dienste zu belassen und nicht den Gesamtumsatz mit Fernmeldediensten und anderen Diensten des Unternehmens heranzuziehen.

Hinsichtlich der detaillierten Überlegungen zu den einzelnen Artikeln des E-VÜPF verweisen wir auf die Verbandsstellungnahme der asut, die wir uns insofern zu eigen machen und die wir vollumfänglich unterstützen.



Insofern bitten wir Sie, sehr geehrter Herr Bundesrat, die Teilrevision mit dem erforderlichen Augenmass voranzutreiben und nur dort zu revidieren, wo tatsächlich ein Anlass geboten erscheint. Das ist bei der von uns dargestellten Regelung nicht der Fall.

Für allfällige Rückfragen stehen wir Ihnen sehr gern zur Verfügung.

Mit freundlichen Grüßen
für die Verizon Switzerland AG

A handwritten signature in blue ink, appearing to read "Pey".

Dr. Andreas Peya
Leiter Regulierung
Zentral- und Osteuropa



Schweiz. Konsumentenforum, Belpstrasse 11, 3007 Bern

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Per Mail an ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 5. Mai 2025

Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrte Damen und Herren

Der Bundesrat hat am 29. Januar 2025 die Vernehmlassung zur Teilrevision der zwei Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs eröffnet (VÜPF UND VD-ÜPF). Wir danken für die Einladung zur Stellungnahme. Gerne lassen wir Ihnen nachstehend die Konsumentensicht zukommen.

Als Konsumentenorganisation mit einem klaren Fokus auf Eigenverantwortung, Datensouveränität und marktwirtschaftliche Lösungen vertreten wir die Interessen von Konsumenten, die auf ein sicheres und freiheitliches digitales Umfeld angewiesen sind. Aus ihrer Sicht ist das Problem, dass sich aus der geplanten Revision ergibt, offensichtlich: je mehr Daten der Konsumenten gespeichert werden müssen, desto mehr Datenlecks werden riskiert, und dies in einer Zeit, in der sie zunehmend zu einer Bedrohung werden. Jede zusätzliche, nicht zielgerichtete Vorratsdatenspeicherung erhöht die Angriffsfläche – mit potentiell schwerwiegenden Folgen für die Nutzer.

Ausweitung der Überwachungspflichten ist intransparent und unverhältnismässig: die geplante Revision sieht eine massive Ausweitung der Überwachungspflichten auf nahezu alle internetbasierten Kommunikationsdienste ab 5'000 Nutzern vor – mit besonders einschneidenden Pflichten ab einer Million Nutzer oder CHF 100 Millionen Umsatz. Auch kleine und mittlere Anbieter (KMU), auf die viele Schweizer Konsumenten heute setzen, wären betroffen. Diese Schwelle ist tief angesetzt und zieht einen Grossteil der Schweizer Kommunikationsanbieter in die Pflicht – ohne erkennbaren Mehrwert für die Strafverfolgung.

Datenschutz und Kommunikationsgeheimnis gefährdet: die verlangte Identifikation der Nutzer und die Speicherung sekundärer Daten (z. B. IP-Adressen, Geolokalisierung) stehen im Widerspruch zum Kommunikationsgeheimnis und dem Recht auf Privatsphäre und öffnen Tür und Tor für Missbrauch. Besonders problematisch ist, dass viele dieser Informationen künftig nicht mehr durch einen richterlichen Entscheid geschützt wären, sondern automatisch durch Informationsersuchen zugänglich gemacht werden sollen. Für Konsumenten bedeutet das: wer Schweizer Dienste nutzt, wird automatisch zum gläsernen Bürger.

Keine echte Wahl mehr für Konsumenten: Die vorgesehene Kategorisierung nach kumulierten Nutzerzahlen aller Dienste eines Anbieters sowie das automatische Inkrafttreten der Pflichten ohne

Einzelfallentscheidung führen dazu, dass es für datenschutzbewusste Konsumenten keine Alternativen mehr gibt. Nutzer, die weiterhin den Schutz ihrer Privatsphäre ernst nehmen wollen, werden gezwungen sein, zu Anbietern ins Ausland auszuweichen. Damit verlieren Konsumenten nicht nur den Zugriff auf vertrauenswürdige Schweizer Anbieter – sie verlieren auch die Kontrolle über ihre eigenen Daten.

Fazit:

Wir lehnen die vorgelegte Revision in der jetzigen Form klar ab. Sie ist weder verhältnismässig noch effektiv, sondern schadet der digitalen Souveränität der Schweiz und setzt die Daten der Konsumenten unnötigen Risiken aus.

Unsere Empfehlungen:

- 👉 Keine generelle Vorratsdatenspeicherung für abgeleitete Kommunikationsdienste.
- 👉 Kein Zwang zur Nutzeridentifikation ab 5'000 Nutzern.
- 👉 Kein automatischer Eintritt in erhöhte Pflichten ohne Einzelfallprüfung.
- 👉 Rückbesinnung auf den Grundsatz: Datenschutz ist Konsumentenschutz.

Wir danken Ihnen bestens für die Prüfung unserer Argumente

Mit freundlichen Grüßen



Babette Sigg Frank, Präsidentin
praesidentin@konsum.ch; 076 373 83 18

Der Lesefreundlichkeit verpflichtet, verzichtet das kf auf Gendersprache und setzt auf generisches Maskulinum.

Monsieur le Conseiller fédéral
Jans Beat
Chef du Département fédéral de justice et
police (DFJP)
Palais fédéral ouest
3003 Berne

Lausanne, le 6 mai 2025

RÉVISION PARTIELLE DE DEUX ORDONNANCES D'EXÉCUTION DE LA SURVEILLANCE DE LA CORRESPONDANCE PAR POSTE ET TÉLÉCOMMUNICATION (OSCPT ET OME-SCPT)

Monsieur le Conseiller fédéral,

La Chambre vaudoise du commerce et de l'industrie (CVCI) a pris note de la consultation relative à la révision partielle de deux ordonnances d'exécution de la surveillance de la correspondance par poste et télécommunication (OSCPT et OME-SCPT).

La CVCI est préoccupée par le fait que les propositions visant à étendre massivement la surveillance étatique tout en réduisant le contrôle judiciaire menacent les droits fondamentaux des citoyens suisses ainsi que ceux de nos clients à l'échelle internationale.

La CVCI constate que le nombre d'entreprises et de services concernés par les différentes obligations est extrêmement important et fait craindre la mise en œuvre d'un système s'apparentant à une surveillance généralisée en Suisse. Parmi ces dernières, de nombreuses voix s'élèvent contre cette réforme, comme Protonmail et Threema qui estiment que cette révision va trop loin. Ces entreprises soulignent que pour livrer des données automatiquement, le cryptage des métadonnées doit être supprimé, ce qui prétérira encore plus leur confidentialité. Ces dernières années, la Suisse et le Canton de Vaud se sont engagés fortement pour le développement d'un territoire de la confiance numérique via des initiatives comme la Trust Valley et nous estimons que cette révision vient mettre en difficulté cet écosystème en pleine croissance. La proposition est rédigée en des termes si généraux qu'elle pourrait s'appliquer à pratiquement toutes les entreprises technologiques suisses et risquer de nuire à la compétitivité du secteur technologique suisse à un moment où celui-ci connaît une opportunité de croissance sans précédent en Europe.

La Suisse s'est forgée au cours d'un siècle une réputation mondiale en matière de stabilité, de protection de la sphère privée et de sécurité. Cela a grandement profité à de nombreux secteurs de l'économie suisse au cours du siècle dernier et continue d'être l'un des principaux avantages concurrentiels de la Suisse. Dans ce contexte, il est pour le moins étonnant qu'une ordonnance d'exécution outrepasse le silence de la loi. Cette automatisation de l'accès à nos données, qui paraît explicitement dans la dernière révision de l'OSCPT, soulève des interrogations quant à la protection de la sphère privée.

Nous estimons que certaines propositions, telles que la conservation obligatoire des métadonnées appliquée de manière générale, éloignent la Suisse des normes européennes au risque de nuire de manière permanente à la réputation de la Suisse en matière de confiance, de sécurité et de protection de la vie privée, au détriment d'un large éventail d'industries actuelles et futures.

En conséquence, la CVCI demande le retrait du projet de modification mis en consultation et demande une redéfinition des catégories de fournisseurs concernés, une modification des différentes obligations et appelle à un dialogue avec les milieux concernés dans les meilleurs délais.

En vous remerciant de la suite que vous donnerez à la présente, je vous prie de croire, Monsieur le Conseiller fédéral, à l'expression de mes salutations respectueuses.

Fondation pour l'Innovation et la Technologie (FIT)

Julien Guex

Directeur et Secrétaire général



PRISE DE POSITION SUR LA RÉVISION DE L'ORDONNANCE SUR LA SURVEILLANCE DE LA CORRESPONDANCE PAR POSTE ET TÉLÉCOMMUNICATION (OSCPT)

6 mai 2025

La section suisse d'Amnesty International soumet la présente prise de position dans le cadre de la procédure de consultation 2022/21 menée par le Département fédéral de justice. **Nous rejetons la révision de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT) en raison des graves risques qu'elle fait peser sur les droits humains.** Sa mise en œuvre entraînerait la mise en place d'un système de surveillance généralisé et serait ainsi incompatible avec les droits fondamentaux et le droit en vigueur, y compris les engagements internationaux pris par la Suisse.

La sphère privée est protégée par la Constitution fédérale, qui dispose que toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications. Ce droit est aussi garanti, *inter alia*, par la Convention européenne des droits de l'homme et le Pacte international relatif aux droits civils et politiques, ratifiés par la Suisse. De plus, selon l'article 36 de la Constitution, toute restriction d'un droit fondamental doit être fondée sur une base légale, justifiée par un intérêt public et proportionnée au but visé. Lorsque la restriction ne répond pas à ces critères, elle doit être considérée illégale et/ou arbitraire.

La révision de l'OSCPT s'écarte du principe de légalité. L'article 36 de la Constitution fédérale dispose que les restrictions graves aux droits fondamentaux doivent être prévues par une loi. Or, dans le cadre de la révision mise en consultation, le Conseil fédéral entend étendre massivement la surveillance étatique par voie d'ordonnance. La grande majorité des fournisseurs de services de communication seraient *de facto* soumise à ces obligations, y compris les fournisseurs de services de communication dérivés tels que les services de messagerie ou de partage de documents. Dès lors qu'elles atteignent le seuil de 5 000 utilisateurs, ces entreprises seraient soumises à de vastes obligations impliquant la conservation des données secondaires de communication et leur accès automatisé par l'Etat, ainsi que l'identification des utilisateurs de ces services. Une telle incursion dans la sphère privée ne devrait être décidée qu'au niveau de la loi, sujette à la possibilité d'un référendum, pour autant que les principes de nécessité et de proportionnalité soient eux aussi respectés.

Le principe de proportionnalité est également mis à mal par la révision réglementaire. Celle-ci prévoit un élargissement significatif de l'accès automatisé aux données, sans contrôle humain préalable ni possibilité effective pour les fournisseurs de contester des demandes injustifiées. Cette suppression de garanties élémentaires réduit les obstacles qui, jusqu'ici, constituaient des garde-fous essentiels. La transmission automatique d'informations personnelles, sans filtrage ni évaluation individualisée, apparaît disproportionnée au vu du but poursuivi, de même que l'obligation de conserver les métadonnées des utilisateurs pendant six mois. La Cour de Justice de l'Union européenne a d'ailleurs jugé une telle pratique illégale car contraire aux droits fondamentaux (affaires jointes C-293/12 et C-594/12, 8 avril 2014). L'introduction d'une obligation d'identification des utilisateurs pour la grande majorité des fournisseurs de services de communication dérivés représente elle aussi une ingérence disproportionnée dans la sphère privée des utilisateurs.

L'élargissement de l'obligation d'identification apparaît par ailleurs contraire au droit en vigueur. Alors que la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication – dont l'ordonnance est censée encadrer l'application – ne prévoit une telle obligation que pour un nombre limité de fournisseurs, les nouveaux seuils de classification introduits par la révision entraîneraient une extension considérable de cette obligation. De plus, le principe de minimisation des données découlant

de la Loi fédérale sur la protection des données serait lui aussi mis à mal, en ce que l'obligation élargie exigerait des entreprises de collecter des données excédant celles strictement nécessaire à l'exercice de leur activité.

Enfin, la révision augmenterait la vulnérabilité de certains groupes nécessitant une protection particulière. Il s'agit en priorité de ceux dont l'activité requiert des canaux de communication sûrs et confidentiels pour l'exercice légitime de leurs droits, tels que les défenseurs des droits humains, les lanceurs d'alerte et autres activistes. Dans le cas où la révision devait être adoptée, la disparition annoncée des fournisseurs respectant l'autodétermination informationnelle des utilisateurs engendrerait des difficultés supplémentaires pour ces groupes. On peut donc s'attendre à ce que la révision ait un effet dissuasif entravant leur jouissance effective des droits humains, notamment le droit à la liberté d'expression. D'autres groupes soumis au secret professionnel sont aussi concernés, tels que les journalistes, les avocats et les médecins, avec des conséquences potentielles sur la liberté de la presse, le droit à un procès équitable et l'accès à la santé, tous pourtant protégés dans l'ordre juridique suisse.

La section suisse d'Amnesty International invite ainsi le Conseil fédéral à abandonner la révision en cours de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication, celle-ci étant dangereuse, incompatible avec les garanties constitutionnelles, la législation en vigueur et les obligations internationales de la Suisse en matière de droits humains.

En cas de questions, merci de vous adresser à M. Illan ACHER, expert thématique droits numériques, Amnesty International, section suisse : iacher@amnesty.ch

Bundesrätin Karin Keller-Sutter
Eidgenössisches Finanzdepartement EFD
Staatssekretariat für internationale Finanzfragen SIF
CH-3003 Bern

Eingereicht per Email an:
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 6. Juni 2025

Vernehmlassung 2022/21 zu den Teilrevisionen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat Beat Jans
Sehr geehrte Frau Lan Lê und sehr geehrter Herr Antonio Abat
Sehr geehrte Damen und Herren

Gerne nutzen die Demokratischen Jurist*innen Schweiz (DJS) die Gelegenheit zur Stellungnahme betreffend der beiden Teilrevisionen zweier Ausführungsverlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF). Die Vernehmlassung deckt sich weitgehend mit der Vernehmlassungen der Digitalen Gesellschaft Schweiz, welche wir vollumfänglich unterstützen und auf welche wir verweisen.

1 Einleitung

Die geplante Revision der VÜPF ist ein Frontalangriff auf unsere Grundrechte, die Rechtsstaatlichkeit sowie den IT- und Innovationsstandort Schweiz.

Mit ihrer Umsetzung würde geltendes Recht in einem Ausmass verletzt, das alarmieren muss: Die Revision ist in vielerlei Hinsicht unvereinbar mit dem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), verstösst gegen das Datenschutzgesetz (DSG), steht in klarem Widerspruch zu den verfassungsmässigen Grundrechten und verstösst gegen Völkerrecht.

Die vorgesehenen Änderungen führen zu einer massiv ausgeweiteten Überwachung – ganz grundsätzlich und flächendeckend. Dies ist mit der Ausrichtung des BÜPF, das eine fein austarierte Interessenabwägung zwischen Freiheit und Privatsphäre einerseits und Sicherheit durch Überwachungsmassnahmen andererseits verfolgt, absolut nicht vereinbar.

Die Auswirkungen auf den Wirtschafts- und Innovationsstandort Schweiz wären verheerend: Die Ausweitung der Überwachung und die damit verbundenen, übermässigen Mitwirkungspflichten machen die Schweiz für IT-Anbieter äusserst unattraktiv. Renommierte Unternehmen wie Proton oder Threema, deren Geschäftsmodelle durch die Vorlage direkt ins Visier geraten, würden in ihrer Existenz bedroht. Die ersten Konsequenzen sind bereits sichtbar: Proton hat angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen (siehe Tages-Anzeiger vom 1. April 2025). Der Chef des Unternehmens erklärte in einem Interview: «Diese Entscheidung ist wirtschaftlicher Selbstmord für die Schweiz» (watson.ch vom 9. April 2025). Ähnlich äussert sich Threema-Chef Robin Simon: «Der Wirtschaftsstandort würde durch die Revision geschwächt und für Tech-Start-ups unattraktiv.» Aktuell lasse sich Threema alle Optionen offen (Tages-Anzeiger vom 8. April 2025). Diese Warnzeichen sind ernst zu nehmen und zeigen das verheerende Ausmass der geplanten Revision.

Neben den verheerenden wirtschaftlichen Auswirkungen wird gleichzeitig der grundrechtlich garantie Anspruch auf sichere und vertrauliche Kommunikation ausgehöhlt. Wenn Anbieterinnen abwandern, bleibt jedoch – als wäre dies nicht genug – nicht nur privaten Nutzer*innen der Zugang zu geschützten Kommunikationsmitteln verwehrt.

Ebenso betroffen sind auch Personen, die einem Berufsgeheimnis unterstehen, wie Journalistinnen oder Anwälte. Die Änderungen treffen zudem schutzbedürftige Personengruppen besonders hart: Whistleblower*innen, Menschen mit ungeklärtem Aufenthaltsstatus oder ohne Papiere aber auch Aktivist*innen verlieren ebenso den Zugang zu vertraulichen Kommunikationsmitteln. Die Revision ignoriert diese Schutzbedürfnisse und erweitert stattdessen die Eingriffsbefugnisse des Staates in einer Weise, die hochgefährlich ist.

Besonders widersprüchlich erscheint das Vorgehen des Bundes angesichts der Tatsache, dass ausgerechnet der Bundesrat selbst Threema als Messenger nutzt – ein Dienst, den er nun faktisch aus dem Markt drängt. Damit sägt die

Regierung ausgerechnet an jenem Ast, auf dem sie in Sachen sicherer Kommunikation bislang selbst sitzt.

Hinzu kommt: Die geplanten Regelungen sind technisch unausgereift, unnötig komplex und in Teilen schlicht nicht umsetzbar. Vielmehr wird ein kaum noch durchschaubares Normengeflecht geschaffen, das weder den Mitwirkungspflichtigen noch den Betroffenen ein Mindestmass an Rechtsklarheit bietet. Die Revision wird ausserdem präsentiert, als handle es sich dabei um Änderungen zur besseren Überblickbarkeit der Rechtslage und zur Schaffung von mehr Rechtssicherheit - tatsächlich aber wird der persönliche Anwendungsbereich der Mitwirkungspflichtigen enorm erweitert und eine Vielzahl neuer Anbieterinnen in den Kreis der Mitwirkungspflichtigen einbezogen. Von Transparenz kann nicht die Rede sein.

Es ist im Übrigen nicht haltbar, dass eine dermassen breit angelegte Ausweitung von Pflichten auf Verordnungsstufe angelegt wird. Solch einschneidende Veränderungen mit weitreichenden Konsequenzen sind in Gesetzesform zu erlassen. Der Bundesrat überschreitet seine Kompetenzen hier um ein Weites.

Diese Vorlage schwächt nicht nur den Innovations- und Wirtschaftsstandort Schweiz – sie untergräbt gleichzeitig im grossen Stil verfassungsmässig geschützte Rechte. Aus grundrechtlicher, datenschutzrechtlicher und gesellschaftspolitischer Sicht ist sie schlicht inakzeptabel. Die geplanten Änderungen stehen dem erklärten Ziel von mehr Freundlichkeit sowie allgemeinen rechtsstaatlichen Grundsätzen sowie Schutzbedürfnissen Einzelner diametral entgegen.

Deshalb lehnen wir die Revision vollumfänglich und in aller Deutlichkeit ab.

2 Bemerkungen zu einzelnen Artikeln der VÜPF

2.1 Alle Artikel

Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung (Art. 6 Abs. 3 DSG) gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kund*innen auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.

Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.ä. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.

Vorschlag DJS:

Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.

2.2 Art. 16b Abs. 1 VÜPF

Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile (Art. 16b Abs. 1 lit. b Ziff. 2 VE-VÜPF) wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Mitwirkungspflichten in Kauf nehmen.

Dazu kommt, dass das Kriterium bezüglich der Überwachungsaufträge nicht vom BÜPF gestützt wird, denn: Die Anzahl von Überwachungsaufträgen ist von der wirtschaftlichen Bedeutung einer FDA völlig losgelöst. Die wirtschaftliche Bedeutung ist aber gemäss Art. 26 Abs. 6 BÜPF ausschlaggebend dafür, ob eine FDA von den vollen Pflichten (teilweise) befreit werden kann. Im Umkehrschluss ist die wirtschaftliche Bedeutsamkeit somit Erfordernis für die Auferlegung von vollen Pflichten. Wenn eine FDA nun aber rein aufgrund einer bestimmten Anzahl von Überwachungsaufträgen nach Art. 16b Abs. 1 lit. b Ziff. 1 VE-VÜPF als vollpflichtige FDA qualifiziert wird, steht dies im Widerspruch zum BÜPF und entbehrt damit einer Rechtsgrundlage.

Dieses bereits in der aktuellen Version der VÜPF vorhandene Problem sollte im Zuge einer Revision nicht bestehen bleiben, sondern muss behoben werden.

Vorschlag DJS:

Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.» Es ist auf die Regelung in Art. 26 Abs. 6 BÜPF abzustellen und eine Einzelfallbetrachtung zur Einstufung vorzunehmen.

2.3 Art. 16c Abs. 3 VÜPF

Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen

falsche oder unberechtigte Anfragen zu wehren. Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als «natürliche» Schutzmechanismen gegen eine übermässige oder missbräuchliche Nutzung solcher Massnahmen durch die Untersuchungsbehörden. Die automatisierte Erteilung von Auskünften ist unverhältnismässig und widerspricht dem Prinzip der Datenminimierung. Die pauschale und undifferenzierte Regel beeinträchtigt zwangsläufig den Grundrechtsschutz.

Der vorgesehene Umsetzungszeitraum von 12 Monaten zur Umsetzung eines dermassen komplexen Systems ist ausserdem unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel.

Vorschlag DJS:

Streichung von lit. a «automatisierte Erteilung der Auskünfte» (ebenso in Art. 18 Abs. 2).

2.4 Art. 16d VÜPF

Gemäss erläuterndem Bericht stellen Kommunikationsdienste, die nicht zu den in Art. 16a Abs. 1 aufgezählten Fernmelddiensten gehören und auf die die Ausnahmen nach Art. 16a Abs. 2 nicht zutreffen, abgeleitete Kommunikationsdienste dar. Diese klarere Definition des Begriffs AAKD ist begrüssenswert, doch ist die Konkretisierung der abgeleiteten Kommunikationsdienste im erläuternden Bericht einerseits rechtsstaatlich problematisch und andererseits geht die neue Auslegung nach den Ausführungen im erläuterndem Bericht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdiensten wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter etc.) genutzt werden.

Art. 2 lit. c BÜPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft jedoch auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug in die Auslegung unrechtmässig ist – auch hier setzt sich die Revision über die gesetzlichen Vorgaben des BÜPF hinweg.

Zudem anerkennt der erläuternde Bericht zwar, dass VPNs zur Anonymisierung der Nutzer*innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil angebrachte Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kern-dienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglich. Das Bedürfnis, auch künftig VPN-Dienste in Anspruch nehmen zu können,

ist zu schützen und darf nicht vereitelt werden. Anbieter von VPNs sind daher ebenfalls aus Art. 16d auszunehmen.

Es ist irritierend, dass die bewusst separat ausgestalteten Kategorien AAKD und FDA einander zunehmend angeglichen werden, und zwar zuungunsten der AAKD, die als Kategorie mit grundsätzlich weniger weitreichenden Pflichten als die FDA konzipiert wurde. Dies missachtet den Willen des Gesetzgebers, den es zu wahren gilt.

Vorschlag DJS:

Streichung von Onlinespeicherdielen und VPN-Anbietern aus der Aufzählung der möglichen abgeleiteten Kommunikationsdiensten im erläuternden Bericht zu Art. 16d VBÜPF.

2.5 Art. 16e, 16f und Art. 16g VÜPF

Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch komplett entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung mit deutlich erweiterten Pflichten. Entscheidend ist, dass neuerdings das Kriterium von 5'000 Nutzer:innen allein zum Auferlegen massiver Überwachungspflichten ausreicht: Erreicht eine AAKD diese Grösse, fällt sie neu in die Kategorie der AAKD mit reduzierten Pflichten und untersteht somit bereits sehr weitgehenden Mitwirkungspflichten, insbesondere der Identifikationspflicht.

Die Einführung von 5'000 Nutzer:innen als gesondert zu beurteilende Untergrenze verletzt Art. 27 Abs. 3 BÜPF, denn 5'000 Personen sind keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strengerem Überwachungsmaßnahmen, gerechtfertigt wären. 5'000 Nutzer:innen werden in der digitalen Welt vielmehr sehr rasch erreicht – die Revision verkennt technische Realitäten.

Zusätzlich führt das Einführen eines Konzernatbestandes in Art. 16f Abs. 3 zu massiven Problemen: Produkte und Dienste müssen nicht mehr für sich allein bestimmte Schwellenwerte erreichen – es genügt, wenn das Mutterunternehmen oder verbundene Gesellschaften diese überschreiten. Insbesondere bei Unternehmen mit Beteiligungsstrukturen führt dies dazu, dass sämtliche Angebote pauschal der höchsten Überwachungsstufe unterstellt werden – unabhängig davon, ob sich einzelne Dienste noch im frühen Entwicklungsstadium befinden oder faktisch kaum genutzt werden. Somit müsste jedes neue Projekt von Beginn an mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden, was Innovation behindert. Zudem missachtet der

Konzerntatbestand das Verhältnismässigkeitsgebot: Unterschiedliche organisatorische Einheiten mit eigenständigen Angeboten werden unrechtmässig zusammengefasst, obwohl sie individuell zu prüfen wären. Die Anwendung starrer Schwellen auf ganze Konzerne statt auf einzelne Dienste umgeht eine notwendige Einzelfallprüfung.

Eine solche Regelung stünde sodann im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali, das die zu seltene Anwendung von Downgrades kritisierte:

«Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»

Statt KMU zu entlasten, führt die Revision neu zu einem «automatischen» Upgrade per Verordnung ohne Verfügung (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.

Eine Analyse der offiziellen VÜPF-Statistik unterstreicht diese offensichtliche Unverhältnismässigkeit. Im Jahr 2023 betrafen 98,97% der total 9'430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,03% für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,74% wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100% des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.

Die neue Vorlage schliesst nun ebenfalls sowohl die Registrierung via normaler E-Mail als auch die komplett anonyme Registrierung (z. B. Signal oder Telegram) aus, da AAKD bereits mit reduzierten Pflichten neu automatisch zwingend die Endnutzer:innen identifizieren müssen. Hiervon betroffen sind nicht nur alle AAKD mit reduzierten Pflichten, sondern auch all deren Wiederverkäufer. Faktisch resultiert das Gesetz somit darin, dass man sich bei keinem Dienst mehr anmelden können soll, ohne den Pass, Führerschein oder die ID entweder direkt oder indirekt zu hinterlegen. Dass Nutzer:innen künftig hierzu gezwungen wären, stellt einen massiven Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 BV) dar und ist unzumutbar.

Ein weiteres Kernproblem, das die automatische Hochstufung mit sich bringt, ist die Rechtsunsicherheit. Die Vorlage will mit klarer definierten Kategorien und Pflichten ein übersichtlichere Situation schaffen, verfehlt dieses Ziel jedoch gänzlich. Bislang fand die Hochstufung per Verfügung statt, wodurch es

für die Mitwirkungspflichtigen klar erkennbar war, wann sie unter welche Pflichten fallen. Ausserdem bewirkt diese Praxis eine sinnvolle Einzelfallbe trachtung anstelle pauschaler und unzweckmässiger automatischer Hochstufungen. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den massgebenden Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes kann aber im Zweifelsfall nur schwer zu beantworten sein. Gerade deshalb besteht ein schutzwürdiges Interesse der Anbieter an Klarheit über ihre Pflichten, da sie fortan eventuell die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Diese Umstrukturierung lässt ich nicht mit der Funktionsweise von Verwaltungsverfahren vereinbaren. Die Pflicht zur Abklärung, wann eine Hochstufung vorliegt und was diese für das Unternehmen bedeutet, darf nicht in die Verantwortung der Unternehmen fallen. Der Staat zieht sich hier aus der Verantwortung und schiebt diese den Unternehmen zu, wodurch diesen zwangsläufig zeitlicher und finanzieller Mehraufwand entsteht. Von einer automatischen Hochstufung von AAKD ist daher abzusehen.

Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.

Gegenüber der geltenden VÜPF erweitert die Revision die Pflichten zur Automatisierung noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragetypen wie z. B. "IR_59" und "IR_60", welche ebenfalls automatisiert und ohne manuelle Intervention abge fragt werden können sollen. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.

Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 lit. b der geltenden VÜPF), die dazu führt, dass eine Unternehmung nicht mehr ab geleitete Kommunikationsdienste als einen «grossen[n] Teil ihrer Geschäftstätig keit» anbieten muss, um als AAKD zu gelten. Damit fallen auch Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz.

Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Auch hiermit werden neue Hürden für Innovation geschaffen. Die Regelung ist unverhältnismässig und nicht sachdienlich.

Auch Non-Profit-Organisationen geraten unter die verschärften Vorgaben. Unter den neuen Kriterien wird aber allein auf die Anzahl der Nutzer:innen abgestellt für die Einstufung als AAKD. Dieses Kriterium greift jedoch zu kurz: Es berücksichtigt insbesondere nicht die wirtschaftliche Tragfähigkeit der Anbieter:innen. Gerade bei Open-Source- und Non-Profit-Lösungen mit grosser Reichweite, aber geringem Budget, führt dies zu einer verheerenden finanziellen Belastung: Anbieter:innen mit solchen Projekten würden gezwungen, umfangreiche Überwachungsmassnahmen einzuführen. Solche Anbieter:innen würden gezielt aus dem Schweizer Markt gedrängt, während gleichzeitig bestehende Monopole wie WhatsApp (96% Marktanteil in der Schweiz) gestärkt würden.

Es muss ausserdem klar festgehalten werden, dass sich das BÜPF und die VÜPF nur auf Anbieter:innen beziehen können, die in der Schweiz tatsächlich tätig sind. Die Erlasse dürfen nicht so ausgelegt werden, dass sie eine extra-territoriale Wirkung entfalten und internationale Dienste wie Signal, WhatsApp oder Microsoft Teams erfasst sind.

Das Kriterium der reinen Nutzer*innenzahl ist ungeeignet und muss gestrichen werden.

Die Regelung schwächt auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade us-amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger*innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, End-zu-End-verschlüsselter Kommunikation ist heute wichtiger denn je und fällt in den Bereich grundrechtlich geschützter Ansprüche, die es zu wahren gilt. Diese Ansprüche dürfen nicht aufs Spiel gesetzt werden, um ein knallhartes Überwachungsregime der Kommunikation in der Schweiz durchzusetzen – die Prioritäten werden höchst fragwürdig gesetzt.

Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade illegal ist (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer*innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, diese zu erhebenden Datenmengen sind von enormem Ausmass und bergen folglich massive Risiken für Hackerangriffe.

Des Weiteren ist nicht belegt, dass die Speicherung der betreffenden Daten zu spürbar mehr erfolgreichen Ermittlungen führt. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an

Kindern im Internet und Kindsmisshandlung via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfüge, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.

Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren.

Diese Handhabe bedeutet einen Verstoss gegen das Legalitätsprinzip und untergräbt legislative Kompetenzen. Ausserdem verfügt die Schweiz bereits über reichlich Mittel zur Aufklärung und Verfolgung von Straftaten, die Behörden können bereits heute auf sicherheitsrelevante Daten zurückgreifen. Unternehmen wie Proton (s. «Positionspapier zur Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)» von Proton) kooperieren seit Jahren mit den Schweizer Strafverfolgungsbehörden und dem Nachrichtendienst des Bundes (NDB). Wenn nun solche Unternehmen aus bereits genannten Gründen zur Abwanderung gezwungen werden, bewirkt die Revision auch hier das genaue Gegenteil ihrer erklärten Ziele: Anstatt der Schaffung besserer Möglichkeiten zur Strafverfolgung würden die Schweizer Behörden wie etwa Fedpol den Zugriff auf wichtige Partner bei der Beschaffung sicherheitsrelevanter Daten verlieren.

Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Integrität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.

Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das DSG. Der Entwurf bringt nicht, wie der Begleitbericht den Leser*innen weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit, steht in direktem Gegensatz zum besagten Postulat 19.4031 und bedeutet massive Eingriffe in grundrechtlich geschützte Sphären, sowohl von Unternehmen als auch von Nutzer*innen.

Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen und das bestehende System muss beibehalten werden.

Vorschlag DJS:

Streichung der Artikel und Beibehaltung der bestehenden Kriterien und der zwei Kategorien von AAKD. + Ausnahmen für Pilotprojekte (auch von grossen Firmen) und Non-Profits per se. Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).

2.6 Art. 16h VÜPF

Art. 16h VÜPF konkretisiert die Kategorie der «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» aus Art. 2 lit. e BÜPF. Die Vorschrift verfehlt ihr Ziel – anstatt Unsicherheiten darüber zu beheben, wer unter diese Kategorie fällt, schafft sie weitere Unklarheiten. Der schwammig formulierte Verordnungstext könnte dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist*innen, Whistleblower*innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber*innen solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer*innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen. Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt. Die Unklarheit bezüglich der Einordnung von TOR-Servern wirft weitere Fragen auf, denn wenn TOR nicht als PZD zu qualifizieren ist, müsste TOR – gleich wie die VPNs – der Kategorie der AAKD zugeordnet werden. Somit stünden Betreiber*innen von TOR-Servern – wie etwa die Digitale Gesellschaft – unter der Identifikationspflicht. Diese ist jedoch, wie dargelegt, nicht umsetzbar.

Es braucht somit entweder die Zusicherung, dass Betreiberinnen von TOR-Nodes nicht dem BÜPF und der VÜPF unterstellt sind oder aber Kategorien von Mitwirkungspflichten, die so gestaltet sind, dass ein*e Betreiber*in eines TOR-Nodes nicht einer Identifikationspflicht unterstellt wird – z. B. indem die Schwelle für das Auferlegen der Identifikationspflicht auf 1 Mio. Nutzer*innen angehoben wird.

Wären Betreiberinnen von TOR-Nodes von der Identifikationspflicht erfasst, würde dies fundamentale Grundrechte wie das Recht auf Privatsphäre und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK), die Meinungs- und Informationsfreiheit (Art. 16 BV, Art. 10 EMRK) gefährden. Ebenso würde das datenschutzrechtliche Prinzip der Datensicherheit (Art. 8 DSG) komplett unterlaufen. Diese Eingriffe in national und international geschützte Rechtsansprüche sind nicht hinzunehmen.

Dieser potentielle Angriff auf die genannten Grundrechte setzt ein politisches Statement: Die Schweiz bewegt sich weg von Grundrechtsschutz hin zum hochgerüsteten Überwachungsstaat.

Vorschlag DJS:

Es muss sichergestellt werden, dass Technologien wie TOR oder I2P nicht vom Anwendungsbereich der VÜPF erfasst sind.

2.7 Art. 16h Abs. 2 VÜPF

Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Endbenutzer*innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 VE-VÜPF: Gemäss diesem Artikel trägt die das WLAN erschliessenden FDA die Verantwortung zur Identifikation der Nutzer*innen. Die Regelung führt also dazu, dass FDA, die einen Vertrag haben mit «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» (PZD), sehr schnell für die Identifikation der Endnutzer*innen ihrer Vertragspartner zuständig sind. Diese Regelung ist unsinnig und schlicht nicht umsetzbar.

Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer*innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24), die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22) oder der Verwendung von IPv6. Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDA unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden.

Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten: FDA resp. Anbieterinnen von öffentlichen WLAN-Zugängen dürfen nur unter einer Identifikationspflicht stehen, wenn die PZD, die den Zugang der FDA nutzt, «professionell betrieben» ist – und zwar nach der aktuellen Auslegungsform (s. Erläuternder Bericht zur (letzten)Totalrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs): «Mit «professionell betrieben» ist gemeint, dass eine FDA oder eine auf öffentliche WLAN- Zugangspunkte spezialisierte IT-Dienstleisterin den technischen Betrieb des öffentlichen WLAN-Zugangspunktes durchführt, die dies auch noch für andere öffentliche WLAN-Zugangspunkte an anderen Standorten macht.

Wenn eine natürliche oder juristische Person an ihrem Internetzugang selbst einen öffentlichen WLAN-Zugangspunkt technisch betreibt und diesen Zugang Dritten zur Verfügung stellt, muss die FDA, die den Internetzugang anbietet, keine Identifikation der Endbenutzenden sicherstellen.» Nur so wird sichergestellt, dass FDA nicht unmöglich umzusetzenden Pflichten unterstellt werden.

Vorschlag DJS:

Streichung der Ausführung im erläuternden Bericht. Das Kriterium «professionell betrieben» ist nach der bislang geltenden Regelung zu verstehen. Art. 16h Abs. 2 ist ersatzlos zu streichen und im Zusammenhang mit Art. 19 Abs. 2 ist auf die aktuelle Definition von «professionell betrieben» abzustellen.

2.8 Art. 16b Abs. 2, Art. 16f Abs. 3 und Art. 16g Abs. 2 VÜPF

Bei Konzernen knüpft die VE-VÜPF nicht mehr an die Umsatz- und Nutzer*inenzahlen des betroffenen Unternehmens an, neu sind die Zahlen des Konzerns ausschlaggebend für eine Hoch- oder Herunterstufung. Die Begründung, dies diene der Vereinfachung, ist unlogisch und irreführend: Unternehmen müssen ihre Zahlen ohnehin produktbezogen ausweisen, die nötigen Daten liegen also längst vor. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.

Vorschlag DJS:

Streichung des «Konzernatbestand» und Beibehaltung der bestehenden Regelung.

2.9 Art. 19 Abs. 1 VÜPF

Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD – erfasst sind die AAKD mit reduzierten und mit vollen Pflichten – widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht. Durch die neuen Schwellenwerte zur Einstufung findet eine beachtliche Ausweitung der Identifikationspflicht statt.

Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des DSG, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch insbesondere der Grundrechtsschutz von Nutzer*innen in der Schweiz massiv beeinträchtigt wird. Die Identifikationspflicht greift immens in das Recht auf informationelle Selbstbestimmung ein und hält einer Grundrechtsprüfung nach Art. 36 BV schon allein aufgrund ihrer Unverhältnismässigkeit nicht stand.

Bezüglich einschneidender Pflichten, die potentiell schwere Grundrechtseingriffe bedeuten – wie es bei Identifikationspflichten zweifellos der Fall ist – muss Rechtsetzung in jedem Fall mit äusserster Sorgfalt und unter strenger Beachtung des Verhältnismässigkeitgebots erfolgen. Ausserdem darf sich eine solche Pflicht nicht über gesetzliche Vorgaben, wie in diesem Fall vom BÜPF vorgegeben, hinwegsetzen.

Durch die breite Auferlegung einer solchen Pflicht werden datenschutzfreundliche Unternehmen bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.

Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Nur so können datenschutzrechtliche Vorgaben und die Rechte Betroffener gewahrt werden.

Vorschlag DJS:

Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation von Teilnehmenden.

2.10 Art. 18 VÜPF

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.

Vorschlag DJS:

Streichung Teil «Anbieter mit reduzierten Pflichten».

2.11 Art. 12 Abs. 2 VÜPF

Das Kriterium «professionell betrieben» ist nach der bestehenden Regelung auszulegen (s. vorstehen). Es sei ausserdem darauf hingewiesen, dass sich aus dieser Regelung eine vertragsrechtliche Problematik zwischen den FDA und den PZD ergeben würde, die nicht tragbar ist.

Vorschlag DJS:

Auslegung des Kriteriums «professionell betrieben» nach der bestehenden Regelung und nicht i. S. v. Art. 16h Abs. 2.

2.12 Art. 21 Abs. 1 lit. a VÜPF

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.

Vorschlag DJS:

Streichung.

2.13 Art. 22 VÜPF

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.

Vorschlag DJS:

Beibehaltung.

2.14 Art. 11 Abs. 4 VÜPF

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.

Für allfällige Rückfragen zu unserer Stellungnahme stehen wir gerne zur Verfügung.

Vorschlag DJS:

Streichung.

2.15 Art. 16b VÜPF

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.

Vorschlag DJS:

Streichung.

2.16 Art. 31 Abs. 1 VÜPF

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.

Vorschlag DJS:

Streichung Teil «Anbieter mit reduzierten Pflichten»

2.17 Art. 51 und 52 VÜPF

Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.

Vorschlag DJS:

Beibehaltung.

2.18 Art. 60a VÜPF

Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Durch die neue Massnahme aus Art. 60a kann eine ordnende Behörde laut den Erläuterungen bewusst auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten. Art. 60a ist zu streichen.

Vorschlag DJS:

Streichung.

2.19 Art. 42a und 43a VÜPF

Art. 42a und 43a führen neu die Abfragetypen «IR_59» und «IR_60» ein, über die sensible Daten automatisiert abgefragt werden können. Sie verlangen von Anbieterinnen, dass sie jederzeit Auskunft geben können bezüglich des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Auch für das Auferlegen dieser Pflicht gilt die fragliche Schwelle von 5'000 Nutzer*innen. Erfasst ist somit nahezu die gesamte AAKD-Landschaft der Schweiz.

Das Problem liegt darin, dass die «IR_»-Abfragen zu Informationen nach Art. 42a und 43a neu automatisiert abgerufen werden können – im Gegensatz zu den «HD_»- (historische Daten) und «RT»- (Echtzeitüberwachung) Abfragen, die strengeren Regeln und einer juristischen Kontrolle unterliegen. Bei den «IR_59»- und «IR_60»-Abfragen handelt es sich allerdings um sensible

Informationen wie etwa das Abrufen einer IP-Adresse. Solche Informationen mussten bislang zurecht über strengere Abfragetypen eingeholt werden. Es ist nicht nachvollziehbar, warum Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber.

Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser automatisierten Auskünfte ergibt. Unternehmen sind daher nur unzureichend geschützt vor missbräuchlichen Anfragen und vor Kosten, die ihnen durch die Pflicht, diese Auskünfte automatisch weiterzugeben, entstehen wird.

Künftig könnten so umfangreiche Informationen über die neuen Abfragetypen beschafft werden, die bislang zurecht den strengeren Regeln der rechtlich sichereren Informations-/Überwachungstypen «HD_» und «RT_» unterworfen waren. «IR_59» und «IR_60» ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne den erforderlichen Kontrollen dieser invasiven Überwachungstypen unterworfen zu sein.

Die Entwicklung, dass mittels «IR_»-Abfragen neu auch personenbezogene sensible Nutzungsdaten eingeholt werden können, widerspricht der Logik der unterschiedlichen Abfragetypen und öffnet Tür und Tor für missbräuchliche Abfragen und eine Echtzeitüberwachung von Millionen von Nutze*:innen. Auch hier stehen grundrechtlich geschützte Ansprüche auf dem Spiel, die mit einer solchen Regelung auf nicht nachvollziehbare Weise untergraben und missachtet werden.

Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind. Die AAKD müssten künftig gewisse Datenkategorien systematisch erheben, um dieser Pflicht nachzukommen. Art. 27 Abs. 2 BÜPF erklärt allerdings, dass AAKD «auf Verlangen die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person liefern» müssen. Bei einer dahingehenden Auslegung des Bestimmungen bedeutete dies einen weiteren Verstoss gegen das BÜPF. Die beiden Artikel sind daher vollumfänglich zu streichen.

Unter rechtsstaatlichen Gesichtspunkten gilt es außerdem die geplante Schwächung des Zwangsmassnahmengerichts auf das Schärfste zu kritisieren. Mit der Schaffung der zwei neuen Auskunftstypen, die mittels einfacher Auskunftsanfrage automatisch abgerufen werden, werden rechtliche Kontrollmechanismen wie das Zwangsmassnahmengericht umgangen und der Einflussbereich der Staatsanwaltschaft noch weiter ausgebaut. Art. 42a und 43a sind daher ersatzlos zu streichen.

Vorschlag DJS:

Streichung.

2.20 Art. 50a VÜPF

Art. 50a sieht vor, dass Anbieter*innen verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Auch diese Pflicht soll eine Vielzahl neuer Unternehmen erfassen: Betroffen sind nicht mehr nur FDA (Art. 26 BÜPF) und ausnahmsweise AAKD (Art. 27 BÜPF), sondern sämtliche Anbieter*innen mit mehr als 5'000 Nutzer*innen. Im Ergebnis wäre fast die gesamte Schweizer AAKD-Branche betroffen (kaum ein Produkt ist lebensfähig mit weniger als 5'000 Teilnehmer*innen).

Die Ausdehnung dieser Pflicht auf AAKD stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar: Es findet keine Einzelfallprüfung statt und die AAKD werden dieser Pflicht unterworfen, auch wenn sie keineswegs «Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten», was jedoch gesetzliche Vorgabe ist (Art. 27 Abs. 3 BÜPF).

Problematisch ist zudem, dass aufgrund dieser Vorgabe Anbieter*innen ihrer Verschlüsselungen so konfigurieren müssen, dass sie von ihnen aufgehoben werden können – eine durch Anbieter*innen aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung allerdings in jedem Fall. Dies führt zu schwächeren Verschlüsselungen und der Abnahme der Sicherheit von Kommunikationsdiensten.

Daraus ergibt sich eine Grundrechtsproblematik von erheblicher Tragweite: Das Verhältnismässigkeitsgebot aus Art. 36 BV kann nicht eingehalten werden, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Die Interessenabwägung darf hier nicht zuungunsten der Grundrechtsträger*innen erfolgen, da es sich bei deren Interessen um solche von fundamentalem Gewicht – dem Zugang zu sicherer Kommunikation und damit direkt verbunden dem Recht auf freie Meinungsäußerung – handelt.

Wichtig ist, dass Verschlüsselungen, die auf dem Endgerät der Nutzer*innen erfolgen – also End-zu-End-Verschlüsselungen – nicht unter die Pflicht zur Aufhebung gemäss Art. 50a VE-VÜPF fallen dürfen. Diese Form der Verschlüsselung liegt ausschliesslich in der Sphäre der Nutzer*innen und es wäre untragbar, die Pflicht zur Aufhebung von Verschlüsselungen in dieser Sphäre zu verlangen. Die Anbieter*innen dürfen daher nicht dazu verpflichtet werden, diese Inhalte zu entschlüsseln und zugänglich zu machen. Im Gegensatz dazu betrifft die Transportverschlüsselung «lediglich» die Verbindung zwischen Client und Server und kann von Anbieter*innen kontrolliert werden. Es ist wichtig,

dass diese technischen Unterscheidungen und unterschiedlichen Schutzwirkungen und -richtungen bei rechtlichen Umsetzungen beachtet werden. Wir begrüssen die Klarstellung im erläuternden Bericht, dass die End-zu-End-Verschlüsselung vom Anwendungsbereich ausgenommen ist. Es muss jedoch ebenso klar sein, dass das ganze Endgerät von Nutzer*innen aus dem Anwendungsbereich von Art. 50a VE-VÜPF ausgenommen ist.

Es braucht im Übrigen auch eine Klarstellung darüber, dass eine rückwirkende Möglichkeit zur Aufhebung klar ausgeschlossen ist. Eine solche würde de facto eine Vorratsdatenspeicherung verschlüsselter Inhalte und Keys darstellen, die mit dem Prinzip der Datenminimierung (Art. 6 Abs. 3 DSG) und dem Schutz der Privatsphäre (Art. 13 BV) unvereinbar ist.

Vorschlag DJS:

Streichung der «Anbieterin mit reduzierten Pflichten» aus dem Anwendungsbereich sowie eine Klarstellung darüber, dass die Aufhebung von Verschlüsselungen auf dem Endgerät der Nutzer:innen sowie eine rückwirkende Verpflichtung zur Aufhebung ausgeschlossen sind.

3 Bemerkungen zu einzelnen Artikeln der VD-ÜPF

3.1 Art. 14 Abs. 3 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer*innen) unverhältnismässig und wirtschaftlich nicht tragbar, was das Einführen von Fristen obsolet werden lässt. Der Absatz ist daher ersatzlos zu streichen.

Vorschlag DJS:

Streichung.

3.2 Art. 14 Abs. 4 VD-ÜPF

Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der Unterworfenen AAKD – da auch AAKD mit reduzierten Pflichten erfasst sind – massiv. Dies ist wie bereits ausgeführt weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.

Vorschlag DJS:

Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten»

3.3 Art. 20 Abs. 1 VD-ÜPF

Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen, ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.

Vorschlag DJS:

Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»

4 Schlussbemerkung

Trotz des Umfangs dieser Stellungnahme gilt: Das Ausbleiben einer expliziten Bemerkung zu einzelnen Bestimmungen bedeutet keine Zustimmung der Digitalen Gesellschaft. Die Ablehnung der Revision bleibt vollumfänglich bestehen.

Besten Dank für die Berücksichtigung unserer Stellungnahme.

Mit freundlichen Grüßen



Lea Schlunegger
Generalsekretärin DJS

Eidgenössisches Justiz- und Polizeidepartement EJPD

Einreichung per Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Zürich, 6. Mai 2025

Die Swiss Startup Association lehnt die Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs ab

Sehr geehrte Damen und Herren

Die Swiss Startup Association (SSA) ist der grösste und wichtigste Startup-Verband der Schweiz mit über 1'800 Startups als Mitgliedern und vertritt dadurch ca. 50 % aller Startups in der Schweiz. Diese 1'800 Mitglieder sind alle in den letzten 4 Jahren Mitglied geworden. Die Organisation ist, wie die gesamte Startup-Landschaft der Schweiz, aktuell sehr stark am Wachsen. Insgesamt arbeiten in der Schweiz bereits heute ca. 50'000 Menschen in einem Startup. Die Swiss Startup Association hat sich u.a. zum Ziel gesetzt, die Rahmenbedingungen für Neugründungen und Startups in der Schweiz zu verbessern. Um diese Ziele zu erreichen, stehen wir in dauerndem und sehr engem Austausch mit unseren Mitgliedern. Die Swiss Startup Association agiert partei- und branchenunabhängig, ist eine non-profit Organisation und sieht sich als Dachorganisation vom Schweizer Startup-Ökosystem.

Die geplanten Revisionen des VÜPF und des VD-ÜPF treffen die Schweizer Startup Branche in ihren Grundfesten. Sie schaden dem Innovationsstandort Schweiz und zwingen Unternehmen aufgrund marktverzerrender Regulierung dazu, ihren Standort ins Ausland zu verlegen. Dies trifft junge Unternehmen im Technologie- und Innovationssektor besonders hart.

Die Swiss Startup Association lehnt die Revision aus den folgenden Gründen dezidiert ab:

1. Unverhältnismässig hohe Auflagen für Unternehmen

Die Revision sieht eine Ausweitung der Mitwirkungspflichten auf alle internetbasierten Kommunikationsdienste ab 5'000 Nutzerinnen und Nutzer vor. In der Realität wären damit faktisch sämtlichen Startups für internetbasierte Kommunikationsdienstleistungen bereits während ihrer Aufbauphase von den Verschärfungen betroffen. Die damit verbundenen Auflagen zur Mitwirkungspflicht und technischen Anforderungen sind für diese Unternehmen unternehmerisch nicht stemmbar. Dazu kommt, dass für etablierte Unternehmen ab einer Million User oder CHF 100 Millionen Umsatz weitreichende Pflichten angesetzt werden sollen, welche unternehmerische Mehrkosten in Millionenhöhe verursachen. Dies schreckt Startups in der Wachstumsphase zusätzlich davon ab, ihren unternehmerischen Erfolg in der Schweiz zu suchen. Die geplanten Verschärfungen und die daraus resultierenden Kosten für Technologieunternehmen sind komplett unverhältnismässig.

2. Internationale Wettbewerbsfähigkeit der Schweizer Startups gefährdet

Die vorgesehene Revision führt unmittelbar dazu, dass Schweizer Technologieunternehmen im internationalen Umfeld nicht mehr wettbewerbsfähig sind. Die digitale Kommunikation findet in einem hoch globalisierten Markt statt – und die Schweiz ist keine Insel. Die geplanten Massnahmen des Bundes stehen im diametralen Gegensatz zum Naturell dieser digitalen Welt. Gewisse

Dienstleistungen wie beispielsweise der Betrieb eines VPNs wären unter der geplanten Revision in der Schweiz schlicht nicht mehr möglich, da beispielsweise die Speicherung von Geolokalisierungs- und IP-Daten dem Zweck eines VPNs im Grundsatz widerspricht. Dies zeigt beispielhaft, welches marktzerrende Potenzial die geplante Revision im internationalen Umfeld hat. Denn in keinem anderen westlichen Land sind Unternehmen solch scharfen Überwachungsmassnahmen ausgesetzt. Dieses innovationsfeindliche Umfeld beeinträchtigt nicht nur den direkt betroffenen Technologieunternehmen, sondern langfristig der gesamten Startup Branche.

3. Die Schweiz hat einen Ruf zu verlieren

Die Schweiz geniesst bei Gründerinnen und Gründern aus der ganzen Welt einen ausgezeichneten Ruf. Der Zugang zu den besten Forschungseinrichtungen und Universitäten, gute Rahmenbedingungen und marktfreundliche Regulierungen machen die Schweiz zu einem attraktiven Innovationsstandort. Die in der Revision vorgesehenen unverhältnismässigen Eingriffe in die digitale Privatsphäre sind jedoch eine Gefahr für die Zukunftsfähigkeit der Schweizer Technologiebranche. Sie schaden dem internationalen Ruf der Schweiz als Hüterin von Grundrechten und sind Gift für die Innovationsfähigkeit der Schweiz. Ausländische Startups werden davon absehen in der Schweiz ein Unternehmen zu gründen und bereits ansässige Startups suchen den Weg ins Ausland. Die langfristigen volkswirtschaftlichen Auswirkungen sind kaum zu beziffern. Zu den negativen Folgen der geplanten Verschärfung des VÜPF gehört außerdem ein erhöhtes Risiko für Cyberattacken. Die hohe Konzentration an sensiblen Primär- und Sekundärdaten über 6 Monate für hunderte Millionen Nutzerkonten macht die Schweizer Technologieunternehmen zu einem lohnenden Angriffsziel – mit entsprechend negativen Auswirkungen auf die öffentliche Sicherheit und den Wirtschaftsstandort Schweiz.

Aus den dargelegten Gründen erachten wir die geplante Revision als eine Gefahr für das Startup-Ökosystem der Schweiz und lehnen die Revision in Gänze ab. Wir danken Ihnen herzlich für die Berücksichtigung unserer Argumente und stehen Ihnen gerne für weitere Auskünfte zur Verfügung



Raphael Tobler
Präsident

Universität Basel, Rektorat, Postfach, 4001 Basel

Per E-Mail an:
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Basel, 6. Mai 2025

Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF): Stellungnahme

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zur obengenannten Vorlage Stellung nehmen zu können.

Nach dem aktuellen Wortlaut von Art. 51 Abs. 1 VÜPF hat eine Anbieterin von Fernmeldediensten (FDA) dann reduzierte Überwachungspflichten, wenn sie ihre Fernmeldedienste nur im Bereich Bildung und Forschung anbietet oder wenn sie beide der nachstehenden Grössen nach Art. 51 Abs. 1 Bst. b VÜPF (kumulativ) nicht erreicht, nämlich:

1. Überwachungsaufträge zu 10 verschiedenen Zielen (Target) der Überwachung in den letzten 12 Monaten (Stichtag: 30. Juni)
2. Jahresumsatz in der Schweiz mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten von 100 Millionen Franken in zwei aufeinander folgenden Geschäftsjahren.

Die Universität Basel betreibt ihre eigene Netzwerkinfrastruktur. Neben der Nutzung des Netzwerkes durch die Mitarbeitenden und Studierenden der Universität Basel selber, stellt die Universität Basel den Zugang auch diversen weiteren eigenständigen öffentlich-rechtlichen und privatrechtlichen Institutionen zur Verfügung. So gewährt die Universität Basel Netzwerkzugang etwa mit der Universität Basel assoziierten Institutionen, wie unter anderem dem Universitätsspital Basel (USB), dem Universitäts-Kinderspital beider Basel (UKBB) oder dem Schweizerischen Tropen und Public-Health Institut (Swiss TPH). Daneben erhalten auch diverse weitere Kooperationspartner Zugriff auf das universitäre Netzwerk. Die Universität Basel ist dadurch eine FDA im Sinne des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). Die Nutzung des universitären Netzwerks erfolgt in der Regel kostenlos oder wird den betreffenden Dritten nach dem Grundsatz der Kostendeckung in Rechnung gestellt. Die Universität Basel macht keinen Umsatz indem sie Dritten den Netzwerkzugang zur Verfügung stellt.

Seite 1/3

Gemäss der Verfügung des Dienstes Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) vom 20. Juli 2021 erfüllte die Universität Basel die Voraussetzung, um als FDA mit reduzierten Überwachungspflichten eingestuft werden zu können.

Im Rahmen der Teilerevision der VÜPF wird nun beabsichtigt die Kriterien für einen Down Grade zur FDA mit reduzierten Überwachungspflichten gemäss Art. 51 Abs. 1 Bst. b Ziff. 1 und 2 VÜPF zu ändern. Der Bundesrat wies in seinem Bericht vom 18. Oktober 2023 (S. 7) darauf hin, er beabsichtige «mit der laufenden Revision der VÜPF (Revision des Geltungsbereichs) die rechtlichen Grundlagen so zu optimieren, dass es anhand der Definitionen einfach ersichtlich sein wird, welcher Kategorie eine Anbieterin zugewiesen ist». Dies werde dazu führen, so der Bundesrat, «dass von den beim Dienst ÜPF elektronisch erfassten Anbieterinnen nur wenige in der Kategorie FDA verbleiben, wovon die grosse Mehrheit in den Genuss von reduzierten Pflichten kommen dürfte».

So soll mit Inkrafttreten der Vorlage gemäss Art. 16b Abs. 1 lit. b Ziff. 2 E-VÜPF neu der Gesamtumsatz des gesamten Unternehmens in der Schweiz massgebend sein und nicht – wie bisher in Art. 51 Abs. 1 Bst. b Ziff. 2 VÜPF – nur auf den Jahresumsatz abgestellt werden, der in der Schweiz mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten erzielt wurde. Wie im erläuternden Bericht zur Eröffnung des Vernehmlassungsverfahrens des Eidgenössischen Justiz und Polizeidepartement (EJPD) vom 8. Januar 2025 ausgeführt wird, erfolgt diese Änderung aus Gründen der Vereinfachung, da es sich in der Praxis gezeigt habe, dass der gesamte Unternehmensumsatz viel einfacher ermittelt und belegt werden kann.

Die Universität Basel würde nach dem vorgeschlagenen Wortlaut die Voraussetzung für eine FDA mit reduzierten Überwachungspflichten allerdings nicht mehr erfüllen, da ihr Umsatz – sofern man bei einer birkantonal finanzierten, öffentlich-rechtlichen Hochschule wie der Universität Basel, überhaupt von «Umsatz» sprechen kann – deutlich über dem Wert von CHF 100 Mio. pro Jahr liegt. Vor diesem Hintergrund würde die vorgeschlagene Änderung der VÜPF im Fall der Universität Basel, wie auch weiterer öffentlich-rechtlicher Hochschulen in der Schweiz, genau das Gegenteil dessen bewirken, was mit der Vorlage eigentlich beabsichtigt wird.

Die Universität Basel beantragt daher, dass in Art. 16b Abs. 1 lit. b Ziff. 2 E-VÜPF – zumindest für Hochschulen – weiterhin auf den mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten erzielten Umsatz abgestellt wird und nicht auf den Jahresumsatz des gesamten Unternehmens.

Art. 16 Abs. 1 lit. a E-VÜPF belässt die bisher in Art. 51 Abs. 1 lit. a VÜPF vorgesehene Ausnahme für FDA im Bereich Bildung und Forschung unverändert bestehen. Obwohl der Gesetzgeber Bildungsinstitutionen wie etwa Universitäten bereits bisher in der VÜPF vorgesehen hatte, fand diese Ausnahmebestimmung aufgrund ihrer restriktiven Formulierung tatsächlich im Fall der Universität Basel gar keine Anwendung. Da die Universität Basel ihre Fernmeldedienste nicht «nur» im Bereich Bildung und Forschung anbietet, konnte sie ihr Gesuch für einen «down grade» zur FDA mit reduzierten Überwachungspflichten nicht auf Art. 51 Abs. 1 lit. a VÜPF stützen.

Sollte der Bundesrat an der Änderung gemäss Art. 16b Abs. 1 lit. b Ziff. 2 E-VÜPF festhalten wollen, beantragt die Universität Basel im Gegenzug den Wortlaut von Art. 16b Abs. 1 lit. a E-VÜPF dahingehend zu ändern, dass es zur Qualifikation als FDA mit reduzierten Überwachungspflichten in Zukunft ausreichend wäre Fernmeldedienste «überwiegend» im Bereich Bildung und Forschung anzubieten. Somit müssten sich Schweizer Hochschulen nicht mehr auf die Ausnahmebestimmung gemäss Art. 51 Abs. 1 Bst. b Ziff. 2 VÜPF resp. Art. 16b Abs. 1 lit. b Ziff. 2 E-VÜPF stützen, um weiterhin die Voraussetzungen einer FDA mit reduzierten Überwachungspflichten erfüllen zu können.

Für Rückfragen stehen Ihnen Dr. iur. Poonsap Stähelin (p.staehelin@unibas.ch) und MLaw David Schaub (d.schaub@unibas.ch) gerne zur Verfügung.

Mit freundlichen Grüßen



Prof. Dr. Dr. h.c. mult. Andrea Schenker-Wicki
Rektorin



*Vernehmlassungsantwort zu den Teilrevisionen der VÜPF und der VD-ÜPF
gemäss Schreiben des EJPD vom 29. Januar 2025*

Datum	6. Mai 2025
Verfasser (Unternehmen)	Threema GmbH, CHE-221.440.104, Churerstrasse 82, 8808 Pfäffikon SZ
Kontaktperson bei Fragen (Name/Tel./E-Mail)	Peter Szabó Legal Counsel und Datenschutzberater der Threema GmbH legal@threema.ch

Dieses Dokument geht an:

Eidgenössisches Justiz- und Polizeidepartement EJPD, ptss-aemterkonsultationen@isc-ejpd.admin.ch.

Threema.

Sehr geehrter Herr Bundesrat Jans, sehr geehrte Damen und Herren

Wir beziehen uns auf das am 29. Januar 2025 eröffnete Vernehmlassungsverfahren zu Teilrevisionen von VÜPF und VD-ÜPF und bedanken uns für die Möglichkeit einer Stellungnahme.

Wir lehnen die geplante Teilrevisionen der VÜPF und der VD-ÜPF in aller Deutlichkeit und vollumfänglich ab.

Im Bericht des Bundesrates zur aktuellen Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF und der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) ist zu lesen, dass die Revision im Wesentlichen auf die Anpassung der Verordnungen an die KMU-Freundlichkeit abziele. Ein grosser Teil der vorgeschlagenen Änderungen *verfolgt aber gerade das Gegenteil*.

Die Geschäftsgrundlagen von Schweizer Unternehmen wie Threema, Proton und anderer KMU, die weltweit einen hervorragenden Ruf als Anbieterinnen sicherer Kommunikationsdienste im Internet geniessen, drohen durch die Vorlage zerstört zu werden. Die Sicherheit des Internets in der Schweiz soll mit der Revision der Überwachung jeglichen Internetverkehrs regelrecht untergeordnet werden: **«Sicherheit vor Freiheit» ist das neue Paradigma.** Dieses zieht sich wie ein roter Faden quer durch diese völlig verunglückte Reform. Für KMU, die aus der Schweiz heraus Internetdienste anbieten (**«abgeleitete Kommunikationsdienste»** in der Terminologie des Gesetzes), soll die Schweiz als Standort geradezu vergällt werden. Dies scheint denn auch zu gelingen: **Erste der betroffenen Unternehmen haben bereits angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen** (siehe Tages-Anzeiger vom 1. April 2025).

Ein derartiger Paradigmenwechsel, weg von KMU-Schutz und Überwachung mit Augenmass, hin zu knallharter Überwachung, die alle anderen Interessen unterordnet, wird durch das geltende Gesetz (BÜPF) keineswegs gestützt. Der Paradigmenwechsel widerspricht vielmehr geradezu dem Geist des ursprünglichen BÜPF, dass Internetdienste, die in der Schweiz meist von KMU betrieben werden, gerade von der Implementierung teurer Überwachungsmassnahmen schützen wollte, und das eine austarierte Interessenabwägung vorsah zwischen Privatsphäre und Freiheit auf der einen Seite und staatlicher Überwachung auf der anderen Seite.

Entgegen dem im Begleitbericht zum vorgelegten Entwurf erklärten Ziel, die «finanzielle Belastung der KMU gering zu halten», stuft die Vorlage eine grosse Mehrheit der Schweizer Anbieterinnen von Internetdiensten in eine höhere Stufe auf, und zwingt sie neu auch in jenen Bereichen zu einer kostspieligen aktiven Überwachungstätigkeit, wo bisher nur eine KMU-freundliche Duldungspflicht bestand. Dies verschiebt das bisherige Gleichgewicht der Interessen zwischen Strafverfolgung und betroffenen Anbieterinnen in drastischer Weise zulasten der betroffenen Anbieterinnen.

Die vorgeschlagenen Anpassungen bringen ganz erhebliche Risiken für den Innovations- und Wirtschaftsstandort Schweiz mit sich und erfüllen die Kernziele der Revision, die Entlastung von KMU, gerade nicht. Der Ruf der Schweiz als sicherer Hafen für vertrauenswürdige IT-Anbieter droht durch die Revision nachhaltig beschädigt zu werden. Deshalb lehnen wir die Revision vollumfänglich ab.

Threema.

Auch **die Schweizer Armee** nutzt solche Dienste, wie beispielsweise Threema, und zwar gerade aufgrund des hohen gebotenen Sicherheitsstandards. Die Annahme dieser Revision, welche dieses Sicherheitsniveau gezielt untergraben will, verletzt damit indirekt auch das direkte Interesse der Schweiz an lokal betriebenen Hochsicherheitsanwendungen. Gerade in der heutigen Zeit, in der die Zuverlässigkeit der grossen US-Anbieter in ihrer Abhängigkeit von einer zunehmend erratisch agierenden US-Regierung mehr und mehr in Frage steht, erscheint dies als **inakzeptable Hochrisikostrategie**.

Nicht zuletzt ist mit Nachdruck darauf hinzuweisen, dass die Revision die Überwachung ganz allgemein stark ausweitet. Dies ist mit der durch den Gesetzgeber im BÜPF festgelegten, fein austarierten Interessenabwägung zwischen Freiheit und Privatsphäre der Einwohnerinnen und Einwohner der Schweiz einerseits und Sicherheit durch Überwachungsmassnahmen andererseits absolut nicht vereinbar. Die Revision entpuppt sich geradezu als eine Art Wunschkonzert für Überwachungsbehörden. Insbesondere ist künftig auch **eine komplette inhaltliche Überwachung des gesamten Internetverkehrs** der Schweiz vorgesehen. Dies, ohne dass eine solche inhaltliche Überwachung durch die gesetzlichen Grundlagen des BÜPF in irgendeiner Weise gedeckt wäre: Zulässig ist gemäss BÜPF einzig und allein die Überwachung von Randdaten des Fernmeldeverkehrs, und selbst die Zulässigkeit der in diesem Kontext angewendeten anlasslosen Vorratsdatenspeicherung von Randdaten ist bis heute umstritten und Gegenstand von Gerichtsverfahren, ja in der EU bereits höchstrichterlich als menschenrechtswidrig erkannt. Die durch die Verordnungsrevision eingeführte *Inhaltsüberwachung* ist in der Schweiz damit erst recht **offensichtlich illegal und verfassungswidrig**.

Abschliessend sei noch der Hinweis angebracht, dass wir die Gesetzgebungstechnik des Entwurfs für überaus schlecht halten. **Sowohl der Verordnungstext als auch der zugehörige erläuternde Bericht sind über weite Strecken höchst verwirrend und unverständlich formuliert**, unter anderem mit einer Vielzahl von Querverweisen, technischen Fehlern und unklarer Begrifflichkeit (für ein Beispiel hierfür siehe unten, Bemerkungen zu Art. 43a). Die Texte sind in dieser Form selbst für Fachleute über weite Strecken nicht zu verstehen, geschweige denn als Ganzes zu überblicken. Für KMU, die durch die Revision neu mit erheblich strengeren Pflichten konfrontiert werden, ist eine rechtskonforme Umsetzung dieser Vorlage daher ein schlicht aussichtloses Unterfangen.

Das Legalitätsprinzip gemäss Art. 5 Bundesverfassung fordert vom Gesetzgeber, dass Gesetzestexte für die Adressaten verständlich formuliert sind. Die Texte der Verordnungsrevision genügen dieser Anforderung offensichtlich in keiner Weise. Nur schon aufgrund der völlig fehlenden Verständlichkeit ist die Verfassungsmässigkeit der Revision insgesamt *höchst zweifelhaft*. Wir fordern nur schon deshalb einen Rückzug der vorgelegten Texte, eine komplette Überarbeitung zur Verbesserung der Verständlichkeit und eine erneute Auflage zur Vernehmlassung.

Mit freundlichen Grüßen


Robin Simon
CEO der Threema GmbH

Threema.

Bemerkungen zu einzelnen Artikeln der VÜPF

Nr.	Artikel	Antrag	Begründung / Bemerkung
VÜPF / OSCPT / OSCPT			
0.	Alle Artikel	Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.	<p>Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kunden auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.</p> <p>Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.dgl. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.</p>
1.	16b, Abs. 1	Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.»	Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile, wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Anforderungen in Kauf nehmen.

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
2.	16c, Abs. 3	Streichung von lit. a «automatisierte Erteilung der Auskünfte (Art. 18 Abs. 2);»	<p>Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Dies untergräbt rechtsstaatliche Prinzipien doppelt: Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als «natürliche» Schutzmechanismen gegen eine überschiessende, missbräuchliche oder zumindest unverhältnismässige Nutzung solcher Massnahmen durch die Untersuchungsbehörden.</p> <p>Der vorgesehene Umsetzungszeitraum von 12 Monaten für die rechtssichere Implementierung eines derart komplexen Systems völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.</p>
3.	Art. 16d	Streichung von Onlinespeicherdiensten und VPN-Anbietern in der Auslegung	<p>Eine klarere Definition des Begriffs AAKD ist begrüssenswert, doch die neue Auslegung gemäss erläuterndem Bericht geht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdiensten wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter, etc.) genutzt werden.</p> <p>Art. 2 lit. c BÜPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug den gesetzlichen Rahmen sprengt. Onlinespeicherdienste sind deshalb aus Art. 16d zu streichen.</p> <p>Zudem anerkennt der erläuternde Bericht, dass VPNs zur Anonymisierung der Nutzerinnen und Nutzer dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Anbieter von VPNs sind daher ebenfalls aus dem Geltungsbereich von Art. 16d auszunehmen.</p>
4.	Art. 16e, Art. 16f und Art. 16g	<p>Streichung der Artikel und Beibehaltung der bestehenden Kriterien</p> <p>Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b)</p>	<p>Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch diametral entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung. Dies daher, weil neu KMU bereits mit mehr als 5'000 Nutzern erfasst werden.</p>

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
		Ziff. 1).	<p>Die Einführung von 5'000 Nutzern als gesondert zu beurteilende Untergrenze verletzt aus unserer Sicht bereits Art. 27 Abs. 3 BÜPF, denn 5'000 Personen keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strengereren Überwachungsmassnahmen, gerechtfertigt wären. 5'000 Nutzer werden in der digitalen Welt vielmehr sehr rasch erreicht.</p> <p>Zusätzlich führt das Einführen eines «Konzerntatbestandes» in Art. 16f Abs. 3 zu massiven Problemen, da die Produkte nun nicht mehr für sich alleine eine bestimmte Grösse erreichen müssen, sondern die relevanten Zahlen anhand des Umsatzes des Unternehmens, bzw. in Konzernverhältnissen sogar des Konzerns bestimmt werden. Vor allem bei Unternehmen mit Beteiligungsfirmen im Hintergrund fallen nun neu alle Dienstleistungen und Produkte automatisch unter die härteste Stufe, egal ob sie sich erst in einem frühen Entwicklungsstadium befinden. Dies behindert Innovation, da jedes Projekt bereits mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden müsste. Durch diese extreme Einstiegshürde wird der Innovationsstandort Schweiz nachhaltig geschädigt.</p> <p>Gleichzeitig wird auch der Wirkungsbereich der VÜPF stark erweitert. Während heute ein Unternehmen einen grosse[n] Teil seiner Geschäftstätigkeit durch abgeleitete Kommunikationsdienste erbringen muss (Art. 22 Abs. 1 lit. b und Art. 52 Abs. 1 lit. b VÜPF), fällt dieses Kriterium neu weg. Dadurch können künftig auch Unternehmen, deren Geschäftstätigkeit nur am Rande auf abgeleiteten Kommunikationsdiensten basiert, wie Onlineshops, Marktplätze, Auktionsplattformen, Zeitungen, Computerspielhersteller und zahlreiche weitere Unternehmen, unter die VÜPF fallen – allein deshalb, weil ihre Produkte irgendeine Form privater Kommunikation zwischen Nutzerinnen und Nutzern und/oder Drittanbietern ermöglichen.</p> <p>Die vorgeschlagene Regelung stünde sodann im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali, das die zu weite Betroffenheit und die seltene Anwendung von Downgrades kritisierte: «Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»</p> <p>Statt KMU zu entlasten, führt die Revision neu sogar zu einer «automatischen» Hochstufung per Verordnung ohne konkretisierende Verfügung (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.</p> <p>Die neue Regelung steht zudem in offensichtlichem Widerspruch zur bisherigen Praxis, denn</p>

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>bis heute wurde gemäss Angaben des Dienst-ÜPF keine einzige AAKD hochgestuft. Auch der Bundesrat stützte sich ausdrücklich auf die geltende Kombination von drei Schranken – einem Unternehmensfokus auf Kommunikationsdienste, einer Umsatzgrenze von 100 Millionen Franken sowie einer grossen Nutzerzahl – als er noch 2023 begründete, die Umsetzung des BÜPF sei gerade wegen der genannten Schranken als KMU-freundlich zu verstehen. Die vorliegende Revision hebt jedoch genau diese Kombination kumulativer Kriterien auf und will die einzelnen Kriterien künftig alternativ anwenden bzw. streicht sie sogar vollständig. Dadurch verlieren die bisherigen Schutzmechanismen ihre Wirkung, und das BÜPF soll neu auf viele KMU Anwendung finden, die früher nicht unter Gesetz und Verordnung fielen.</p> <p>Die Analyse der offiziellen Statistik des Dienstes ÜPF macht die offensichtliche Unverhältnismässigkeit dieses Ansinnens deutlich. Im Jahr 2023 betrafen 98,95 % der total 9'430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,05 % für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,73 % wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100 % des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliarden-schwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.</p> <p>Wesentlich ist insbesondere eine neue Pflicht zur Identifikation der Nutzer: Hiervon betroffen sind nicht nur alle AAKD mit reduzierten oder vollen Pflichten (und damit de facto fast alle AAKD der Schweiz), sondern auch all deren Wiederverkäufer. Im Ergebnis führt die neue Verordnung aus unserer Sicht dazu, dass man sich bei keinem marktrelevanten Dienst mehr anmelden kann, ohne den Pass, Führerschein oder ID zu hinterlegen oder zumindest Daten wie eine Telefonnummer anzugeben, die man ohne Pass oder ID nicht erhalten kann.</p> <p>Die automatische Hochstufung an sich führt bereits zu erheblicher Rechtsunsicherheit bei den betroffenen Unternehmen. Unter dem bestehenden System werden die generell-abstrakten Normen der VÜPF mittels Verfügung auf einen konkreten Einzelfall angewendet. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes ist aber im Zweifelsfall möglicherweise nur schwer zu beantworten. Zweifelsohne besteht hier ein schutzwürdiges Interesse seitens der AAKD daran, zu wissen, ob sie die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststel-</p>

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>lungsverfügung erkundigen. Nur das bisherige System entspricht den allgemeinen Grundsätzen des Verwaltungsverfahrens, welches für die Anwendung einer generell-abstrakten Norm eine Konkretisierung durch die Verwaltung voraussetzt. Von einer automatischen Hochstufung von AAKD ist daher aus Gründen der Rechtssicherheit abzusehen. Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMU (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.</p> <p>Gegenüber der alten VÜPF erweitert die Revision die Pflichten zur Automatisierung sodann noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragen wie z.B. IR_59 und IR_60, welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen. Genau diese Möglichkeit einer manuellen Intervention ist aber für die Provider kritisch, um Missbräuche zu verhindern, die wiederum die Verträge mit ihren Kunden und das Fernmeldegeheimnis verletzen könnten. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente damit erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.</p> <p>Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 Bst. b der alten VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grosse[n] Teil ihrer Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. Damit fallen insbesondere bereits Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz. Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Dies setzt der Innovation in der Schweiz neue riesige Hürden entgegen.</p> <p>Auch Non-Profit-Organisationen wie die Signal Foundation, die kaum Umsätze erwirtschaften, geraten unter diese verschärften Vorgaben. Während sie bisher unter Duldungspflichten verbleiben konnten, solange sie Art. 22 Abs. 1 VÜPF nicht erfüllten, wird neu allein auf die Anzahl der Nutzerinnen und Nutzer abgestellt, womit z.B. Signal neu als AAKD mit vollen Pflichten erfasst würde. Dies würde dazu führen, dass Signal in der Schweiz entweder zu ei-</p>

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>nem Rückzug aus dem Markt gezwungen wird oder erhebliche rechtliche Konsequenzen risikiert, da Signal keine IP-Adressen speichert und somit gegen Art. 19 revVÜPF verstößt.</p> <p>Die Regelung ignoriert zudem wirtschaftliche Realitäten: Ein hoher Nutzerkreis bedeutet bei Non-Profits keine finanzielle Tragfähigkeit für umfangreiche Überwachungsmassnahmen. Damit werden Open-Source- und Non-Profit-Lösungen gezielt aus dem Markt gedrängt, während bestehende Monopole wie WhatsApp (96 % Marktanteil in der Schweiz) gestärkt werden. Die neue Regelung ist daher aus ökonomischer Sicht zu verwerfen. Das Kriterium der reinen Nutzerzahl ist ungeeignet und muss gestrichen werden.</p> <p>Nicht zuletzt schwächt die Regelung auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürgerinnen und Bürgern der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, Ende-zu-Ende-verschlüsselter Kommunikation ist heute wichtiger denn je.</p> <p>Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade als rechtswidrig gilt (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzerinnen und Nutzer dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, sondern allein diese Anhäufung an Daten malt eine Zielscheibe auf den Rücken von Schweizer Unternehmen und Dienstleistungen für Hackerangriffe aus der ganzen Welt.</p> <p>Weiters ist zu erwähnen, dass es gar nicht erwiesen ist, dass die Speicherung der fraglichen Daten eine merklich höhere Quote erfolgreicher Ermittlungen durch die Strafverfolgungsbehörden mit sich bringen würde. Im Gegenteil müssen die bereits existierenden Sekundärdaten, die allein durch die Bereitstellung eines Dienstes für den Nutzer entstehen, besser genutzt werden. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisshandlung via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfügt, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismäßigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden</p>

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden. Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren.</p> <p>Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Souveränität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.</p> <p>Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das Datenschutzgesetz. Der Entwurf bringt nicht, wie der Begleitbericht dem Leser in geradezu in Orwell'scher Manier weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit und steht in direktem Gegensatz zum besagten Postulat 19.4031.</p> <p>Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen, und das bestehende System muss beibehalten werden.</p>
5.	Art. 16h Abs. 2	Streichung der Ausführung im erläuternden Bericht und ein Abstellen der Formulierung auf die gleichzeitige Anzahl Nutzer.	<p>Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Nutzerinnen und Nutzer den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 revVÜPF, gemäss dem die das WLAN erschliessenden FDA die Verantwortung für die Identifikation der Nutzer der WLANs tragen.</p> <p>Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzerinnen und Nutzer zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24) oder die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22). Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDA unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht</p>

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden. Unter der bestehenden Regelung konnte eine FDA anhand der Lokation (z.B. Bibliothek, Flughafen) eine Einschätzung treffen. Die neue Definition hingegen würde von ihr verlangen, Zugriff auf jedes private Netzwerk zu erhalten, um Hardware und Einstellungen zu prüfen – ein offensichtlich verfassungswidriges und auch praktisch unmögliches Unterfangen. Diese vage Formulierung führt zu anhaltender Rechtsunsicherheit für FDA.</p> <p>Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten.</p> <p>Zudem könnte Art. 16h dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalistinnen, Whistleblower und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzerinnen und Nutzer gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen. Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt.</p>
	Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2	Streichung des «Konzernatbestand» und Beibehaltung der bestehenden Regelung	<p>Die Verordnung nimmt neu nicht mehr die Umsatz- und Nutzerzahlen der betroffenen Unternehmen, sondern die Zahlen des jeweiligen Konzerns als Basis für Up- und Downgrades. Die Begründung zur Einführung dieses «Konzernatbestands», wonach die neue Regelung für die betroffenen Unternehmen zu einer Vereinfachung führe, ist kontraintuitiv, ja offensichtlich falsch und irreführend. In der Praxis sind die betroffenen Unternehmen nämlich schon heute verpflichtet, ihre Buchhaltung nach Produkten aufzugliedern. Somit können die Kennzahlen bereits heute sehr einfach festgestellt werden. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.</p>
6.	Art. 19 Abs. 1	Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation von	<p>Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht.</p> <p>Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des Schweizer Datenschutzgesetzes, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch der</p>

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
		Teilnehmenden.	<p>Schutz der Schweizer Kundschaft massiv beeinträchtigt wird. Datenschutzfreundliche Unternehmen werden bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.</p> <p>Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Dies wahrt nicht nur den Datenschutz, sondern schützt auch die Wettbewerbsfähigkeit von KMU, stärkt den Innovationsstandort Schweiz und die digitale Souveränität unseres Landes.</p>
7.	Art. 18	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.
8.	Art. 19 Abs. 2	Ersatzlose Streichung zugunsten bestehender Regelung	Eine Überwachung von Kunden durch FDA, ob diese die neuen Vorgaben der VÜPF zu WLANs einhalten (Art. 19 Abs. 2 revVÜPF), und erst recht die dazu gelieferte Erklärung im erläuternden Bericht, wonach die FDA die Identifikation der WLAN-Nutzer vorzunehmen hätten, ist weder gesetzeskonform noch zumutbar (siehe vorstehend). Art. 19 Abs. 2 ist ersatzlos zu streichen.
9.	Art. 21 Abs. 1 lit. a	Streichung	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.
10.	Art. 22	beibehalten	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.
11.	Art. 11 Abs. 4	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.
12.	Art. 16b	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.
13.	Art. 31 Abs. 1	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
14.	Art. 51 und 52	beibehalten	Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.
15.	Art. 60a	Streichung des Artikels	<p>Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu urteilen.</p> <p>Art. 60a VÜPF (Erläuterung Bundesrat: «...lediglich redaktionelle Änderungen....») sieht vor, dass Fernmeldedienstanbieterinnen über einen rückwirkenden Zeitraum von 6 Monaten alle Ziel-IP-Adressen liefern müssen, welche ihre Kunden besucht haben. Damit wird einerseits das Surfverhalten der gesamten schweizerischen Bevölkerung anlasslos und völlig unverhältnismässig ausspioniert. Andererseits wird die klare Vorgabe des BÜPF umgangen, dass nur die Speicherung von Randdaten, aber nicht die Speicherung von Inhaltsdaten vorsieht.</p> <p>Die geplante Überwachung des Internetverkehrs führt zu einer Überwachung, wer im Internet welche Adressen besucht hat. Dies geht zweifellos über die Schranken der gesetzlichen Regelung hinaus, dies insbesondere nachdem bereits die Aufzeichnung reiner Randdaten höchst umstritten und Gegenstand laufender Gerichtsverfahren ist. Hinzu kommt folgendes: Während bislang die Überwachung einer IP-Adresse nur im Rahmen einer sog. Echtzeit-Überwachung zulässig war, welche entsprechende Bewilligungen durch ein Gericht erforderte, muss neu nur noch ein einfaches Auskunftsbegehren durch die zuständige Behörde genehmigt werden. Die Abfragen erfolgen automatisiert.</p> <p>Art. 60a sieht weiter vor, dass bei nicht exakt zuordenbaren IP-Adressen die kompletten Listen aller Nutzerinnen und Nutzer zu liefern ist. IP-Adressen sind ein rares Gut. Alle FDA teilen diese den Nutzenden im Millisekunden-Takt zu. Da die Zeitstempel der Systemanbieter nicht immer übereinstimmen, sind diese IP-Adressen nicht immer eindeutig einem Nutzenden zuzuordnen. Neu müssen Provider nun komplette Listen aller Nutzenden liefern. Dies bringt Zehntausende in den Fokus von Überwachungsbehörden, was auf eine Art Rasterfahndung nach Delikten über grosse Teile der Bevölkerung hinausläuft. Entdecken Strafverfolger dabei zufälligerweise etwas, können sie umgehend Strafverfahren einleiten.</p> <p>Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde sodann gemäss Bericht gezielt auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten.</p>

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			Art. 60a ist zu streichen.
16.	Art. 42a und Art. 43a	Streichung des Artikels	<p>Sowohl Art. 42a als auch Art. 43a fordern die Abrufbarkeit des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Nicht nur gilt auch hier wieder die Limite von 5'000 Nutzern, was somit fast die gesamte AAKD-Landschaft der Schweiz flächendeckend umfasst, sondern solche Abfragen sollen nun auch durch eine einfach «IR_» Abfrage gemacht werden können, welche im Gegensatz zu den «HD_»-Abfragen und den «RT_»-Überwachungen ohne weitere juristische Aufsicht automatisiert abgerufen werden können, obwohl es sich auch hier um das Abrufen einer IP-Adresse in der Vergangenheit handelt, genau wie bei den «HD_» abfragen, welche deutlich strenger reglementiert sind. Es ist nicht nachvollziehbar und verletzt aus unserer Sicht die gesetzliche Grundlage des BÜPF, dass Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber.</p> <p>Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser Automatisierten Auskünfte ergibt. Durch das Fehlen solcher Limiten könnte daher z.B. alle 5 Minuten eine solche Anfrage automatisiert gestellt werden. Zunächst können sich dadurch lärmende Kosten für die betroffenen AAKD ergeben. Sodann können die Anfragen an ein automatisiertes Auskunftssystem gestellt werden, und es können auf diese Weise viele der Informationen welche ursprünglich über die juristisch sichereren HD_ und RT_ Auskunfts-/Überwachungstypen liefen, neu über den rechtlich unsicheren IR_-Typ eingeholt werden. IR_59 und IR_60 ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne dass sie den benötigten Kontrollen dieser invasiven Überwachungsarten unterliegen würden.</p> <p>Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind, wie dies das BÜPF vorsieht.</p> <p>Die beiden Artikel sind daher vollumfänglich zu streichen.</p> <p>Diese neue Regelung und der zugehörige erläuternde Bericht sind im Übrigen eklatante Beispiele für die eingangs bemängelte, überaus verwirrende und unverständliche Darstellung von Verordnungstext und erläuterndem Bericht.</p>

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Im erläuternden Bericht steht auf S. 39 wörtlich:</p> <p>«In Absatz 1 sind die zu liefernden Angaben geregelt. Gemäss Buchstabe a ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin der oder dem Teilnehmenden einen solchen zugeteilt hat. Der «eindeutige Dienstidentifikator» gemäss Buchstabe b bezeichnet den Fernmelde- oder abgeleiteten Kommunikationsdienst, auf den sich die Antwort bezieht, eindeutig im Bereich der Anbieterin. In Buchstabe c werden die zu liefernden Angaben über den Ursprung der Verbindung bei der letztenzugriffsrelevanten Aktivität aufgezählt. Diese Angaben können für die Identifikation der Benutzerinnen und Benutzer nützlich sein.»</p> <p>Der Leser bzw. die Leserin urteile selber über die Verständlichkeit.</p> <p>Folgende Begriffe sind auch für den fachkundigen Leser nicht nachvollziehbar, bzw. es stellen sich folgende Verständnisfragen:</p> <ul style="list-style-type: none"> - Eindeutiger Identifikator: Was ist gemeint? Ist die Kundennummer des Internetproviders gemeint? Oder jene des genutzten dritten Fernmeldedienstes oder abgeleiteten Kommunikationsdienstes? Wie soll der Internetprovider überhaupt an diese Daten herankommen? - Eindeutiger Dienstidentifikator: Muss der Internetprovider eine Liste aller möglichen durch seine Kunden im Internet genutzten Kommunikationsdienste führen und aufzeichnen, muss er zudem aufzeichnen welcher Kunde welchen Dienst wann genau genutzt hat? Woher hat er diese Liste? Wie kann er herausfinden, ob ein Kunde gerade einen bestimmten Dienst nutzt? Gilt dies auch für ausländische Dienste? Nur für AAKD, für ausländische Fernmeldedienste, oder für alle Internetangebote weltweit? Der erläuternde Bericht bleibt hier völlig unklar. - Was ist mit «Antwort» gemeint? Die Antwort des Servers des abgeleiteten Kommunikationsdienstes, den der Kunde besucht hat, oder die Antwort des Kundengeräts auf eine Nachricht von diesem Kommunikationsdienst? - Was ist mit «eindeutig im Bereich der Anbieterin» gemeint? Die Formulierung ist auch hier unverständlich. - Wie soll man sich eine «Antwort von einem anderen Fernmeldedienst» vorstellen? Muss ein Internetprovider die Herkunft sämtlicher auf seinem Netz eintreffenden Datenpakete aufzeichnen und dem Dienst ÜPF auf Anfrage diese Aufzeichnungen herausgeben? Wie soll die gigantische Masse an Daten, die durch ein solches Logging anfällt, durch die Internetprovider gemanaged werden?

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<ul style="list-style-type: none"> - Was ist mit «letzter zugriffsrelevanter Aktivitäten» gemeint? Geht es hier um die durch Kunden des Internetproviders aufgerufenen AAKD und andere Internetangebote? Wie soll der Internetprovider wissen, ob eine durch den Kunden aufgerufene IP-Adresse zu einem überwachungspflichtigen AAKD gehört, oder allenfalls zu einem nicht überwachungspflichtigen Dienst? Muss er einfach den ganzen Verkehr aufzeichnen? Wie weit zurück gehen die «zugriffsrelevanten» Aktivitäten? Müssen alle Daten für sechs Monate aufbewahrt werden? - Abgesehen davon: Wo wäre die gesetzliche Grundlage im BÜPF für die vorgesehene inhaltliche Überwachung des Internetverkehrs? Das BÜPF selber regelt bisher ausschliesslich die Überwachung der Randdaten, nicht aber von Inhaltsdaten, und spätestens dann, wenn Randdaten en passant auch Auskunft über die vom Kunden abgerufenen Inhalte geben, handelt es sich dabei um Inhaltsdaten, deren Sammlung erst recht gesetzes- und verfassungswidrig wäre, nachdem schon das Sammeln reiner Randdaten als menschenrechtswidrig taxiert wurde.
17.	50a	Artikel streichen	<p>Art. 50a sieht neu vor, dass Anbieter verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Diese Pflicht gilt nicht mehr nur für FDA (Art. 26 BÜPF) oder ausnahmsweise für ausgewählte AAKD von hoher wirtschaftlicher Bedeutung (Art. 27 BÜPF), sondern soll nun vorgabemässig und ohne Differenzierung auf sämtliche Anbieter mit mehr als 5'000 Teilnehmern angewendet werden, womit wohl fast die gesamte Schweizer AAKD-Branche betroffen ist (kaum ein Produkt ist lebensfähig mit weniger als 5'000 Teilnehmern).</p> <p>Dies stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar.</p> <p>Diese Ausweitung ist nicht nur unverhältnismässig, sondern gefährdet aktiv nahezu die gesamte Schweizer IT-Branche: Indem de facto alle Anbieter vorgabemässig gezwungen werden, ihre Verschlüsselungssysteme für Behörden jederzeit entschlüsselbar zu gestalten, entstehen enorme Sicherheitsrisiken, denn Verschlüsselung ist wie eine Eierschale: Unversehrt ist sie stark, aber der kleinste Riss führt zu einer erheblichen Schwächung. Die betroffenen Systeme werden durch den vom Verordnungsgeber nun verpflichtend vorgesehenen Einbau von Hintertüren anfälliger für Hackerangriffe, Datenmissbrauch und Spionage. Dies widerspricht Art. 13 BV und dem diesen konkretisierenden Datenschutzgesetz, das den Schutz</p>

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>personenbezogener Daten ausdrücklich durch wirksame technische Massnahmen – insbesondere Verschlüsselung – vorschreibt. Eine durch den Anbieter aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung in jedem Fall.</p> <p>Genau eine solche Schwächung der Verschlüsselung wurde kürzlich vom Europäischen Gerichtshof für Menschenrechte im Fall PODCHASOV gegen Russland (33696/19) als Verstoss gegen Grundrechte gewertet. Art. 50a verstösst somit auch gegen geltendes Völkerrecht.</p> <p>Nebst diesem Verstoss gegen das Völkerrecht wird aber auch das Gebot der Verhältnismässigkeit aus Art. 36 BV nicht eingehalten, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Wie bereits bei Art. 16e, Art. 16f und Art. 16g erwähnt, müssen zuerst die einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.</p> <p>Zusätzlich, und wie bereits bei Art. 16d erwähnt, verhindert Art. 50a die effektive Erbringung von VPN-Diensten. Bei solch einem VPN kontrolliert der Betreiber sowohl den Eingangs- als auch den Endpunkt. Da die Kommunikation vom Endpunkt zu einer Webseite aufgrund der vorherrschenden Struktur im allgemeinen Internet nicht Ende-zu-Ende-verschlüsselt erfolgen kann, werden schon kleine VPNs (mit 5'000 Nutzern) dazu gezwungen ihre eigene Verschlüsselung zu entfernen und ihre Kunden zu überwachen. Da der Schutz der Privatsphäre der Nutzerinnen und Nutzer von VPNs just den Kernpunkt oder USP der Dienstleistung darstellt, werden Schweizer VPN-Anbieterinnen hierdurch am internationalen Markt übermässig benachteiligt, ja ihres eigentlichen Daseinszwecks beraubt.</p> <p>Wesentlich ist zudem, dass Anbieter von Mail- oder Messaging-Apps zwangsläufig die Nachricht in der App in einer menschenlesbaren Version anzeigen müssen, und dass an dieser Stelle die Ende-zu-Ende-Verschlüsselung notwendigerweise bereits entfernt ist. Der Wortlaut von Art. 50a lässt entgegen sämtlichen Beteuerungen des Dienstes ÜPF bereits anlässlich der letzten Revision der VÜPF weiterhin offen, ob eine Entfernung der Verschlüsselung auch an dieser Stelle gefordert werden können soll. Angesichts der seit Jahren erkennbaren Tendenz der Schweizer Überwachungsbehörden, die Anwendbarkeit des Überwachungsrechts laufend weiter auszudehnen und sich dabei nur durch Gerichte bremsen zu lassen, ist bei dieser Gelegenheit erneut die Klarstellung zu fordern, wonach die Entfernung von Verschlüsselungen, die erst in der Sphäre des Benutzers angebracht werden (wenngleich auch durch</p>

Threema.

Nr.	Artikel	Antrag	Begründung / Bemerkung
			Software der Anbieterin) nicht verlangt werden darf. Dies ist zumindest im erläuternden Bericht zu erwähnen. Der erneute Verzicht wäre nichts anderes als eine Einladung an die Überwachungsbehörden, die Einführung einer offensichtlich illegalen und vom BÜPF keineswegs vorgesehenen «Chatkontrolle» auf dem «Auslegungsweg» vorzunehmen.

Threema.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Artikel	Antrag	Begründung / Bemerkung
VD-ÜPF / OME-SCPT / OE-SCPT		
Art. 14 Abs. 3 VD-ÜPF	Streichung	Wie bereits bei Art. 16e bis 16f revVÜPF angesprochen, ist ein aktives Tätigwerden für alle AAKD (auch für solche mit 5'000 Nutzerinnen und Nutzer) unverhältnismässig und nicht wirtschaftlich tragbar. Der Absatz ist daher ersatzlos zu streichen.
Art. 14 Abs. 4 VD-ÜPF	Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten.»	Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der Unterworfenen AAKD massiv. Dies ist wie beschrieben weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.
Art. 20 Abs. 1 VD-ÜPF	Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f revVÜPF angesprochen ist ein aktives Tätigwerden für alle AAKD (auch für solche mit mehr als 5'000 Nutzerinnen und Nutzer) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.

Eidgenössisches Justiz- und Polizeidepartement EJPD

Herr Bundesrat Beat Jans

Informatik Service Center ISC-EJPD

Eichenweg 3

3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Vernehmlassungsantwort zur Teilrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrte Damen und Herren,

Mit grossem Interesse haben wir die Vernehmlassung zur Teilrevision VÜPF zur Kenntnis genommen. Unsere Organisation CH++ setzt sich unabhängig für eine nachhaltige, wohlhabende, handlungsfähige und sichere Schweiz ein – durch Wissenschaft und Technologie. Nach sorgfältiger Prüfung lehnen wir die vorgeschlagenen Änderungen ab und bitten um eine grundlegende Überarbeitung der Vorlage.

Angesichts der Tatsache, dass sich BÜPF-Vorlagen notorisch in einem politisch sehr sensiblen Bereich bewegen, halten wir vorliegenden Entwurf für ungenügend:

1. Unklarer Sicherheitsgewinn

Die Ziele der Vorlage sind nicht hinreichend ersichtlich oder nachvollziehbar. Zwar wird eine klarere Definition der Mitwirkungspflichtigen (MWP) angestrebt. Abgesehen davon, dass die Definitionen mit dieser Vorlage jedoch nicht einfacher werden, wird im erläuternden Bericht kaum dargelegt, welche Erleichterungen für die Strafverfolgung erreicht werden bzw. wo deren Probleme in der bisherigen Praxis mit den bisherigen Kategorien der MWP bestanden haben. Zwar wird darauf hingewiesen, dass der Ausschuss des beratenden Organs («Ausschuss FMÜ») die Vollzugstauglichkeit geprüft habe. Zu dessen Prüfpunkten und -erkenntnissen wird hingegen gar nichts dargelegt. So bleibt auch weitgehend unklar, wie man auf die 5000 Teilnehmenden als Untergrenze für AAKD mit reduzierten Pflichten gekommen ist.

2. Unzureichende Gewährleistung des Datenschutzes

Die vorgeschlagene Revision wirft erhebliche Bedenken hinsichtlich einer Ausweitung staatlicher Überwachungsmassnahmen auf, die potenziell weitreichende Auswirkungen auf die Privatsphäre und Grundrechte der Schweizer Bevölkerung haben könnte. Die neu vorgesehenen umfangreichen Speicher- und Identifikationspflichten stehen in einem Spannungsverhältnis zum Prinzip der Datenminimierung, das als wesentlicher Bestandteil im Datenschutzgesetz (Art. 6 Abs. 3 DSG) verankert ist. Diese Entwicklung gibt Anlass zur Sorge, da sie nicht nur Fragen bezüglich der persönlichen Freiheit und der informationellen Selbstbestimmung (Art. 13 BV) aufwirft, sondern auch eine sorgfältige Prüfung im Kontext international anerkannter Datenschutzstandards erfordert.

Zudem wäre es zielführend, wenn die offenbar durchgeführte Datenschutzfolgeabschätzung DSVA zugänglich wäre. Zwar wird auf eine durchgeführte DSVA hingewiesen: Ob und inwieweit deren Erkenntnisse in die Vorlage eingeflossen sind, bleibt jedoch offen¹.

2. Negative wirtschaftliche Auswirkungen

Die vorgesehenen Änderungen gefährden den Wirtschafts- und Innovationsstandort Schweiz erheblich. Insbesondere Unternehmen, deren Geschäftsmodelle auf starkem Datenschutz und Vertraulichkeit basieren, wie beispielsweise Proton und Threema, würden durch die Einführung übermässiger Mitwirkungspflichten massiv belastet. Dies könnte zur Abwanderung dieser und ähnlicher innovativer Firmen führen, was langfristig die technologische Wettbewerbsfähigkeit und Attraktivität der Schweiz für digitale Unternehmen nachhaltig beeinträchtigen würde.

3. Unverhältnismässigkeit und fehlender Sicherheitsgewinn

Die vorgeschlagenen Massnahmen bringen nachweislich keinen substanziellem Sicherheitsgewinn und sind unverhältnismässig. Es liegt kein überzeugender Nachweis dafür vor, dass bestehende Kompetenzen und Mittel der Strafverfolgungsbehörden unzureichend sind. Vielmehr stellt die Vorlage einen Eingriff in Freiheitsrechte dar, ohne dass der Schutz der Gesellschaft dadurch signifikant verbessert würde. Grundrechtseingriffe

¹ Vgl. demgegenüber DSVA zur Passenger Name Records von fedpol:
<https://www.fedpol.admin.ch/dam/fedpol/en/data/polizeizusammenarbeit/PNR/factsheet-pnr-dsfa.pdf.download.pdf/factsheet-pnr-dsfa-e.pdf>

müssen stets verhältnismässig und notwendig sein – beides trifft bei dieser Revision nicht zu.

4. Risikoerhöhung durch geschwächte Verschlüsselung und Datenvorräte

Besonders kritisch sehen wir die geplante Verpflichtung der Anbieter, Verschlüsselungen jederzeit aufheben zu können (Art. 50a VE-VÜPF). Dies reduziert die Sicherheit der Kommunikation deutlich, schafft neue Risiken für Cyberangriffe und Spionage und widerspricht jeglichem Bestreben, Cybersicherheit und Datenschutz zu stärken. Zudem birgt die Ausweitung der Vorratsdatenspeicherung grosse Risiken, ohne dass nachgewiesen wäre, dass diese Massnahme effektiv zur Strafverfolgung beiträgt. Ausserdem wird durch eine solche Regelung das Vertrauen der Kunden der Anbieter untergraben, da etwaige Verschlüsselungen durch den Anbieter bei Bedarf entfernt werden müssen, was den Zweck der Verschlüsselung wesentlich untergräbt.

Aus den genannten Gründen fordert CH++ eine **Rückweisung der vorgeschlagenen Revision und eine umfassende Überarbeitung der Vorlage, welche die Grundrechte, den Datenschutz und die Innovationsfähigkeit der Schweiz respektiert und bewahrt**. Wesentliche Eingriffe in Grundrechte dürfen nur auf Gesetzesebene erfolgen, um demokratische Legitimität und ausreichende öffentliche Debatte sicherzustellen.



**Stellungnahme von Swisscows AG zur Vernehmlassung betreffend der Revision des Bundesgesetzes
betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)**

Datum: 6. Mai 2025

Ort: Egnach, Schweiz

Sehr geehrte Damen und Herren

Als Schweizer Unternehmen, das sich seit 2014, seit seiner Gründung konsequent dem Schutz der Privatsphäre und der digitalen Selbstbestimmung verpflichtet hat, nehmen wir mit grosser Sorge die geplante Revision des BÜPF zur Kenntnis. Swisscows lehnt die geplante Ausweitung der digitalen Überwachung in der vorliegenden Form entschieden ab.

1. Gefährdung der digitalen Privatsphäre

Die geplante Gesetzesrevision sieht tiefgreifende Eingriffe in die digitale Kommunikation und die Freiheitsrechte der Bürgerinnen und Bürger der Schweiz vor. Insbesondere die geplante Möglichkeit zur flächendeckenden Überwachung verschlüsselter Kommunikation und der Einsatz von sogenannter „Govware“ stellen eine ernsthafte Bedrohung für die Grundrechte auf Privatsphäre und informationelle Selbstbestimmung dar. Als Anbieter einer anonymen Suchmaschine Swisscows und andere Alternativen, die zum Schutz von Privatsphäre dienen, sehen wir in solchen Massnahmen eine unverhältnismässige Ausweitung staatlicher Kompetenzen.

2. Unverhältnismässigkeit und Unklarheit der Massnahmen

Die Revision bleibt in zentralen Punkten vage und unbestimmt, etwa hinsichtlich der technischen Standards, der Kontrolle über den Einsatz von Überwachungstechnologien oder der konkreten Kriterien für deren Einsatz. Diese Unklarheiten bergen das Risiko von Missbrauch und führen zu einer erheblichen Rechtsunsicherheit – nicht nur für die Bevölkerung, sondern auch für Anbieter digitaler Dienste.

3. Falsches Sicherheitsgefühl

Ein übermässiges Vertrauen in Überwachungsmassnahmen kann zu einem trügerischen Sicherheitsgefühl führen. Wenn der Fokus einseitig auf Überwachung liegt, besteht die Gefahr, dass andere wichtige Bereiche der Sicherheitsarchitektur – wie Bildung, Prävention, dezentrale Schutzsysteme oder IT-Sicherheit – vernachlässigt werden. Sicherheit entsteht nicht durch Kontrolle allein, sondern durch ein ganzheitliches Konzept, das auch die Stärkung von Eigenverantwortung und technologischer Resilienz umfasst.

Swisscows AG

Bucherstrasse 2
9322 Egnach
Schweiz

Tel.: +41 (0) 716 667 931
Fax: +41 (0) 716 667 930
Email: info@swisscows.com



4. Innovationshemmnis für datenschutzfreundliche Technologien

Die neuen Anforderungen, insbesondere die Pflicht zur Umsetzung von Überwachungsschnittstellen durch Anbieter, führen zu einem erheblichen wirtschaftlichen und technischen Druck auf innovative Schweizer Unternehmen. Dies trifft insbesondere auch Anbieter wie Swisscows, die aus Überzeugung vor Überwachung schützen und auf eine Architektur setzen, die diesen Schutz dem Nutzer bietet. Solche Anforderungen widersprechen dem Ziel, einen digitalen Standort Schweiz zu fördern, der auf Vertrauen, Sicherheit und technologischem Fortschritt basiert.

Die geplante Gesetzesrevision gefährdet den Ruf der Schweiz als neutraler und sicherer digitaler Standort. Die Schweiz geniesst international ein hohes Ansehen als Land mit starkem Datenschutz und politischer Unabhängigkeit – ein entscheidender Standortvorteil für Unternehmen, die vertrauenswürdige digitale Dienste entwickeln. Mit der Einführung staatlich verordneter Überwachungsstrukturen droht dieser Vorteil verspielt zu werden. Die Schweiz riskiert, ihren Status als „digitaler Hort der Sicherheit“ zu verlieren – mit negativen Folgen für Innovation, Standortattraktivität und internationale Glaubwürdigkeit.

5. Demokratie lebt von der Freiheit, nicht von Überwachung

Swisscows ist überzeugt: Eine freie und demokratische Gesellschaft lebt vom Schutz der Privatsphäre – nicht von ihrer systematischen Aushebelung. Die aktuellen Vorschläge bewegen sich in Richtung präventiver Massenüberwachung und hebeln grundlegende rechtsstaatliche Prinzipien aus. Wir fordern das Parlament der Schweiz daher auf, die Revision grundlegend zu überarbeiten und einen echten Ausgleich zwischen Sicherheit und Freiheit zu gewährleisten.

Swisscows fordert den Verzicht auf jene Elemente der Gesetzesrevision, die eine generelle Ausweitung der digitalen Überwachung und den Zwang zur Umgehung von Verschlüsselungstechnologien bedeuten. Stattdessen braucht es eine klare, transparente und grundrechtskonforme Regulierung, die den hohen Stellenwert der digitalen Privatsphäre im 21. Jahrhundert anerkennt.

Mit freundlichen Grüßen

Andreas Wiebe

Gründer und CEO der Swisscows AG

www.swisscows.com

Swisscows AG

Bucherstrasse 2

9322 Egnach

Schweiz

Tel.: +41 (0) 716 667 931

Fax: +41 (0) 716 667 930

Email: info@swisscows.com



Swisscom (Schweiz) AG, Regulatory & Policy, 3050 Bern

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundeshaus West
CH-3003 Bern

per E-Mail: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Datum	6. Mai 2025	Seite
Ihr Kontakt	Diego Chocomeli / +41 79 757 76 58 / diego.chocomeli@swisscom.com	1 von 1
Thema	Vernehmlassung Teilrevision zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-VÜPF)	

Sehr geehrte Damen und Herren

Wir danken Ihnen für die uns im Rahmen der Anhörung zu den zwei Ausführungsbestimmungen (VÜPF, VD-VÜPF) des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) gebotene Möglichkeit zur Stellungnahme.

Gerne teilen wir Ihnen mit, dass sich Swisscom diesbezüglich **vollumfänglich der Stellungnahme und den Änderungsanträgen des Branchenverbandes asut anschliesst.**

Wir danken Ihnen für die Berücksichtigung der Anliegen der Telekommunikationsbranche und stehen für Rückfragen und Erläuterungen jederzeit zur Verfügung.

Freundliche Grüsse
Swisscom (Schweiz) AG

Diego Chocomeli
Senior Counsel, Rechtsanwalt

Hubert Wagner
LI Officer

zu Handen von
Bundesrat Beat Jans
Vorsteher, Eidgenössisches Justiz- und Polizeidepartement
Bundeshaus West
3003 Bern

Ausschliesslich per E-Mail an:
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Zürich, 6. Mai 2025

Vernehmlassungsantwort von swissICT zur Teilrevision des VÜPF

Sehr geehrter Herr Bundesrat Jans
Sehr geehrte Damen und Herren

Der Verband swissICT bedankt sich für die Möglichkeit der Einreichung einer Vernehmlassungsantwort zur Teilrevision des VÜPF gemäss Schreiben des EJPD vom 29. Januar 2025. Wir reichen unsere Stellungnahme hiermit fristgerecht ein.

swissICT ist der primäre Repräsentant des ICT-Werkplatzes Schweiz und der grösste Fachverband der Branche. swissICT verbindet über 2200 ICT-Unternehmen, Anwender-Unternehmen und Einzelpersonen. Der Verband fördert den Informationsaustausch, bündelt Bedürfnisse, publiziert die wichtigste Salärumfrage, formuliert ICT-Berufsbilder und ist Veranstalter des wichtigsten Informatik- und Businesspreises «Digital Economy Award». swissICT ist zudem Co-Initiant der Zertifizierungsinitiative «SI-Professional» zur Sicherstellung von Informatikkompetenz in der Arbeitswelt.

1. Einführung

swissICT hält die VÜPF für revisionsbedürftig und begrüßt deshalb zwar generell das Vorhaben, die VÜPF einer Revision zu unterziehen, lehnt aber deren Stossrichtung und die einzelnen im Revisionsentwurf vorgeschlagenen Anpassungen umfassend ab. Aus diesem Grund wird auf eine Vernehmlassung zu einzelnen Bestimmungen des Revisionsentwurfs verzichtet; stattdessen wird im Folgenden zum Entwurf generell Stellung bezogen und die ablehnende Haltung von swissICT begründet.

2. Gründe der Ablehnung durch swissICT

2.1 Ausweitung des Kreises mitwirkungspflichtiger Unternehmen ohne Notwendigkeit

Der Kreis mitwirkungspflichtiger Unternehmen (MWP) wird sowohl bei den Fernmeldedienstanbietern (FDA) wie auch bei den Anbietern abgeleiteter Kommunikationsdienste (AAKD) merklich ausgeweitet: Bei den FDA werden bei der Anzahl Überwachungsaufträgen nicht mehr zwischen FDA und AAKD unterschieden und bei der Umsatzgrenze neu der gesamte Unternehmens- oder gar Konzernumsatz berücksichtigt, wofür kein sachlicher Grund besteht. Auch bei den AAKD würde neu auf den Unternehmens- bzw. Konzernumsatz abgestellt, was einer Ausweitung gleichkommt.

Für solche Ausweitungen besteht kein Anlass – ganz im Gegenteil: Bereits heute konzentriert sich der ganz überwiegende Teil von Überwachungsmassnahmen auf sehr wenige und grosse MWP; die Erfassung zahlreicher weiterer MWP, die für Überwachungsmassnahmen letztlich bedeutungslos sind, führt zu erheblichem betrieblichem Mehraufwand und zu unnötigen Mehrkosten für jene MWP, bei denen es sich häufig um KMU handelt.

Auch die eben erst vom Dienst ÜPF publizierte Statistik zur Fernmeldeüberwachung vom 29. April 2025 macht deutlich, dass das gegenwärtige System der Überwachungsmassnahmen offenbar gut funktioniert und rege genutzt wird: So ist die Anzahl von Überwachungen und Auskünften gegenüber dem Vorjahr teils erheblich angestiegen. Die Zahlen sprechen nicht dafür, dass Überwachungsmassnahmen daran scheitern würden, dass der Kreis von MWP zu eng gefasst sei.

2.2 Starker Ausbau der Überwachungsmassnahmen und entsprechend weitgehende Eingriffe in die Grundrechte

Sowohl bei den FDA als auch bei den AAKD werden einzelne Überwachungsmassnahmen neu eingeführt und der Kreis der von bestimmten Überwachungsmassnahmen erfassten MWP massiv ausgebaut: Pflichten, die bislang nur für FDA bzw. AAKD mit weitergehenden Pflichten (also die höchste Stufe) galten, finden neu auch auf FDA bzw. AAKD mit reduzierten Pflichten (also die tiefere Stufe) Anwendung. Dies betrifft beispielsweise die Pflicht zur Aufbewahrung der für die Auskunftserteilung/Identifikation erforderlichen Daten während der Dauer der Kundenbeziehung und während 6 Monaten danach.

Neu eingeführt wird für AAKD mit vollen Pflichten unter anderem die Pflicht zur Lieferung des Inhalts und der Randdaten der Kommunikation der überwachten Person; bislang ist diese Pflicht auf die Lieferung der dem AAKD jeweils zur Verfügung stehenden Randdaten beschränkt und würde mit der Revision somit erheblich ausgeweitet.

Dies führt nicht nur zu teils erheblichen Mehraufwänden für die neu oder weitergehend erfassten MWP, sondern zu einem generellen und massiven Ausbau der staatlichen Überwachungsmöglichkeiten, was aus grundrechtlicher Optik stark kritisiert werden muss.

Hinzu kommt, dass mit der Ausweitung der Pflichten zahlreiche Geschäftsmodelle, bei denen der Persönlichkeits- und Datenschutz der Teilnehmer im Vordergrund stehen, faktisch verunmöglich oder jedenfalls stark erschwert werden.

2.3 Unklare Regelung der Ende-zu-Ende Verschlüsselung und Infragestellung zentraler Geschäftsmodelle

Mit der Revision würde eine für AAKD mit reduzierten oder vollen Pflichten eine neue Pflicht zur Entfernung von Verschlüsselungen eingeführt. Gemäss der neuen Bestimmung würden AAKD verpflichtet, von ihnen oder für sie angebrachte Verschlüsselungen zu entfernen, damit Überwachungsdaten ohne solche Verschlüsselungen geliefert werden können. Hiervon sollen gemäss Angaben des Diensts ÜPF und Ausführungen im Erläuternden Bericht zwar Ende-zu-Ende Verschlüsselungen zwischen Endkunden nicht betroffen sein; doch bleibt unklar, ob dies auch dann gilt, wenn diese Ende-zu-Ende Verschlüsselung vom AAKD angebracht würde.

Damit wird für Anbieter von Kommunikationsdiensten mit Ende-zu-Ende Verschlüsselung und für deren Kunden eine erhebliche Unsicherheit geschaffen. Zahlreiche Geschäftsmodelle, bei denen die Verschlüsselung von Kommunikation im Zentrum steht (z.B. VPN- oder Messenger-Dienste), können möglicherweise nicht weiterbetrieben werden.

2.4 Schwerfällige und undurchsichtige Vorlage

Die Revisionsvorlage muss insgesamt als schwerfällig und vor allem undurchsichtig bezeichnet werden, was nicht alleine der Komplexität der Materie geschuldet wird. Neben der bereits erwähnten Unsicherheit im Bereich der Ende-zu-Ende Verschlüsselung gilt dies namentlich bei der Einführung einer dritten Kategorie von MWP bei den AAKD, nämlich den AAKD mit minimalen Pflichten. Mit der Vorlage wird der Eindruck vermittelt, für jene Kategorie gälten gegenüber dem Status Quo weniger Pflichten – effektiv ist jedoch das Gegenteil der Fall: Die AAKD mit minimalen Pflichten übernehmen die Pflichten der bisherigen AAKD mit reduzierten Pflichten, während jene praktisch sämtlichen Pflichten der AAKD mit vollen Pflichten unterstellt werden (vgl. oben). Dies wird sowohl in der Vorlage selbst als auch in der synoptischen Darstellung der Änderungen und im erläuternden Bericht kaum transparent gemacht. Stattdessen wird die faktische Verschärfung als vermeintliche Erleichterung dargestellt.

2.5 Erhebliche Nachteile für den Wirtschaftsstandort Schweiz

Bei Umsetzung des Revisionsentwurfs und namentlich der zuvor angeführten Kritikpunkte würde in der Schweiz eine Überwachungsregelung eingeführt, die weit über jene des europäischen Auslands hinausgeht. Damit wären nicht nur erhöhte Grundrechtseingriffe verbunden, sondern auch erhebliche Mehraufwände und -kosten für die hiesige ICT-Industrie. Durch die Gefährdung oder Verhinderung in der Schweiz bewährter und erfolgreicher Geschäftsmodelle ist zudem eine Abwanderung von ICT-Unternehmen aus der Schweiz zu befürchten, was von einzelnen Exponenten auch bereits in Aussicht gestellt wurde. Dies alles kann nicht im Interesse des Wirtschafts- und ICT-Standorts Schweiz liegen und muss auch deshalb vermieden werden.

3. Fazit

Die Revisionsvorlage schiesst aus Sicht von swissICT weit über das Ziel hinaus und hätte eine in Europa ungesehene und sehr weitgehende Überwachungsregelung zur Folge. Die damit verbundenen Grundrechtseingriffe, die zusätzlichen Bürden für MWP und die damit verbundenen Wettbewerbsnachteile gegenüber dem Ausland, die fehlende Notwendigkeit und die damit verbundene generelle Schwächung des Wirtschafts- und ICT-Standorts Schweiz

sowie die mit der Vorlage einhergehende Unsicherheit und Intransparenz veranlassen swissICT, die Revisionsvorlage gesamthaft und in ihren einzelnen Anpassungen abzulehnen.

Entsprechend wird seitens swissICT die umfassende Zurückweisung der Revisionsvorlage beantragt und um Unterbreitung eines neuen und im Sinne der vorstehenden Kritikpunkte nachgebesserten Entwurfs ersucht. Gerne sind wir bereit, hier auch unterstützend mitzuwirken.

Wir bitten um gebührende Berücksichtigung unserer Vernehmlassungsantwort und stehen für Fragen und ergänzende Auskünfte gerne zur Verfügung.

Freundliche Grüsse

Im Namen von swissICT



Christian Hunziker
Geschäftsführer



Roland Mathys
Co-Leitung Rechtskommission



Sven Kohlmeier
Politikkommission

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Per Email an:
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 6. Mai 2025

Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat,
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die am 29. Januar 2025 eröffnete Vernehmlassung zur «Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)» und danken Ihnen für die Einladung zur Stellungnahme. Der Schweizerische Verband der Telekommunikation (asut) vertritt die Interessen der Telekommunikations-, Netzwerk- und Datacenter-Branche. Unsere Mitglieder, insbesondere die Anbieterinnen von Fernmeldediensten (FDA) und die Anbieterinnen von abgeleiteten Kommunikationsdiensten (AAKD) sind die vornehmlich direkt betroffenen Adressaten der vorgeschlagenen Anpassungen. Gerne nehmen wir die Möglichkeit zur Stellungnahme wahr und übermitteln Ihnen fristgerecht unsere Einschätzung.

Grundsätzliche Einschätzung zur Teilrevision der VÜPF

Mit der Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs am 1. März 2018 wurden verschiedene Kategorien von Mitwirkungspflichtigen geschaffen. Die Umsetzung dieser Kategorien in der VÜPF und in der Praxis gestaltete sich jedoch schwierig. So führte eine Referenz zum Fernmeldegesetz (FMG) dazu, dass bei verschiedenen Anbieterinnen unklar war, ob sie gemäss BÜPF als FDA oder als AAKD gelten. Zudem fehlte eine verbindliche Definition der abgeleiteten Kommunikationsdienste, so dass es für Anbieterinnen von Internetdiensten bis heute unklar ist, ob sie nun mitwirkungspflichtige AAKD gemäss BÜPF sind oder nicht. Erst die Revision des Fernmeldegesetzes vom 22. März 2019 brachte eine Klärung betreffend der FDA gemäss BÜPF. Hinsichtlich der AAKD fällte das Bundesgericht 2021 zwei wegweisende Entscheide. Mit der vorliegenden Revision der VÜPF sollen nun die Kategorien der FDA und der AAKD neu geregelt werden.

Angesichts der unbefriedigenden Umsetzung des BÜPF und der VÜPF in den vergangenen Jahren begrüßt asut die Absicht des Bundesrates, die verschiedenen Kategorien der Mitwirkungspflichtigen besser zu regeln. Die vorliegende Vernehmlassungsvorlage wird diesem Ziel jedoch nicht gerecht. Vielmehr würde der vorliegenden Entwurf der VÜPF (E-VÜPF) zu einer Zunahme der Anzahl betroffener Unternehmen führen, und es fehlen bei den AAKD weiterhin klare Definitionen, welche Dienste in den Geltungsbereich der Fernmeldeüberwachung fallen. Folgende Gründe führen zu unserer Einschätzung:

- Umsetzung nicht gesetzeskonform: Das BÜPF erlaubt eine Differenzierung der Pflichten von FDA und AAKD. Ausschlaggebend ist dabei gemäss BÜPF nicht das ganze Unternehmen. Vielmehr muss jeder einzelne Dienst hinsichtlich dessen wirtschaftlicher Bedeutung oder Benutzerschaft separat betrachtet werden. Zudem ist es auch möglich, dass ein Unternehmen sowohl FDA als auch AAKD ist, aber nur für die jeweiligen Dienste. Im Widerspruch dazu sieht der E-VÜPF jedoch vor, dass beim Umsatz zur Einstufung einer FDA oder einer AAKD nicht der Umsatz eines Dienstes betrachtet wird, sondern der Gesamtumsatz des Unternehmens (Konzernumsatz). Damit werden mehr FDA und AAKD die kritische Schwelle beim Jahresumsatz von CHF 100 Mio. überschreiten, was zu einer Zunahme der Anzahl Mitwirkungspflichtigen mit vollen Pflichten führt. Und dies obwohl ein Teil des Umsatzes gar nichts mit dem entsprechenden Fernmeldedienst oder abgeleiteten Dienste zu tun hat und somit zu keinem Zusatzznutzen für die Strafverfolgung führt.
- Unverhältnismässige Ausweitung der betroffenen Unternehmen: Gemäss der Statistik des Bundes zur Fernmeldeüberwachung wurden 2024 insgesamt 527'344 Auskünfte erteilt und 20'591 Überwachungen durchgeführt. 94% der Auskünfte und 99% der Überwachungen betrafen lediglich vier Unternehmen, die bereits heute den vollen Pflichten der VÜPF unterliegen. Die erweiterte Betrachtung beim Umsatz (d.h. Gesamtumsatz) sowie die Schwellenwerte bei den AAKD betreffend die Teilnehmer werden die Anzahl Unternehmen und Dienste, welche einer reduzierten oder vollständigen Pflicht unterliegen, deutlich erhöhen. Die betroffenen Unternehmen müssen dann entsprechende Prozesse und Systeme einführen und betreiben, was beträchtliche Mittel erfordern kann. Dieser Aufwand erscheint angesichts der wenigen zu erwartenden Auskünfte und Überwachungen unverhältnismässig, da der zusätzliche Aufwand kaum einem entsprechenden Nutzen gegenübersteht. An dieser Stelle sei zudem darauf hingewiesen, dass die Zunahme der Unternehmen mit vollen Pflichten auch einen entsprechenden Kontroll- und Überwachungsaufwand beim Dienst ÜPF nach sich ziehen wird.
- Fehlende Definitionen der AAKD: Der erläuternde Bericht enthält auf den Seiten 19 und 20 eine Beschreibung möglicher AAKD, weist aber gleichzeitig darauf hin, dass eine abschliessende Auflistung nicht möglich sei. Damit besteht eine grosse Rechtsunsicherheit für Anbieterinnen von internetbasierten Diensten, da weiterhin offen bleibt, welche Dienste den Auskunfts- oder Überwachungspflichten unterliegen. Die Auflistung im erläuternden Bericht ist zudem viel zu umfangreich und würde beispielsweise auch das Internet der Dinge (IoT) umfassen, wo Messwerte und Signale übertragen werden können. Angesichts der Bedeutung der Digitalisierung und der Vielzahl an Diensten und Applikationen, die in irgendeiner Form einen Datenaustausch zulassen, ist eine klare und international kompatible Definition jedoch zwingend notwendig. Im Zentrum sollen dabei interpersonale Kommunikationsdienste stehen.
- Unklare Auswirkungen im Geschäftskundenbereich: Vernetzung und Digitalisierung ermöglichen Unternehmen heute ein «Outsourcing» von Applikationen oder Betriebsbereichen. Beispielsweise wird die Buchhaltungssoftware nicht mehr im eigenen Rechenzentrum betrieben, sondern aus der Cloud bezogen oder ein Teil des Firmennetzwerks wird bei einer FDA zugekauft. Damit könnten firmeninterne Netze und Dienste, die heute betreffend Überwachung nur einer Duldungspflicht unterliegen, je nach Outsourcing-Partner plötzlich der vollen Überwachung unterstehen. Dies hätte gravierende Auswirkungen für die betroffenen Unternehmen. Die E-VÜPF trägt den Anforderungen und Entwicklungen im Geschäftskundenbereich nicht Rechnung und wird daher zu grossen Schwierigkeiten bei der Umsetzung und zu Rechtsunsicherheit führen.
- Schwächung des Digitalstandortes Schweiz: Cybersecurity und der Schutz der Privatsphäre haben in den letzten Jahren eine zentrale Bedeutung im Rahmen der Digitalisierung erhalten. Kommunikationsdienste sind heute weitgehend End-to-End-Verschlüsselt und nur die Benutzer selbst bzw. ihre Endgeräte sind in der Lage die Inhalte zugänglich zu machen. Die E-VÜPF fordert neu bei den AAKD eine stärkere Identifikation der Benutzer sowie die Aufbewahrung von Randdaten. Da jedoch viele AAKD ihre Dienste aus dem Ausland anbieten, werden nur jene Unternehmen von den Massnahmen betroffen sein, die ihren Sitz in der Schweiz haben. Dies führt zu Wettbewerbsnachteilen für Schweizer Unternehmen und schwächt den Digitalstandort Schweiz.

Aus diesen Gründen lehnt asut die vorliegende Teilrevision der VÜPF ab und fordert weitgehende Anpassungen, um einen gesetzeskonforme Umsetzung der Fernmeldeüberwachung sicherzustellen.

Detaillierte Überlegungen zu den einzelnen Artikeln der E-VÜPF

1. Abgrenzung der Kategorien von Mitwirkungspflichtigen (Art. 16a bis 16g E-VÜPF)

Eine zentrale Änderung der Revision betrifft die neuen Definitionen der FDA und AAKD mit den jeweiligen Unterkategorien. Damit sollen die im BÜPF definierten Kategorien von Mitwirkungspflichtigen besser in der Verordnung abgebildet werden. Die damit angestrebte Klarheit und Rechtssicherheit wird seitens asut grundsätzlich begrüßt.

Kritisch beurteilt asut jedoch die in der E-VÜPF definierten Unterscheidungskriterien, welche über das Ausmass der Auskunfts- und Überwachungspflichten entscheiden. Diese entsprechen in Teilen nicht den gesetzlichen Vorgaben des BÜPF und sind weder sachgerecht noch verhältnismässig.

Nicht einverstanden erklären kann sich asut insbesondere mit dem Vorschlag, wonach Unternehmen mit einem jährlichen Gesamtumsatz von CHF 100 Mio. stets den vollen Überwachungspflichten unterliegen sollen und dies vollständig unabhängig von der Bedeutung der jeweils angebotenen Dienstleistungen. Diese pauschale Regelung soll gemäss E-VÜPF sowohl für den Bereich der Fernmeldedienste (Art. 16b Abs. 1 Bst. b Ziffer 2 E-VÜPF) als auch für den Bereich der abgeleiteten Kommunikationsdienste (Art. 16g Abs 1 Bst. b E-VÜPF) zur Anwendung kommen. Damit steht der Entwurf im klaren Widerspruch zu den Vorgaben des BÜPF.

Entscheidendes Unterscheidungskriterium für die Bestimmung der Auskunfts- und Überwachungspflichten ist gemäss den Vorschriften des BÜPF einzig die Bedeutung des konkreten Dienstes und dies unabhängig davon, von welchem Unternehmen der Dienst angeboten wird. Dies geht bereits aus dem Wortlaut von Art. 26 Abs. 6 sowie Art. 27 Abs. 3 BÜPF hervor, wo explizit auf die Bedeutung der jeweiligen Dienstleistung Bezug genommen wird. Die Botschaft des BÜPF hält dazu unmissverständlich fest, dass jede Tätigkeit (bzw. Dienstleistung) jeweils unabhängig von der anderen betrachtet werden muss und deshalb ein Unternehmen je nach Tätigkeit, die es ausübt, ohne Weiteres mehreren Kategorien angehören kann und somit entsprechend diesen Tätigkeiten unterschiedlichen Überwachungspflichten unterliegt¹. Das Bundesamt für Justiz hielt in einer vom Generalsekretariat des EJPD beauftragten Einschätzung der Rechtslage dazu ergänzend fest, dass dieser Umgang mit verschiedenen Aktivitäten derselben Akteure in der Gesetzgebung üblich sei und sich die Pflichten von Akteuren in aller Regel auf die betreffende Aktivität und nicht auch noch auf andere Aktivitäten beziehen. Hat ein Unternehmen verschiedene Aktivitäten in mehreren Bereichen, so seien diese jeweils gesondert zu betrachten (Aktennotiz BJ zu den Kategorien gemäss BÜPF vom 9. Februar 2019).

Der Revisionsentwurf zielt nunmehr jedoch genau in die gegenteilige Richtung. Er betrachtet bei der Kategorisierung jeweils pauschal alle von einem Unternehmen angebotenen Dienste (vgl. Art. 16b Abs. 1 Best. b Ziffer 1 und Art. 16g Abs. 1 E-VÜPF) und unterstellt grössere Unternehmen ganz generell den vollen Überwachungspflichten. Mit anderen Worten dürfte in der Praxis kaum ein Unternehmen für unterschiedliche Dienste unterschiedlichen Überwachungspflichten unterliegen, wie dies der Gesetzgeber fordert.

Die vom Bundesrat in der E-VÜPF vorgenommene Einteilung bzw. Kategorisierung lässt sich weiter auch sachlich, aus der Optik der Strafverfolgung nicht rechtfertigen. Dies lässt sich am besten anhand eines Beispiels illustrieren: gemäss Art. 16g E-VÜPF würde ein neuer Cloud- oder Messagingdienst einer Start-Up-Tochterfirma eines grösseren Unternehmens (z.B. eine Versicherungsgesellschaft mit CHF 500 Mio. Umsatz) mit 50 Teilnehmern als AAKD mit vollen Überwachungspflichten eingestuft, während dieselben Dienste eines mittelgrossen Unternehmens mit CHF 90 Mio. Umsatz und 900'000 Teilnehmern gemäss Art. 16f E-VÜPF lediglich den reduzierten Überwachungspflichten unterliegen würde. Ein solches Ergebnis ist offensichtlich stossend und es kann schlichtweg nicht im Interesse der Strafverfolgung liegen, dass Dienste von sehr untergeordneter Bedeutung strenger überwacht werden müssen als Dienste mit einer relevanten Anzahl von Nutzerinnen und Nutzern. Für die Strafverfolgung von Relevanz ist nicht die Umsatzgrösse eines Unternehmens oder die Frage, ob ein Unternehmen allenfalls bereits einen anderen Telekommunikationsdienst anbietet, sondern die Bedeutung des konkreten Dienstes und dieser spiegelt sich gemäss BÜPF in der wirtschaftlichen Bedeutung sowie der Benutzerschaft wider.

Zusätzlich berücksichtigt die E-VÜPF die Anzahl der Überwachungsaufträge bei der Beurteilung, ob eine FDA nur reduzierten oder den vollen Pflichten unterliegt. Bei den AAKD hingegen, soll die Anzahl Auskunftsgesuche und Überwachungsaufträge nicht mehr berücksichtigt werden. Aus Sicht asut sind diese Anpassungen nicht korrekt. In der Ratsdebatte zum BÜPF führte die zuständige Bundesrätin damals aus,

¹ Vgl. [Botschaft zum BÜPF, BBI 2013, S. 2707](#).

dass die Bedeutung eines Dienstes für die Strafverfolgung selbstverständlich ein Kriterium sein soll, auch wenn es nicht namentlich im Gesetz erwähnt wird. Damit soll verhindert werden, dass Unternehmen in Auskunfts- oder Überwachungssysteme investieren müssen, obwohl dafür seitens der Strafverfolgung kein genügend grosser Bedarf besteht. Daher sollen diese Kriterien auch bei den AAKD zur Anwendung kommen. Zudem soll die Relevanz für die Strafverfolgung kumulativ zur wirtschaftlichen Bedeutung oder Benutzerschaft berücksichtigt werden. Eine FDA würde daher als FDA mit reduzierten Pflichten gelten, wenn sie eine der beiden Kriterien nicht überschreitet.

Weiter weisen wir darauf hin, dass die Aufwände für die Implementierung von Überwachungsmassnahmen grossmehrheitlich jeweils pro (neuen) Dienst anfallen. Es wäre deshalb unverhältnismässig ein Unternehmen gleich am Tag Eins bei der Lancierung eines neuen Dienstes einer vollständigen, aufwändigen und kostenintensiven Überwachungspflicht zu unterstellen, nur weil das Unternehmen eine bestimmte Grösse hat oder allenfalls bereits über einen anderen etablierten Dienst verfügt. Ob sich neue Angebote im Markt erfolgreich durchsetzen werden, ist bekanntlich höchst ungewiss und entsprechend wird sich ein solches Unternehmen zweimal überlegen, ob sich diese erhöhten Investitionen in neue Dienste lohnen. Die vorgesehene Regulierung dürfte deshalb zusätzlich eine innovations- und investitionsemmende Wirkung entfalten. Dies gilt es aus Sicht der Branche zwingend zu vermeiden.

Vor diesem Hintergrund, stellt asut den Antrag, bei der Kategorisierung der Mitwirkungspflichtigen und der entsprechenden Einstufung der Auskunfts- bzw. Überwachungspflichten konsequent und einzig auf die Bedeutung der einzelnen Dienste abzustellen. D.h. massgebend ist – neben der oben erwähnten Anzahl Auskunftsgesuche oder Überwachungsaufträge – der Umsatz eines Dienstes bei den FDA sowie der Umsatz eines Dienstes oder die Anzahl Teilnehmer eines Dienstes bei den AAKD. Sollte der Verordnungsgeber diese Abgrenzungskriterien wider Erwarten jedoch als nicht ausreichend ansehen, dann müsste alternativ auf einen Jahresumsatz von CHF 100 Mio. der betreffenden Dienstleistung abgestellt werden: Bei den FDA beispielsweise auf die entsprechenden Jahresumsätze gemäss Fernmeldestatistik des Bundes. Auf den Umsatz des gesamten Unternehmens abzustellen hat Willkürcharakter und entspricht, wie oben dargelegt, weder dem Willen des Gesetzgebers noch lässt sich dieses Abgrenzungskriterium sachlich rechtfertigen.

Zusätzlich sollen, wie oben erläutert, die Anzahl Auskunftsgesuche oder Überwachungsaufträge als kumulatives Kriterium bei der Einstufung eines FDA oder einer AAKD zur Anwendung kommen. D.h. nur wenn ein FDA die Umsatzschwelle und gleichzeitig die festgelegte Anzahl Überwachungsaufträge überschreitet, gilt er als FDA mit vollen Pflichten. Ansonsten als FDA mit reduzierten Pflichten. Die Anzahl massgeblicher Überwachungsaufträge (bzw. Auskunftsgesuchen bei den AAKD) soll dabei massvoll erhöht werden, da auch die Anzahl Auskünfte und Überwachungen in den letzten Jahren deutlich zugenommen haben.

Bei den AAKD soll eine neue Abstufung der Pflichten eingeführt werden. Davon verspricht sich der Bundesrat eine KMU-freundliche Umsetzung des BÜPF im Bereich der AAKD. In der Praxis wird dieses Ziel jedoch nicht erreicht. Die Anzahl von 5'000 Benutzern ist im Zeitalter von Apps und Social-Media viel zu tief angesetzt und wird dazu führen, dass eine grosse Anzahl von Diensten den zusätzlichen Pflichten unterliegen. Zu diesen Pflichten gehört insbesondere die Identifikation der Teilnehmer, was heute bei vielen Anwendungen nicht dem Kundenbedürfnis entspricht. Betroffene Schweizer Dienste hätten daher im internationalen Wettbewerb gravierende Nachteile gegenüber ausländischen Diensten. Die Regelung ist zudem ungenügend, da weiterhin eine klare und eindeutige Definition fehlt, welche Dienste überhaupt als abgeleitete Dienste gemäss E-VÜPF gelten sollen. Die Aufzählung im erläuternden Bericht geht weit über die interpersonalen Kommunikationsdienste hinaus, welche in den europäischen Ländern der Überwachung unterliegen. Dies führt faktisch dazu, dass eine Vielzahl von Diensten, Smartphone-Apps etc. erweiterten Pflichten unterliegen und die Anbieter entsprechende Anpassungen an ihren Diensten und Systemen vornehmen müssen. Geradezu KMU-unfreundlich ist die Tatsache, dass der «Upgrade» zu AAKD von Verordnung wegen stattfindet, d.h. die betroffenen Unternehmen erhalten keine Verfügung. Mangels eindeutiger Definition eines AAKD führt dies zu grosser Rechtsunsicherheit bei den betroffenen Unternehmen. Es soll daher geprüft werden, ob die neue Kategorie der AAKD mit reduzierten Pflichten gemäss BÜPF überhaupt zulässig ist. Falls dies zutrifft, soll der Schwellenwert hinsichtlich grosser Benutzerschaft deutlich angehoben werden. Zur Bestimmung des Schwellenwertes schlagen wir vor, dass der Bund zuerst in einer Marktstudie den Kreis der betroffenen Unternehmen abklärt.

2. Identifikationspflichten im Bereich der WLAN-Zugänge (Art. 16h und 19 E-VÜPF)

asut hat Verständnis, dass aus Gründen der Praktikabilität öffentliche WLAN-Zugänge nur noch ab einer bestimmten Grösse als «professionell betrieben» gelten sollen (Art. 16h Abs. 2 E-VÜPF). Nicht nachvollziehen können wir jedoch, dass die bestehende Definition gemäss WLAN-Merkblatt des Dienstes ÜPF² nicht übernommen wurde. Dort gelten nur mehrere WLAN-Zugänge an unterschiedlichen Standorten als professionell betrieben. Gemäss E-VÜPF hingegen würde bereits ein einzelner WLAN-Zugang der mehr als 1'000 Verbindungen aufbauen kann, als professionell eingestuft. Heute erhältliche Consumer-Geräte sind bereits in der Lage mehr als 500 Verbindungen aufzubauen. D.h. hätte jemand zwei Accesspoints (z.B. mehrstöckiges Einfamilienhaus, Büro) mit Gastzugang, dann wären diese Zugänge gemäss VÜPF bereits professionell betrieben und würden entsprechenden Pflichten unterliegen. Bei der technischen Entwicklung ist davon auszugehen, dass in kurzer Zeit auch ein einzelner WLAN-Zugang mehr als 1'000 Verbindungen herstellen kann und damit wäre fast jeder private oder geschäftliche WLAN-Accesspoint mit Gastzugang der Überwachung unterstellt.

Verschärfend kommt hinzu, dass künftig offenbar die FDA, welche den zugrundeliegenden Internetzugang sicherstellt, und nicht die natürliche oder juristische Person, welche ihren Internetzugang Dritten mit ihrem WLAN zur Verfügung stellt bzw. die eigentliche Anbieterin des öffentlichen WLAN-Zugangs (PZD) für die Identifikation der Endbenutzerinnen- und -benutzer zuständig zeichnen soll (Art. 19 Abs. 2 E-VÜPF).

Entgegen den Verlautbarungen in den Erläuterungen zur E-VÜPF handelt es sich hierbei um eine sehr weitreichende Änderung, für welche jegliche Begründung fehlt. Gemäss Ziffer 5.1 des aktuellen Merkblatts WLAN vom Dienst ÜPF hat heute richtigerweise diejenige Anbieterin, welche den öffentlichen Zugangspunkt betreibt oder (in ihrem Auftrag) durch einen Dritten betreiben lässt, die Pflicht zur Identifikation der Endbenutzerinnen und -benutzer. Gemäss den Ausführungen im Merkblatt ist dabei insbesondere entscheidend, wer konkret gegenüber diesen Endbenutzerinnen- und -benutzer als Anbieterin des öffentlichen WLAN-Zugangs auftritt³.

Diese Regelung ist nach Ansicht von asut die einzige praktikable und sachgerechte Lösung, weil nur die Anbieterin des öffentlichen, professionell betriebenen WLAN-Zugangs (bzw. die Person, die ihren Zugang Dritten zur Verfügung stellt), den Zugang auf die entsprechende Service-Infrastruktur direkt oder allenfalls mit Hilfe ihres technischen Dienstleisters kontrollieren kann. Nur die PZD, die gegenüber den WLAN-Endnutzenden als Vertragspartnerin bzw. Dienstleisterin auftritt, kann diese gemäss den Vorgaben des VÜPF identifizieren.

Die FDA, welche im Hintergrund einzige den dem PLWAN zugrundeliegenden Internetzugang zur Verfügung stellt, steht demgegenüber in keinem Dienstleistungsverhältnis zu den Endbenutzerinnen und -benutzer des WLAN-Zugangs. Sie ist nicht die Anbieterin dieses Dienstes und hat entsprechend auch keine Kenntnis davon, wer allenfalls den PWLAN-Service der PZD nutzt. Die Internetzugangsanbieterin kann ganz grundsätzlich auch keine wirksame technische Kontrolle darüber ausüben, für welche Zwecke ihre Kundinnen und Kunden die Internetzugänge einsetzen und wem sie Zugang auf eine PWLAN-Einrichtung gewähren. Der Internetzugang funktioniert für die daran angeschlossenen Services vielmehr transparent. Wenn als Beispiel an einem Internetzugang eine Infrastruktur für E-Mails betrieben wird, kann der Zugang zu den E-Mail Accounts nicht am Internetzugang kontrolliert werden. Der Zugang zu den E-Mail Accounts wird vielmehr in der Service-Infrastruktur (E-Mail Server) kontrolliert. Analog verhält es sich bei den professionell betriebenen öffentlichen WLAN-Zugängen. Nur der Gatekeeper der WLAN-Infrastruktur und nicht der Gatekeeper der zugrundeliegenden Internetzugang kann eine Zugangskontrolle ausüben. Die reine Internetzugangsanbieterin ist mit anderen Worten schlichtweg nicht in der Lage, Endnutzerinnen und Endnutzer eines WLAN-Zugangs zu identifizieren. Davon ausgenommen sind selbstredend diejenigen Fälle, wo die Internetzugangsanbieterin ebenfalls den öffentlichen WLAN-Zugang anbietet, d.h. sowohl als FDA (Internetzugangsanbieterin) als auch als PZD agiert.

Vor diesem Hintergrund ist es auch offensichtlich, dass eine reine Internetzugangsanbieterin unmöglich prüfen kann, ob eine PZD auf ihren WLAN-Service-Einrichtungen kumuliert den Schwellenwert von mehr als 1'000 Endnutzerinnen und Endnutzer überschreitet und somit als professionelle Betreiberin i.S. von Art. 16h E-VÜPF eingestuft werden muss. Wie dargelegt, kontrolliert einzige die PZD ihre WLAN-Zugänge und bestimmt die darauf gewährten (Benutzer-)Kapazitäten. Weiter kann ein PZD oder sein technischer Dienstleister die Internetanschlüsse für die einzelnen WLAN-Zugänge ohne weiteres bei verschiedenen Internetzugangsanbieterinnen beziehen (z.B. Wlan1 in Basel mit einer Kapazität von 600 bei FDA1 und Wlan2 in

² [Merkblatt WLAN](#) vom Dienst Überwachung des Post- und Fernmeldeverkehrs vom 1. März 2018.

³ Diese sich am wirtschaftlichen Dienstleistungsbegriff orientierte Definition gilt auch für die Festlegung des Begriffs Anbieterin von Fernmeldediensten (FDA). FDA ist, wer gegenüber den Kunden als Dienstleisterin/Vertragspartnerin auftritt (Vgl. [Faktenblatt zur Registrierung als FDA](#)).

Zürich mit einer Kapazität von 700 in Zürich bei FDA2). Eine FDA kann entsprechend auch aus diesem Grunde gar nicht feststellen, ob ein PZD in der Praxis ein professionelles WLAN mit mehr als 1'000 Endbenutzerinnen und -benutzer betreibt.

Gemäss E-VÜPF sollten neu Internetzugangsanbieter bzw. FDA im Ergebnis für etwas in die Verantwortung genommen werden, für das sie in der Praxis faktisch gar keine Kontrolle ausüben und deshalb auch keine Verantwortung übernehmen können. Eine solche Regelung ist offensichtlich stossend und systemfremd. Dies ergibt sich im Übrigen direkt aus Art. 2 Bst. e BÜPF, wo die PZD als eigenständige mitwirkungspflichtige Personen definiert sind. Gemäss dem Vorschlag in der E-VÜPF würden die PZD aber schlichtweg keinerlei gesetzlichen Mitwirkungspflichten unterliegen, was nicht die Absicht des Gesetzgebers war.

Nach Ansicht von asut ist im neuen Art. 19 E-VÜPF zu präzisieren, dass sich die PZD, d.h. die jeweiligen Anbieterinnen von professionell betriebenen öffentlichen WLAN-Zugängen, für die Identifikation aller Endbenutzerinnen und -benutzer verantwortlich zeichnen.

3. Weitere Änderungsanträge

3.1. FDA (Art. 16a E-VÜPF)

Wie eingangs bereits erwähnt, wurde mit der FMG-Revision vom 22. März 2019 eine Referenz zwischen dem BÜPF und dem FMG gestrichen. Damit sollte sichergestellt werden, dass OTT-Anbieter im Rahmen der Fernmeldeüberwachung als AAKD eingestuft werden und nicht als FDA. Die eigentliche Definition eines FDA blieb davon unberührt. Entscheidend ist bei der Einstufung als FDA, wer gegenüber der Kundin oder dem Kunden die Verantwortung für die fernmeldetechnische Übertragung von Informationen übernimmt. Dies ist daher von Bedeutung, da beim Betrieb eines öffentlichen Fernmeldenetzes auf der technischen Ebene eine Vielzahl von Unternehmen involviert sein können. Nach Art. 16a Abs.1 Bst. a E-VÜPF gilt aber auch als FDA, wer ein öffentliches Fernmeldenetz betreibt. Dies können für dasselbe Netz auch mehrere Unternehmen sein. Damit würde eine unnötige Duplizierung der Pflichten gemäss E-VÜPF für ein und dasselbe öffentliche Fernmeldenetz entstehen. Daher soll Art. 16a Abs. 1 Bst. a E-VÜPF ersatzlos gestrichen werden.

3.2. Teilnehmer- und Benutzeridentifikation (Art. 19 Abs. 1 E-VÜPF)

Neu soll eine Teilnehmer- und Benutzeridentifikation nicht nur für FDA, PZD sowie Wiederverkäuferinnen (Art. 2 Lit. f BÜPF) gelten, sondern auch für die neue Kategorie der AAKD mit reduzierten Pflichten. Da der Schwellenwert für diese AAKD mit 5'000 Benutzern sehr tief angesetzt ist, führt dies faktisch zu einer flächendeckenden Pflicht zur Identifikation von Teilnehmern und Benutzern bei den AAKD. Gemäss erläuterndem Bericht (S.30/31) kann diese mittelbare Identifikation beispielsweise mittels SMS-Zugangscode auf das Handy oder den Autorisierungsdaten bei Kreditkartenzahlungen erfolgen. Dabei erfolgt die Identifikation in der Regel nur bei der erstmaligen Aktivierung eines Dienstes und nicht laufend. Die aufgeführten Identifikationsmittel sind jedoch für viele abgeleitete Kommunikationsdienste nicht praktikabel oder werden von Benutzerinnen und Benutzern nicht geschätzt. Als Alternative schlägt der erläuternde Bericht daher eine Identifikation durch die Auskunftstypen IR_59_EMAIL_LAST und IR_60_COM_LAST vor. Dies hätte zur Folge, dass AAKD mit reduzierten Pflichten in ein Auskunftssystem investieren müssen, obwohl sie noch gar nicht der automatisierten Auskunftspflicht unterstehen. Zudem ist es nicht nachvollziehbar, dass bei Kreditkarten eine einmalige Identifikation des Teilnehmers ausreicht, bei der Identifikation über IR_59 und IR_60 hingegen eine permanente Identifikation notwendig ist.

Diese Ausführungen zeigen deutlich die Mängel, welche durch die Einführung der neuen Kategorie der AAKD mit reduzierten Pflichten entstehen. Daher soll in Art. 19 Abs. 1 die Pflicht für diese AAKD gestrichen werden. Entsprechend sollen die AAKD mit reduzierten Pflichten auch in Art. 21 Abs. 1 Bst. a gestrichen werden.

3.3. Auskunftstypen mit flexibler Namenssuche (Art. 27 Abs. 3 E-VÜPF)

Gemäss der heutigen Regelung ist die flexible Suchfunktion für Namen von natürlichen Personen möglich. Diese flexible Suchfunktion wurde eingeführt, um ein in der Praxis auftretendes Problem bei der Eingabe

von Personennamen zu beheben: Insbesondere bei komplizierteren Namen oder solchen mit anderen Zeichensätzen werden teilweise fehlerhafte bzw. nicht ganz korrekte Eingaben getätigt.

Die nun vorgeschlagene Erweiterung auf juristische Personen lässt sich nach Ansicht von asut demgegenüber nicht rechtfertigen. Erstens sind den FDA im Bereich der juristischen Personen keine ähnlichen, regelmässig auftretenden Probleme bei der Sucheingabe bekannt, und auch in den Erläuterungen wird hierzu nichts ausgeführt. Im Gegensatz zur Personensuche stehen den Strafverfolgungsbehörden bei der Firmensuche ausserdem öffentlich zugängliche Hilfsmittel zur Verfügung, mit denen flexibel gesucht werden kann (z.B. Zefix). Den Strafverfolgern kann durchaus zugemutet werden, eine entsprechende Kontrolle bzw. Suche bei Bedarf selbst durchzuführen. Vermutungsweise wird dies teilweise bereits gemacht. Die flexible («nice to have»-) Suchfunktion nunmehr auf die Mitwirkungspflichtigen abzuwälzen ist vor diesem Hintergrund unnötig und unverhältnismässig. Auch an dieser Stelle gibt asut zu bedenken, dass die Implementierung von neuen technischen Funktionen jeweils bei allen betroffenen Anbietern mit einem nicht unerheblichem Entwicklungsaufwand und entsprechenden Kosten verbunden ist.

asut stellt vor diesem Hintergrund den Antrag, auf die vorgeschlagene Änderung von Art. 27 Abs. 2 E-VÜPF zu verzichten.

3.4. IR_8_IP_NAT: Benutzeridentifikation bei IP Adressen mit NAT (Art. 38 Abs. 2 E-VÜPF)

Der Wortlaut von Art. 38 Abs. 2 VÜPF wird materiell nicht angepasst und auch gemäss den Erläuterungen soll bei diesem Auskunftstyp inhaltlich nichts geändert werden. In denselben Erläuterungen wird jedoch ergänzend angemerkt, dass die beauftragten Mitwirkungspflichtigen eine mögliche Toleranzabweichungen der Systemuhren bei der Suche und Identifikation der Benutzer, der Urheberschaft oder der Herkunft zu berücksichtigen haben.

Eine solche Berücksichtigung stellt nach Ansicht von asut eine materielle Änderung dar, die seitens der FDA in dieser Form jedoch nicht umgesetzt werden kann. Die Strafverfolger erhalten die Informationen für Aufträge dieses Auskunftstyps (öffentliche Source IP-Adresse, Source Port, Zeitpunkt) aus Logfiles, die ihnen von den Content-Anbietern im Internet (Chat-Services, Online-Shops, Webseiten etc.) zur Verfügung gestellt werden. Die Herkunft und Details zur Urheberschaft der Daten sind bei der Übermittlung des Auftrags an die Mitwirkungspflichtigen jedoch nicht vorgesehen. Ihnen ist die Herkunft der Daten, die dem Auftrag zu Grunde liegen, die dort vorhandene technische Infrastruktur und die für die Synchronisation der Zeit verwendeten Methoden und Funktionen somit nicht bekannt. Ohne diese Informationen ist eine Einschätzung von Toleranzabweichungen der Systemuhren bei den FDA jedoch nicht möglich.

Vor diesem Hintergrund ist diese Anmerkung in den Erläuterungen zu Abs. 2 («Ergänzend zu den Ausführungen [...] berücksichtigen hat») zu streichen.

3.5. IR_58_IP_Intersect: Benutzeridentifikation durch Schnittmengenbildung (Art. 38a E-VÜPF)

asut kann sich mit diesem neuen Auskunftstyp einverstanden erklären. Der Zweck des Auskunftstyps wird im Artikel allerdings aus Sicht asut nicht korrekt wiedergegeben. Die Schnittmengenberechnung kommt vor allem zur Anwendung, wenn die Strafverfolger von ihren Quellen keine Informationen zur öffentlichen Quell-Portnummer erhalten. In solchen Fällen kann eine Schnittmengenberechnung von mehreren Internetverbindungen das Fehlen der öffentlichen Quell-Portnummer kompensieren und trotzdem zu einem Resultat führen. Folgerichtig ist deshalb die Angabe der öffentlichen Quell-Portnummer, der öffentlichen Ziel-IP-Adresse und der Ziel-Portnummer nicht notwendig.

Weiter sieht asut Anpassungsbedarf bei zwei Anmerkungen in den Erläuterungen:

- In Absatz 2 der Erläuterungen wird darauf hingewiesen, dass wenn ein Auskunftsgesuch IR_7_IP nicht zu einem eindeutigen Ergebnis führt und auch ein Auskunftsgesuch IR_8_IP_NAT nicht erfolgreich ist, eine Schnittmengenbildung aus den Mehrfachergebnissen zu einer eindeutigen Identifikation führen kann. Dieser Text suggeriert eine nicht vorhandene Verbindung zwischen IR_7_IP und IR_8_IP_NAT. Der Zusammenhang, der hier dargestellt wird, existiert in dieser Form nicht und entsprechend sollte der Hinweis auf das Auskunftsgesuch IR_7_IP gestrichen werden. Darüber hinaus kommt die Schnittmengenberechnung wie oberhalb erwähnt vor allem zur Anwendung, wenn die Strafverfolger von ihren Quellen keine Informationen zur öffentlichen Quell-Portnummer erhalten. Es besteht also auch kein direkter Zusammenhang mit nicht erfolgreichen Auskunftsgesuchen IR_8_NAT. Darum sollte auch dieser Teil des Textes in der Erläuterung gestrichen und der Zweck

des IR_58_IP präzisiert werden.

- Analog zu den Ausführungen bei Art. 39 E-VÜPF fehlen den FDA auch hier die nötigen Informationen, um eine Einschätzung zu möglichen Toleranzabweichungen der Systemuhren berücksichtigen zu können. Deshalb ist auch hier der entsprechende Hinweis in den Erläuterungen zu Abs. 3 («Für diesen Zeitpunkt gilt, wie auch bei Artikel 38 Abs. 2 [...] zu berücksichtigen hat») zu streichen.

3.6. Entfernung von Verschlüsselungen (Art. 50a E-VÜPF)

Gemäss Art. 26 BÜPF sind FDA verpflichtet, im Rahmen von Überwachungen die von ihnen angebrachten Verschlüsselungen zu entfernen. Diese Pflicht kann auch AAKDs mit erweiterten Pflichten gemäss Art. 27 BÜPF auferlegt werden. Neu verlangt jedoch Art. 50a E-VÜPF, dass diese Verpflichtung auch für AAKD mit reduzierten Pflichten gilt. Damit müssten alle AAKD mit mehr als 5'000 Benutzern die Entfernung der von ihnen angebrachten Verschlüsselung vorsehen. Damit geht die E-VÜPF über den gesetzlichen Rahmen der BÜPF hinaus und es zeigt sich erneut, dass die neu geschaffene Kategorie der AAKD mit reduzierten Pflichten nicht gesetzeskonform ist.

Art. 50a verlangt von den AAKD, dass sie ihre Dienste so gestalten, dass die Verschlüsselung jederzeit entfernt werden kann. Da die Verschlüsselung heute ein zentrales Sicherheitselement vieler abgeleiteter Dienste ist, betrifft dies nicht nur die AAKD mit vollen oder reduzierten Pflichten, sondern in der Praxis alle AAKD. Denn kein Unternehmen würde einen Dienst ohne diese Anforderung gemäss Art. 50a konzipieren und einführen, nur um beim Überschreiten eines Schwellenwertens die Sicherheitsfunktionen des Dienstes grundlegend anzupassen. Da die Möglichkeit, eine Verschlüsselung zu entfernen, das Sicherheitsniveau eines Dienstes schwächen kann, führt Art. 50a insgesamt zu negativen Auswirkungen auf die Cyber-Security der Schweiz. Zudem bleibt ungeklärt, welche Auswirkungen Art. 50a auf Verschlüsselungen hat, die durch den AAKD gar nicht mehr entfernt werden können (z.B. asymmetrische Verschlüsselungen) und ob die Anwendung dieser Verschlüsselungen gemäss E-VÜPF überhaupt noch zulässig wären. Der Geltungsbereich von Art. 50a soll daher auf FDAs sowie AAKD mit vollen Pflichten beschränkt werden.

3.7. RT_61_NA_CC-Trunc_IRI: Echtzeitüberwachung von Randdaten und gekürzten Inhalten bei Netzzugangsdiensten (Art. 55a E-VÜPF)

Dieser neue Überwachungstyp ist grundsätzlich eine Nachbildung des bereits existierenden Überwachungstyps gemäss Art. 55 VÜPF mit dem einzigen Unterschied, dass die Mitwirkungspflichtigen einen Teil der in Echtzeit aufgezeichneten Inhaltsdaten wieder aussortieren müssen. Welche Daten bzw. IP-Pakete entfernt bzw. geliefert werden müssen, wird dabei von der anordnenden Strafverfolgungsbehörde bestimmt.

Diese vorgesehene Aussonderungspflicht durch die Mitwirkungspflichtigen ist problematisch und würde eine systemwidrige Zäsur in die bewährte, gesetzlich vorgegebene Aufgabenteilung darstellen.

Das grundsätzliche Anliegen der Strafbehörden, nicht immer sämtliche angefallenen Daten zu erhalten, ist nachvollziehbar und sachlich gerechtfertigt. Mitunter lassen sich bei grossen Datenmengen die tatsächlich relevanten Daten für die Strafverfolger nur schwer auswerten.

Dieses Anliegen ist jedoch bereits auf Gesetzesstufe klar und abschliessend adressiert. Gemäss Art. 17 Bst. g BÜPF gehört es nämlich zu den Aufgaben des Dienstes ÜPF, auf Ersuchen der anordnenden Behörde eine allfällige Sortierung vorzunehmen und bestimmte Daten aus dem Datenfluss herauszufiltern. Diese Aufgabe fällt somit und entgegen der in Art. 55a E-VÜPF vorgeschlagenen Regelung dem Dienst ÜPF und nicht den Mitwirkungspflichtigen zu. Aus den Gesetzesmaterialien geht zudem unmissverständlich hervor, dass es sich hierbei um einen bewussten und begründeten Entscheid handelte. Gemäss Botschaft zum BÜPF «muss die Sortierung, mit der bestimmte Datentypen aus dem Datenfluss ausgesondert werden, entgegen der Bestimmung, die im Vorentwurf vorgesehen war, grundsätzlich durch den Dienst erfolgen. Allein schon aus Fragen der Haftung für die Vollständigkeit der Daten ist es heikler, diese Aufgabe einer anderen Stelle zu übertragen, insbesondere den Fernmeldedienstanbieterinnen»⁴.

Eine Abwälzung der Filter- bzw. Kürzungspflicht auf die Mitwirkungspflichtigen verstösst mit anderen Worten gegen das Legalitätsprinzip. Die Mitwirkungspflichtigen sind von Gesetzes wegen gar *nicht berechtigt*,

⁴ Vgl. [Botschaft zum BÜPF, BBI 2013, S. 2727](#).

den im Rahmen einer angeordneten Überwachung aufgezeichneten Inhalt des Fernmeldeverkehrs herauszufiltern. Vielmehr gehört es zu den Aufgaben des Dienst ÜPF einer allfälligen Anordnung einer Strafbehörde auf Aussonderung von IP-Paketen nachzukommen. Er kann dies direkt gestützt auf Art. 17 Bst. g BÜPF tun. Entsprechend beantragt asut, Art. 55a E-VÜPF ersatzlos zu streichen.

Aus Sicht asut ist es zudem effizienter und sicherer solche Eingriffe in den originären Fernmeldeverkehr jeweils nur von einer zentralen, behördlichen Stelle vornehmen zu lassen.

3.8. HD_62_IP: rückwirkende Überwachung zum Zweck der Teilnehmeridentifikation bei Internetverbindungen (Art. 60a E-VÜPF)

Art. 60a E-VÜPF stellt eine klare Ausweitung dieses Überwachungstyps und damit einen nicht unerheblichen (zusätzlichen) Eingriff in die Grund- bzw. Persönlichkeitsrechte der betroffenen Personen dar.

Gemäss der heutigen Regelung müssen Mitwirkungspflichtige bei den sog. Schnittmengenberechnungen einzig dann Auskünfte erteilen, wenn die Ergebnisse eine eindeutige oder zumindest eine möglichst eindeutige Benutzeridentifikation zulassen. Neu müssten die Mitwirkungspflichtigen auf Verlangen der anordnenden Behörde auch bei nicht eindeutigen Ergebnissen, das heisst bei Mehrfachtreffern, die falsch-positiven Ergebnisse herausgeben. Dies kann eine sehr grosse Anzahl von Personen betreffen. Die Schnittmengenberechnung ist der Versuch, das Fehlen einer wichtigen Information durch den Vergleich mehrerer Ereignisse (d.h. mehrere Internetverbindungen) zu kompensieren. Die meisten dieser Internetverbindungen haben unbedenkliche Inhalte als Ziel. Es befinden sich darunter vielleicht nur wenige (wenn überhaupt), die kritische Inhalte als Ziel haben. Es ist möglich, dass die Strafverfolger aus Gründen, die sie nicht beeinflussen können, nicht in der Lage sind, aussagekräftige Informationen zu beschaffen. Dass aber mit Hilfe dieser nicht aussagekräftigen Informationen und der Schnittmengenberechnung in die Grund- bzw. Persönlichkeitsrechte von vielen betroffenen Personen eingegriffen werden soll, ist aus Sicht asut nicht verhältnismässig.

Mit anderen Worten führt dieser Überwachungstyp zu einer Datenbeschaffung auf Mutmassung zu generellen Abklärungszwecken (sog. fishing expeditions). Wie der Dienst ÜPF in den Erläuterungen richtigerweise ausführt, ist der Überwachungstyp daher in der Schwere des Grundrechtseingriffs mit dem Antennensuchlauf vergleichbar.

Aus Sicht asut, ist es mehr als fragwürdig, ob sich ein solch schwerer Eingriff für nur sehr beschränkt erfolgsversprechende Strafverfolgungszwecke (fishing expeditions) rechtfertigen lässt und inwiefern den Anforderungen aus dem Datenschutzgesetz Art. 25 Abs. 2 lit.c ff. Rechnung getragen werden kann. Die Grundpfeiler des Datenschutzrechts und EMRK Art. 8 scheinen damit tangiert. Fraglich ist zudem auch die genügende gesetzliche Grundlage im BÜPF, weil mit diesem neuen Überwachungstyp viel mehr als nur die Randdaten der überwachten Person im Sinne von Art. 26 Abs. 1 Bst. b BÜPF geliefert werden müssten.

Vor diesem Hintergrund stellt asut den Antrag, Art. 60a E-VÜPF ersatzlos zu streichen.

3.9. Übergangsbestimmungen (Art. 74c E-VÜPF)

Bei den Auskünften gemäss Art. 38a, 42a und 43a handelt es sich um neue, komplexe Auskunftstypen die von den FDA von Grund auf neu entwickelt, implementiert und erfolgreich getestet werden müssen. Die in Art. 74c E-VÜPF veranschlagte Umsetzungsfrist von 6 Monaten ist deshalb klarerweise zu kurz bemessen. Eine Übergangsfrist von 18 Monaten wäre vor diesem Hintergrund angemessen.

asut beantragt gemäss Pkt. 3.5 obenstehend eine ersatzlose Streichung von Art. 60a E-VÜPF. Sollte wider Erwarten diesem Antrag nicht entsprochen werden, so gilt es darauf hinzuweisen, dass dieser neue Überwachungstyp von Grund auf und in Zusammenarbeit im externen Lieferanten entwickelt werden müsste. Die dazu benötigte minimale Umsetzungsfrist beträgt 18 Monate.

asut beantragt gemäss Pkt. 3.4 obenstehend die ersatzlose Streichung von Art. 55a E-VÜPF. Sollte wider Erwarten diesem Antrag nicht entsprochen werden obliegt es den einzelnen Mitgliedern zu entscheiden, ob die Vorschrift trotz der fehlenden gesetzlichen Grundlage gleichwohl umgesetzt wird. Ungeachtet dessen müsste auch hier eine minimale Umsetzungsfrist von 18 Monaten gewährt werden, da auch dieser Echtzeitzeitüberwachungstyp in Zusammenarbeit mit externen Lieferanten von Grund auf neu entwickelt werden müsste.

4. Änderung der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (E-VD-ÜPF)

Mit den vorgeschlagenen Änderungen der VD-ÜPF kann sich asut einverstanden erklären.

Konkrete Änderungsanträge zu einzelnen Artikeln finden Sie im Anhang. Wir danken Ihnen bestens für die Berücksichtigung unserer Anliegen und stehen bei Fragen mit unseren Fachexpertinnen und Fachexperten gerne zur Verfügung.

Freundliche Grüsse



Judith Bellaiche
Präsidentin



Christian Gasser
Geschäftsführer

Politbeobachter
3000 Bern
info@politbeobachter.ch

Eidgenössisches Justiz- und
Polizeidepartement EJPD
3003 Bern
ptss-aemterkonsultationen@isc-ejpd.admin.ch

6. Mai 2025

Vernehmlassung zur Teilrevision VÜPF

Sehr geehrte Damen und Herren

Gerne nutzen wir die Gelegenheit und nehmen zur Vernehmlassung zur Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF) Stellung.

Die vorgeschlagene Teilrevision ist weitreichend und tangiert Grundrechte. Zu erwähnen ist die Wirtschaftsfreiheit (Art. 27 BV) durch die Ausdehnung der Pflichten zur Überwachung von Kommunikationsdiensten und der Privatsphäre (Art. 13 BV) durch diese. Einschränkungen von Grundrechten bedürfen einer gesetzlichen Grundlage (Art. 36 BV). Durch die gewählte Normstufe der Verordnung ist diese Voraussetzung nicht gegeben und somit verstösst die vorgeschlagene Teilrevision gegen die Bundesverfassung.

Aus diesen Überlegungen lehnt der Politbeobachter die Teilrevision des VÜPF ab. Auf eine ausführliche Beschreibung der Problematik der staatlichen Überwachung wird verzichtet.

Mit freundlichen Grüßen

Carin Jahn, Co-Präsidentin

Josef Ender, Co-Präsident

Salt.

Salt Mobile SA
Rue du Caudray 4
CH-1020 Renens 1

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundeshaus West
CH-3003 Bern

Eingereicht als pdf und word per email an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Renens, 06. Mai 2025

Stellungnahme zur Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat

Sehr geehrte Damen und Herren

Wir möchten uns für die Möglichkeit zur Anhörung betreffend die Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) bedanken und nehmen dazu gerne fristgerecht Stellung.

Management Summary

Salt Mobile SA (Salt) ist als eine der drei Schweizer Mobilnetzbetreiberinnen unmittelbar betroffen von den Gesetzesänderungen, da mit gut 99% der Grossteil der Fernmeldeüberwachungen auf den Netzen der drei Schweizer Mobilnetzbetreiberinnen stattfindet.

Gemäss der Vorlage zur revidierten Verordnung soll insb. der Geltungsbereich neu definiert werden, indem die Kriterien für Mitwirkungspflichtige (MWP), also Fernmeldedienstanbieterinnen (FDA) und Anbieterinnen aufgesetzter Kommunikationsdienste (AAKD) angepasst werden. Weiter sollen neue Überwachungsmassnahmen geschaffen werden.

Anpassungen in einer Verordnung bedürfen einer rechtlichen Grundlage im entsprechenden Gesetz – hier das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). Diese ist sowohl betreffend Geltungsbereich als auch betreffend neue Überwachungsformen teilweise nicht gegeben. Der Verordnungsentwurf muss somit entsprechend angepasst, gewisse Artikel sogar gestrichen werden. Die angedachten sog. Fishing Expeditions sind grundsätzlich abzulehnen.

Der Verordnungsentwurf muss zwingend überarbeitet, gewisse Artikel müssen gestrichen werden.

Detaillierte Ausführungen zu einzelnen Artikeln im Entwurf der revidierten VÜPF (E-VÜPF)

Einteilung der Mitwirkungspflichtigen (Art. 16a bis 16g E-VÜPF)

In der Medienmitteilung des Bundesrates vom 29.01.2025¹ zur Eröffnung der Vernehmlassung steht:
*Die Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) unterteilt die Fernmeldedienstanbieterinnen (FDA) weiterhin in zwei Unterkategorien: FDA mit vollen Pflichten und FDA mit reduzierten Pflichten. Anderseits sollen die Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD) neu in drei Unterkategorien unterteilt werden: AAKD mit minimalen Pflichten, AAKD mit reduzierten Pflichten und AAKD mit vollen Pflichten. Diese Differenzierungen sollen eine ausgewogenere Abstufung der Pflichten ermöglichen und eine Angleichung zwischen FDA und AAKD vergleichbarer Grösse und wirtschaftlicher Bedeutung bringen. Eine AAKD mit vollen Pflichten muss mindestens 100 Millionen Franken Umsatz erzielen und/oder 1 Million Nutzer/-innen haben.*¹

Es ist zwar korrekt, dass gemäss BÜPF der Bundesrat die Kategorien der Pflichtigen definieren kann, jedoch muss dies auf Grundlage des Gesetzes erfolgen. Gemäss Art. 26 Abs. 6 und Art. 27 Abs. 3 gilt als Referenz für die Einteilung nicht ein Unternehmen, sondern der angebotene Dienst. Dies geht auch aus der Botschaft des BÜPF klar hervor, wonach *jede Tätigkeit jeweils unabhängig von der anderen betrachtet werden muss und dass ein Unternehmen je nach Tätigkeit, die es ausübt, ohne Weiteres mehreren Kategorien angehören kann und somit entsprechend diesen Tätigkeiten unterschiedlichen Überwachungspflichten unterliegt.*²

Es kann somit für die Einteilung nicht auf den Umsatz eines Unternehmens abgestellt werden. Im BÜPF wird zudem auf die wirtschaftliche Bedeutung und auf die Grösse der Nutzerschaft abgestellt. Das vorgesehene Kriterium von 100 Millionen Franken Umsatz pro Unternehmen steht also im Widerspruch zum BÜPF und muss daher gestrichen werden. Vielmehr muss auf die wirtschaftliche Bedeutung eines Dienstes, also auf den Umsatz pro Dienst resp. auf die Anzahl dessen Nutzer abgestellt werden, allenfalls auf die Anzahl Überwachungsaufträge für diesen Dienst.

Die Artikel sind entsprechend anzupassen.

Identifikationspflichten bei public WLAN (Art. 16h und 19 E-VÜPF)

Im erläuternden Bericht steht zu Art. 16h Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen: *Für solche «professionell betriebenen» WLAN-Zugänge gilt wie bisher die Pflicht, die Endbenutzerinnen und -benutzer mit geeigneten Mitteln zu identifizieren (Art. 19 Abs. 2 VÜPF, sog. indirekte Identifikation, z. B. per SMS an eine Mobilnummer). Diese Identifikationspflicht hat wie bisher jeweils die FDA zu erfüllen, die den Internetzugang erbringt, der dem jeweiligen WLAN-Zugang zugrunde liegt.*³

Für professionell betriebene öffentliche WLAN-Zugänge sind die Betreiberinnen dieser in die Pflicht zu nehmen zur Identifikation der Nutzer mit geeigneten Mitteln. Die Verantwortung dafür kann und darf alleine bei den Anbieterinnen dieser Netze liegen, da die Fernmeldedienstanbieterin, welche den Zugang zum

¹ Vgl. [Medienmitteilung Vernehmlassung](#)

² Vgl. [Botschaft zum BÜPF, BBI 2013, S. 2727](#).

³ Vgl. [Erläuternder Bericht](#)

Internet erbringt gar keine Kenntnis über die Gegebenheiten dieses WLAN-Zugangs hat. Es ist jedoch möglich, dass die Anbieterinnen der WLAN-Zugänge Systeme zur Identifikation der Fernmeldedienstanbieterinnen nutzen; dies ist jedoch eine Abmachung unter diesen Parteien. Die Verantwortung bleibt bei den Betreiberinnen der WLAN-Zugänge.

Der Artikel ist entsprechend anzupassen.

Filtern von Datenströmen (Art. 55a E-VÜPF)

Von den Mitwirkungspflichtigen soll verlangt werden, dass sie die Datenströme einer Echtzeitüberwachung filtern. Eine solche Handlung ist heikel, da damit der Inhalt durch die Mitwirkungspflichtigen verändert wird. Genau aus diesem Grund ist im BÜPF in Art. 16 lit. g dies klar als Aufgabe des Dienstes ÜPF geregelt: *auf Ersuchen der anordnenden Behörde nimmt er eine Sortierung vor, um bestimmte Datentypen aus dem Datenfluss herauszufiltern.*⁴

Auch aus der Botschaft zum BÜPF geht die Aufgabenzuteilung klar hervor: *Falls eine Sortierung vorgenommen werden muss, mit der sich bestimmte Datentypen aus dem Datenfluss aussondern lassen, muss diese entgegen der Bestimmung, die im Vorentwurf vorgesehen war, grundsätzlich durch den Dienst erfolgen. Allein schon aus Fragen der Haftung für die Vollständigkeit der Daten ist es heikler, diese Aufgabe einer anderen Stelle zu übertragen, insbesondere den Fernmeldedienstanbieterinnen.*⁵

Diese Aufgabe kann somit nicht den Fernmeldedienstanbieterinnen auferlegt werden, sondern muss beim Dienst ÜPF verbleiben.

Der Artikel ist somit ersatzlos zu streichen.

Rückwirkende Überwachung zum Zweck der Teilnehmeridentifikation bei Internetverbindungen (Art. 60a E-VÜPF)

Hier befürchten wir, dass mit den vorgeschlagenen Änderungen in unverhältnismässigem Ausmass in die Grundrechte und Privatsphäre von unbeteiligten Dritten eingegriffen werden könnte, wie wir dies bereits bei den Antennensuchläufen wiederholt moniert hatten. Im Gegensatz zur heutigen Regelung, wonach die Mitwirkungspflichtigen nur eindeutige Ergebnisse liefern, müssten sie in Zukunft auch Mehrfachtreffer melden. Dies stellt jedes Mal einen schwerwiegenden Eingriff in die Grundrechte und Privatsphäre von einer allenfalls sehr grossen Anzahl unserer Kundinnen und Kunden dar. Der Bundesdienst ÜPF sieht dies in den Erläuterungen übrigens ebenso.

Gemäss Bundesgesetz BÜPF ist eine Überwachung bis heute immer nur für eine konkrete Person oder ein sogenanntes Target zulässig (Art. 26 Abs. 1 BÜPF), und nicht für viele, allenfalls Tausende mit sog. Schnittstellenberechnungen, um das Target erst noch zu finden.

Man spricht hier auch von sog. Fishing Expeditions, wozu nicht nur die Grundlage im BÜPF äusserst fraglich ist, sondern auch jene aus dem Datenschutzgesetz. Wir als Salt erachten es als unsere Aufgabe, die Daten und Persönlichkeit unserer Kundinnen und Kunden zu schützen und hier darauf hinzuweisen.

Dieser Artikel ist somit ersatzlos zu streichen.

⁴ Vgl. [Art. 16 BÜPF](#)

⁵ Vgl. [Botschaft zum BÜPF, BBI 2013, S. 2727](#).

Übergangsfristen (Art. 74c E-VÜPF)

Sollten neue Überwachungsmassnahmen eingeführt oder bestehende Anforderungen wesentlich geändert werden, sind weitreichende Übergangsfristen vorzusehen.

Bei den Anforderungen für Auskünfte gemäss den Art. 38a, 42a und 43a mit neuen und nicht trivialen Auskunftstypen reicht eine Umsetzungsfrist von 6 Monaten bei Weitem nicht aus. Diese Funktionalitäten müssen im Jahresbudget aufgenommen und in der sogenannten IT-Roadmap eingeplant werden. Dafür ist mindestens eine Umsetzungsfrist von 18 Monaten vorzusehen. Dies gilt auch für die Art. 55a und Art. 60a, sollten diese wider Erwarten nicht ersatzlos gestrichen werden.

Änderung der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (E-VD-ÜPF)

Wir haben keine Bemerkungen zu diesem Verordnungsentwurf.

Fazit und Schlussbemerkungen

Wir fordern die Anpassung und teilweise Streichung von Artikeln im Verordnungsentwurf (E-VÜPF) gemäss unseren gemachten Ausführungen.

Sowohl die Einteilung der Mitwirkungspflichtigen als auch die Ausgestaltung neuer Überwachungsmassnahmen bedürfen einer gesetzlichen Grundlage im Bundesgesetz BÜPF. Ist diese nicht gegeben, sind die Artikel anzupassen resp. sogar zu streichen. Schwerwiegende Grundrechtseingriffe ohne eine klare rechtliche Grundlage lehnen wir stellvertretend für unsere Kundinnen und Kunden ab.

Wir verweisen auf die Stellungnahme unseres Branchenverbands asut und für konkrete Anpassungsvorschläge zu den einzelnen Artikeln auf deren Anhang, welche wir beide vollends unterstützen.

Wir hoffen auf die nötige Gewichtung unserer Aussagen und auf wohlwollende Aufnahme unserer Positionen.

Freundliche Grüsse



Felix Weber, Senior Regulatory Affairs Manager, Salt Mobile SA

Beilagen:

- Stellungnahme der asut
- Anhang zur Stellungnahme der asut

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Per Email an:
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 6. Mai 2025

Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat,
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die am 29. Januar 2025 eröffnete Vernehmlassung zur «Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)» und danken Ihnen für die Einladung zur Stellungnahme. Der Schweizerische Verband der Telekommunikation (asut) vertritt die Interessen der Telekommunikations-, Netzwerk- und Datacenter-Branche. Unsere Mitglieder, insbesondere die Anbieterinnen von Fernmeldediensten (FDA) und die Anbieterinnen von abgeleiteten Kommunikationsdiensten (AAKD) sind die vornehmlich direkt betroffenen Adressaten der vorgeschlagenen Anpassungen. Gerne nehmen wir die Möglichkeit zur Stellungnahme wahr und übermitteln Ihnen fristgerecht unsere Einschätzung.

Grundsätzliche Einschätzung zur Teilrevision der VÜPF

Mit der Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs am 1. März 2018 wurden verschiedene Kategorien von Mitwirkungspflichtigen geschaffen. Die Umsetzung dieser Kategorien in der VÜPF und in der Praxis gestaltete sich jedoch schwierig. So führte eine Referenz zum Fernmeldegesetz (FMG) dazu, dass bei verschiedenen Anbieterinnen unklar war, ob sie gemäss BÜPF als FDA oder als AAKD gelten. Zudem fehlte eine verbindliche Definition der abgeleiteten Kommunikationsdienste, so dass es für Anbieterinnen von Internetdiensten bis heute unklar ist, ob sie nun mitwirkungspflichtige AAKD gemäss BÜPF sind oder nicht. Erst die Revision des Fernmeldegesetzes vom 22. März 2019 brachte eine Klärung betreffend der FDA gemäss BÜPF. Hinsichtlich der AAKD fällte das Bundesgericht 2021 zwei wegweisende Entscheide. Mit der vorliegenden Revision der VÜPF sollen nun die Kategorien der FDA und der AAKD neu geregelt werden.

Angesichts der unbefriedigenden Umsetzung des BÜPF und der VÜPF in den vergangenen Jahren begrüßt asut die Absicht des Bundesrates, die verschiedenen Kategorien der Mitwirkungspflichtigen besser zu regeln. Die vorliegende Vernehmlassungsvorlage wird diesem Ziel jedoch nicht gerecht. Vielmehr würde der vorliegenden Entwurf der VÜPF (E-VÜPF) zu einer Zunahme der Anzahl betroffener Unternehmen führen, und es fehlen bei den AAKD weiterhin klare Definitionen, welche Dienste in den Geltungsbereich der Fernmeldeüberwachung fallen. Folgende Gründe führen zu unserer Einschätzung:

- Umsetzung nicht gesetzeskonform: Das BÜPF erlaubt eine Differenzierung der Pflichten von FDA und AAKD. Ausschlaggebend ist dabei gemäss BÜPF nicht das ganze Unternehmen. Vielmehr muss jeder einzelne Dienst hinsichtlich dessen wirtschaftlicher Bedeutung oder Benutzerschaft separat betrachtet werden. Zudem ist es auch möglich, dass ein Unternehmen sowohl FDA als auch AAKD ist, aber nur für die jeweiligen Dienste. Im Widerspruch dazu sieht der E-VÜPF jedoch vor, dass beim Umsatz zur Einstufung einer FDA oder einer AAKD nicht der Umsatz eines Dienstes betrachtet wird, sondern der Gesamtumsatz des Unternehmens (Konzernumsatz). Damit werden mehr FDA und AAKD die kritische Schwelle beim Jahresumsatz von CHF 100 Mio. überschreiten, was zu einer Zunahme der Anzahl Mitwirkungspflichtigen mit vollen Pflichten führt. Und dies obwohl ein Teil des Umsatzes gar nichts mit dem entsprechenden Fernmeldedienst oder abgeleiteten Dienste zu tun hat und somit zu keinem Zusatzznutzen für die Strafverfolgung führt.
- Unverhältnismässige Ausweitung der betroffenen Unternehmen: Gemäss der Statistik des Bundes zur Fernmeldeüberwachung wurden 2024 insgesamt 527'344 Auskünfte erteilt und 20'591 Überwachungen durchgeführt. 94% der Auskünfte und 99% der Überwachungen betrafen lediglich vier Unternehmen, die bereits heute den vollen Pflichten der VÜPF unterliegen. Die erweiterte Betrachtung beim Umsatz (d.h. Gesamtumsatz) sowie die Schwellenwerte bei den AAKD betreffend die Teilnehmer werden die Anzahl Unternehmen und Dienste, welche einer reduzierten oder vollständigen Pflicht unterliegen, deutlich erhöhen. Die betroffenen Unternehmen müssen dann entsprechende Prozesse und Systeme einführen und betreiben, was beträchtliche Mittel erfordern kann. Dieser Aufwand erscheint angesichts der wenigen zu erwartenden Auskünfte und Überwachungen unverhältnismässig, da der zusätzliche Aufwand kaum einem entsprechenden Nutzen gegenübersteht. An dieser Stelle sei zudem darauf hingewiesen, dass die Zunahme der Unternehmen mit vollen Pflichten auch einen entsprechenden Kontroll- und Überwachungsaufwand beim Dienst ÜPF nach sich ziehen wird.
- Fehlende Definitionen der AAKD: Der erläuternde Bericht enthält auf den Seiten 19 und 20 eine Beschreibung möglicher AAKD, weist aber gleichzeitig darauf hin, dass eine abschliessende Auflistung nicht möglich sei. Damit besteht eine grosse Rechtsunsicherheit für Anbieterinnen von internetbasierten Diensten, da weiterhin offen bleibt, welche Dienste den Auskunfts- oder Überwachungspflichten unterliegen. Die Auflistung im erläuternden Bericht ist zudem viel zu umfangreich und würde beispielsweise auch das Internet der Dinge (IoT) umfassen, wo Messwerte und Signale übertragen werden können. Angesichts der Bedeutung der Digitalisierung und der Vielzahl an Diensten und Applikationen, die in irgendeiner Form einen Datenaustausch zulassen, ist eine klare und international kompatible Definition jedoch zwingend notwendig. Im Zentrum sollen dabei interpersonale Kommunikationsdienste stehen.
- Unklare Auswirkungen im Geschäftskundenbereich: Vernetzung und Digitalisierung ermöglichen Unternehmen heute ein «Outsourcing» von Applikationen oder Betriebsbereichen. Beispielsweise wird die Buchhaltungssoftware nicht mehr im eigenen Rechenzentrum betrieben, sondern aus der Cloud bezogen oder ein Teil des Firmennetzwerks wird bei einer FDA zugekauft. Damit könnten firmeninterne Netze und Dienste, die heute betreffend Überwachung nur einer Duldungspflicht unterliegen, je nach Outsourcing-Partner plötzlich der vollen Überwachung unterstehen. Dies hätte gravierende Auswirkungen für die betroffenen Unternehmen. Die E-VÜPF trägt den Anforderungen und Entwicklungen im Geschäftskundenbereich nicht Rechnung und wird daher zu grossen Schwierigkeiten bei der Umsetzung und zu Rechtsunsicherheit führen.
- Schwächung des Digitalstandortes Schweiz: Cybersecurity und der Schutz der Privatsphäre haben in den letzten Jahren eine zentrale Bedeutung im Rahmen der Digitalisierung erhalten. Kommunikationsdienste sind heute weitgehend End-to-End-Verschlüsselt und nur die Benutzer selbst bzw. ihre Endgeräte sind in der Lage die Inhalte zugänglich zu machen. Die E-VÜPF fordert neu bei den AAKD eine stärkere Identifikation der Benutzer sowie die Aufbewahrung von Randdaten. Da jedoch viele AAKD ihre Dienste aus dem Ausland anbieten, werden nur jene Unternehmen von den Massnahmen betroffen sein, die ihren Sitz in der Schweiz haben. Dies führt zu Wettbewerbsnachteilen für Schweizer Unternehmen und schwächt den Digitalstandort Schweiz.

Aus diesen Gründen lehnt asut die vorliegende Teilrevision der VÜPF ab und fordert weitgehende Anpassungen, um einen gesetzeskonforme Umsetzung der Fernmeldeüberwachung sicherzustellen.

Detaillierte Überlegungen zu den einzelnen Artikeln der E-VÜPF

1. Abgrenzung der Kategorien von Mitwirkungspflichtigen (Art. 16a bis 16g E-VÜPF)

Eine zentrale Änderung der Revision betrifft die neuen Definitionen der FDA und AAKD mit den jeweiligen Unterkategorien. Damit sollen die im BÜPF definierten Kategorien von Mitwirkungspflichtigen besser in der Verordnung abgebildet werden. Die damit angestrebte Klarheit und Rechtssicherheit wird seitens asut grundsätzlich begrüßt.

Kritisch beurteilt asut jedoch die in der E-VÜPF definierten Unterscheidungskriterien, welche über das Ausmass der Auskunfts- und Überwachungspflichten entscheiden. Diese entsprechen in Teilen nicht den gesetzlichen Vorgaben des BÜPF und sind weder sachgerecht noch verhältnismässig.

Nicht einverstanden erklären kann sich asut insbesondere mit dem Vorschlag, wonach Unternehmen mit einem jährlichen Gesamtumsatz von CHF 100 Mio. stets den vollen Überwachungspflichten unterliegen sollen und dies vollständig unabhängig von der Bedeutung der jeweils angebotenen Dienstleistungen. Diese pauschale Regelung soll gemäss E-VÜPF sowohl für den Bereich der Fernmeldedienste (Art. 16b Abs. 1 Bst. b Ziffer 2 E-VÜPF) als auch für den Bereich der abgeleiteten Kommunikationsdienste (Art. 16g Abs 1 Bst. b E-VÜPF) zur Anwendung kommen. Damit steht der Entwurf im klaren Widerspruch zu den Vorgaben des BÜPF.

Entscheidendes Unterscheidungskriterium für die Bestimmung der Auskunfts- und Überwachungspflichten ist gemäss den Vorschriften des BÜPF einzig die Bedeutung des konkreten Dienstes und dies unabhängig davon, von welchem Unternehmen der Dienst angeboten wird. Dies geht bereits aus dem Wortlaut von Art. 26 Abs. 6 sowie Art. 27 Abs. 3 BÜPF hervor, wo explizit auf die Bedeutung der jeweiligen Dienstleistung Bezug genommen wird. Die Botschaft des BÜPF hält dazu unmissverständlich fest, dass jede Tätigkeit (bzw. Dienstleistung) jeweils unabhängig von der anderen betrachtet werden muss und deshalb ein Unternehmen je nach Tätigkeit, die es ausübt, ohne Weiteres mehreren Kategorien angehören kann und somit entsprechend diesen Tätigkeiten unterschiedlichen Überwachungspflichten unterliegt¹. Das Bundesamt für Justiz hielt in einer vom Generalsekretariat des EJPD beauftragten Einschätzung der Rechtslage dazu ergänzend fest, dass dieser Umgang mit verschiedenen Aktivitäten derselben Akteure in der Gesetzgebung üblich sei und sich die Pflichten von Akteuren in aller Regel auf die betreffende Aktivität und nicht auch noch auf andere Aktivitäten beziehen. Hat ein Unternehmen verschiedene Aktivitäten in mehreren Bereichen, so seien diese jeweils gesondert zu betrachten (Aktennotiz BJ zu den Kategorien gemäss BÜPF vom 9. Februar 2019).

Der Revisionsentwurf zielt nunmehr jedoch genau in die gegenteilige Richtung. Er betrachtet bei der Kategorisierung jeweils pauschal alle von einem Unternehmen angebotenen Dienste (vgl. Art. 16b Abs. 1 Best. b Ziffer 1 und Art. 16g Abs. 1 E-VÜPF) und unterstellt grössere Unternehmen ganz generell den vollen Überwachungspflichten. Mit anderen Worten dürfte in der Praxis kaum ein Unternehmen für unterschiedliche Dienste unterschiedlichen Überwachungspflichten unterliegen, wie dies der Gesetzgeber fordert.

Die vom Bundesrat in der E-VÜPF vorgenommene Einteilung bzw. Kategorisierung lässt sich weiter auch sachlich, aus der Optik der Strafverfolgung nicht rechtfertigen. Dies lässt sich am besten anhand eines Beispiels illustrieren: gemäss Art. 16g E-VÜPF würde ein neuer Cloud- oder Messagingdienst einer Start-Up-Tochterfirma eines grösseren Unternehmens (z.B. eine Versicherungsgesellschaft mit CHF 500 Mio. Umsatz) mit 50 Teilnehmern als AAKD mit vollen Überwachungspflichten eingestuft, während dieselben Dienste eines mittelgrossen Unternehmens mit CHF 90 Mio. Umsatz und 900'000 Teilnehmern gemäss Art. 16f E-VÜPF lediglich den reduzierten Überwachungspflichten unterliegen würde. Ein solches Ergebnis ist offensichtlich stossend und es kann schlichtweg nicht im Interesse der Strafverfolgung liegen, dass Dienste von sehr untergeordneter Bedeutung strenger überwacht werden müssen als Dienste mit einer relevanten Anzahl von Nutzerinnen und Nutzern. Für die Strafverfolgung von Relevanz ist nicht die Umsatzgrösse eines Unternehmens oder die Frage, ob ein Unternehmen allenfalls bereits einen anderen Telekommunikationsdienst anbietet, sondern die Bedeutung des konkreten Dienstes und dieser spiegelt sich gemäss BÜPF in der wirtschaftlichen Bedeutung sowie der Benutzerschaft wider.

Zusätzlich berücksichtigt die E-VÜPF die Anzahl der Überwachungsaufträge bei der Beurteilung, ob eine FDA nur reduzierten oder den vollen Pflichten unterliegt. Bei den AAKD hingegen, soll die Anzahl Auskunftsgesuche und Überwachungsaufträge nicht mehr berücksichtigt werden. Aus Sicht asut sind diese Anpassungen nicht korrekt. In der Ratsdebatte zum BÜPF führte die zuständige Bundesrätin damals aus,

¹ Vgl. [Botschaft zum BÜPF, BBI 2013, S. 2707](#).

dass die Bedeutung eines Dienstes für die Strafverfolgung selbstverständlich ein Kriterium sein soll, auch wenn es nicht namentlich im Gesetz erwähnt wird. Damit soll verhindert werden, dass Unternehmen in Auskunfts- oder Überwachungssysteme investieren müssen, obwohl dafür seitens der Strafverfolgung kein genügend grosser Bedarf besteht. Daher sollen diese Kriterien auch bei den AAKD zur Anwendung kommen. Zudem soll die Relevanz für die Strafverfolgung kumulativ zur wirtschaftlichen Bedeutung oder Benutzerschaft berücksichtigt werden. Eine FDA würde daher als FDA mit reduzierten Pflichten gelten, wenn sie eine der beiden Kriterien nicht überschreitet.

Weiter weisen wir darauf hin, dass die Aufwände für die Implementierung von Überwachungsmassnahmen grossmehrheitlich jeweils pro (neuen) Dienst anfallen. Es wäre deshalb unverhältnismässig ein Unternehmen gleich am Tag Eins bei der Lancierung eines neuen Dienstes einer vollständigen, aufwändigen und kostenintensiven Überwachungspflicht zu unterstellen, nur weil das Unternehmen eine bestimmte Grösse hat oder allenfalls bereits über einen anderen etablierten Dienst verfügt. Ob sich neue Angebote im Markt erfolgreich durchsetzen werden, ist bekanntlich höchst ungewiss und entsprechend wird sich ein solches Unternehmen zweimal überlegen, ob sich diese erhöhten Investitionen in neue Dienste lohnen. Die vorgesehene Regulierung dürfte deshalb zusätzlich eine innovations- und investitionsemmende Wirkung entfalten. Dies gilt es aus Sicht der Branche zwingend zu vermeiden.

Vor diesem Hintergrund, stellt asut den Antrag, bei der Kategorisierung der Mitwirkungspflichtigen und der entsprechenden Einstufung der Auskunfts- bzw. Überwachungspflichten konsequent und einzig auf die Bedeutung der einzelnen Dienste abzustellen. D.h. massgebend ist – neben der oben erwähnten Anzahl Auskunftsgesuche oder Überwachungsaufträge – der Umsatz eines Dienstes bei den FDA sowie der Umsatz eines Dienstes oder die Anzahl Teilnehmer eines Dienstes bei den AAKD. Sollte der Verordnungsgeber diese Abgrenzungskriterien wider Erwarten jedoch als nicht ausreichend ansehen, dann müsste alternativ auf einen Jahresumsatz von CHF 100 Mio. der betreffenden Dienstleistung abgestellt werden: Bei den FDA beispielsweise auf die entsprechenden Jahresumsätze gemäss Fernmeldestatistik des Bundes. Auf den Umsatz des gesamten Unternehmens abzustellen hat Willkürcharakter und entspricht, wie oben dargelegt, weder dem Willen des Gesetzgebers noch lässt sich dieses Abgrenzungskriterium sachlich rechtfertigen.

Zusätzlich sollen, wie oben erläutert, die Anzahl Auskunftsgesuche oder Überwachungsaufträge als kumulatives Kriterium bei der Einstufung eines FDA oder einer AAKD zur Anwendung kommen. D.h. nur wenn ein FDA die Umsatzschwelle und gleichzeitig die festgelegte Anzahl Überwachungsaufträge überschreitet, gilt er als FDA mit vollen Pflichten. Ansonsten als FDA mit reduzierten Pflichten. Die Anzahl massgeblicher Überwachungsaufträge (bzw. Auskunftsgesuchen bei den AAKD) soll dabei massvoll erhöht werden, da auch die Anzahl Auskünfte und Überwachungen in den letzten Jahren deutlich zugenommen haben.

Bei den AAKD soll eine neue Abstufung der Pflichten eingeführt werden. Davon verspricht sich der Bundesrat eine KMU-freundliche Umsetzung des BÜPF im Bereich der AAKD. In der Praxis wird dieses Ziel jedoch nicht erreicht. Die Anzahl von 5'000 Benutzern ist im Zeitalter von Apps und Social-Media viel zu tief angesetzt und wird dazu führen, dass eine grosse Anzahl von Diensten den zusätzlichen Pflichten unterliegen. Zu diesen Pflichten gehört insbesondere die Identifikation der Teilnehmer, was heute bei vielen Anwendungen nicht dem Kundenbedürfnis entspricht. Betroffene Schweizer Dienste hätten daher im internationalen Wettbewerb gravierende Nachteile gegenüber ausländischen Diensten. Die Regelung ist zudem ungenügend, da weiterhin eine klare und eindeutige Definition fehlt, welche Dienste überhaupt als abgeleitete Dienste gemäss E-VÜPF gelten sollen. Die Aufzählung im erläuternden Bericht geht weit über die interpersonalen Kommunikationsdienste hinaus, welche in den europäischen Ländern der Überwachung unterliegen. Dies führt faktisch dazu, dass eine Vielzahl von Diensten, Smartphone-Apps etc. erweiterten Pflichten unterliegen und die Anbieter entsprechende Anpassungen an ihren Diensten und Systemen vornehmen müssen. Geradezu KMU-unfreundlich ist die Tatsache, dass der «Upgrade» zu AAKD von Verordnung wegen stattfindet, d.h. die betroffenen Unternehmen erhalten keine Verfügung. Mangels eindeutiger Definition eines AAKD führt dies zu grosser Rechtsunsicherheit bei den betroffenen Unternehmen. Es soll daher geprüft werden, ob die neue Kategorie der AAKD mit reduzierten Pflichten gemäss BÜPF überhaupt zulässig ist. Falls dies zutrifft, soll der Schwellenwert hinsichtlich grosser Benutzerschaft deutlich angehoben werden. Zur Bestimmung des Schwellenwertes schlagen wir vor, dass der Bund zuerst in einer Marktstudie den Kreis der betroffenen Unternehmen abklärt.

2. Identifikationspflichten im Bereich der WLAN-Zugänge (Art. 16h und 19 E-VÜPF)

asut hat Verständnis, dass aus Gründen der Praktikabilität öffentliche WLAN-Zugänge nur noch ab einer bestimmten Grösse als «professionell betrieben» gelten sollen (Art. 16h Abs. 2 E-VÜPF). Nicht nachvollziehen können wir jedoch, dass die bestehende Definition gemäss WLAN-Merkblatt des Dienstes ÜPF² nicht übernommen wurde. Dort gelten nur mehrere WLAN-Zugänge an unterschiedlichen Standorten als professionell betrieben. Gemäss E-VÜPF hingegen würde bereits ein einzelner WLAN-Zugang der mehr als 1'000 Verbindungen aufbauen kann, als professionell eingestuft. Heute erhältliche Consumer-Geräte sind bereits in der Lage mehr als 500 Verbindungen aufzubauen. D.h. hätte jemand zwei Accesspoints (z.B. mehrstöckiges Einfamilienhaus, Büro) mit Gastzugang, dann wären diese Zugänge gemäss VÜPF bereits professionell betrieben und würden entsprechenden Pflichten unterliegen. Bei der technischen Entwicklung ist davon auszugehen, dass in kurzer Zeit auch ein einzelner WLAN-Zugang mehr als 1'000 Verbindungen herstellen kann und damit wäre fast jeder private oder geschäftliche WLAN-Accesspoint mit Gastzugang der Überwachung unterstellt.

Verschärfend kommt hinzu, dass künftig offenbar die FDA, welche den zugrundeliegenden Internetzugang sicherstellt, und nicht die natürliche oder juristische Person, welche ihren Internetzugang Dritten mit ihrem WLAN zur Verfügung stellt bzw. die eigentliche Anbieterin des öffentlichen WLAN-Zugangs (PZD) für die Identifikation der Endbenutzerinnen- und -benutzer zuständig zeichnen soll (Art. 19 Abs. 2 E-VÜPF).

Entgegen den Verlautbarungen in den Erläuterungen zur E-VÜPF handelt es sich hierbei um eine sehr weitreichende Änderung, für welche jegliche Begründung fehlt. Gemäss Ziffer 5.1 des aktuellen Merkblatts WLAN vom Dienst ÜPF hat heute richtigerweise diejenige Anbieterin, welche den öffentlichen Zugangspunkt betreibt oder (in ihrem Auftrag) durch einen Dritten betreiben lässt, die Pflicht zur Identifikation der Endbenutzerinnen und -benutzer. Gemäss den Ausführungen im Merkblatt ist dabei insbesondere entscheidend, wer konkret gegenüber diesen Endbenutzerinnen- und -benutzer als Anbieterin des öffentlichen WLAN-Zugangs auftritt³.

Diese Regelung ist nach Ansicht von asut die einzige praktikable und sachgerechte Lösung, weil nur die Anbieterin des öffentlichen, professionell betriebenen WLAN-Zugangs (bzw. die Person, die ihren Zugang Dritten zur Verfügung stellt), den Zugang auf die entsprechende Service-Infrastruktur direkt oder allenfalls mit Hilfe ihres technischen Dienstleisters kontrollieren kann. Nur die PZD, die gegenüber den WLAN-Endnutzenden als Vertragspartnerin bzw. Dienstleisterin auftritt, kann diese gemäss den Vorgaben des VÜPF identifizieren.

Die FDA, welche im Hintergrund einzige den dem PLWAN zugrundeliegenden Internetzugang zur Verfügung stellt, steht demgegenüber in keinem Dienstleistungsverhältnis zu den Endbenutzerinnen und -benutzer des WLAN-Zugangs. Sie ist nicht die Anbieterin dieses Dienstes und hat entsprechend auch keine Kenntnis davon, wer allenfalls den PWLAN-Service der PZD nutzt. Die Internetzugangsanbieterin kann ganz grundsätzlich auch keine wirksame technische Kontrolle darüber ausüben, für welche Zwecke ihre Kundinnen und Kunden die Internetzugänge einsetzen und wem sie Zugang auf eine PWLAN-Einrichtung gewähren. Der Internetzugang funktioniert für die daran angeschlossenen Services vielmehr transparent. Wenn als Beispiel an einem Internetzugang eine Infrastruktur für E-Mails betrieben wird, kann der Zugang zu den E-Mail Accounts nicht am Internetzugang kontrolliert werden. Der Zugang zu den E-Mail Accounts wird vielmehr in der Service-Infrastruktur (E-Mail Server) kontrolliert. Analog verhält es sich bei den professionell betriebenen öffentlichen WLAN-Zugängen. Nur der Gatekeeper der WLAN-Infrastruktur und nicht der Gatekeeper der zugrundeliegenden Internetzugang kann eine Zugangskontrolle ausüben. Die reine Internetzugangsanbieterin ist mit anderen Worten schlichtweg nicht in der Lage, Endnutzerinnen und Endnutzer eines WLAN-Zugangs zu identifizieren. Davon ausgenommen sind selbstredend diejenigen Fälle, wo die Internetzugangsanbieterin ebenfalls den öffentlichen WLAN-Zugang anbietet, d.h. sowohl als FDA (Internetzugangsanbieterin) als auch als PZD agiert.

Vor diesem Hintergrund ist es auch offensichtlich, dass eine reine Internetzugangsanbieterin unmöglich prüfen kann, ob eine PZD auf ihren WLAN-Service-Einrichtungen kumuliert den Schwellenwert von mehr als 1'000 Endnutzerinnen und Endnutzer überschreitet und somit als professionelle Betreiberin i.S. von Art. 16h E-VÜPF eingestuft werden muss. Wie dargelegt, kontrolliert einzige die PZD ihre WLAN-Zugänge und bestimmt die darauf gewährten (Benutzer-)Kapazitäten. Weiter kann ein PZD oder sein technischer Dienstleister die Internetanschlüsse für die einzelnen WLAN-Zugänge ohne weiteres bei verschiedenen Internetzugangsanbieterinnen beziehen (z.B. Wlan1 in Basel mit einer Kapazität von 600 bei FDA1 und Wlan2 in

² [Merkblatt WLAN](#) vom Dienst Überwachung des Post- und Fernmeldeverkehrs vom 1. März 2018.

³ Diese sich am wirtschaftlichen Dienstleistungsbegriff orientierte Definition gilt auch für die Festlegung des Begriffs Anbieterin von Fernmeldediensten (FDA). FDA ist, wer gegenüber den Kunden als Dienstleisterin/Vertragspartnerin auftritt (Vgl. [Faktenblatt zur Registrierung als FDA](#)).

Zürich mit einer Kapazität von 700 in Zürich bei FDA2). Eine FDA kann entsprechend auch aus diesem Grunde gar nicht feststellen, ob ein PZD in der Praxis ein professionelles WLAN mit mehr als 1'000 Endbenutzerinnen und -benutzer betreibt.

Gemäss E-VÜPF sollten neu Internetzugangsanbieter bzw. FDA im Ergebnis für etwas in die Verantwortung genommen werden, für das sie in der Praxis faktisch gar keine Kontrolle ausüben und deshalb auch keine Verantwortung übernehmen können. Eine solche Regelung ist offensichtlich stossend und systemfremd. Dies ergibt sich im Übrigen direkt aus Art. 2 Bst. e BÜPF, wo die PZD als eigenständige mitwirkungspflichtige Personen definiert sind. Gemäss dem Vorschlag in der E-VÜPF würden die PZD aber schlichtweg keinerlei gesetzlichen Mitwirkungspflichten unterliegen, was nicht die Absicht des Gesetzgebers war.

Nach Ansicht von asut ist im neuen Art. 19 E-VÜPF zu präzisieren, dass sich die PZD, d.h. die jeweiligen Anbieterinnen von professionell betriebenen öffentlichen WLAN-Zugängen, für die Identifikation aller Endbenutzerinnen und -benutzer verantwortlich zeichnen.

3. Weitere Änderungsanträge

3.1. FDA (Art. 16a E-VÜPF)

Wie eingangs bereits erwähnt, wurde mit der FMG-Revision vom 22. März 2019 eine Referenz zwischen dem BÜPF und dem FMG gestrichen. Damit sollte sichergestellt werden, dass OTT-Anbieter im Rahmen der Fernmeldeüberwachung als AAKD eingestuft werden und nicht als FDA. Die eigentliche Definition eines FDA blieb davon unberührt. Entscheidend ist bei der Einstufung als FDA, wer gegenüber der Kundin oder dem Kunden die Verantwortung für die fernmeldetechnische Übertragung von Informationen übernimmt. Dies ist daher von Bedeutung, da beim Betrieb eines öffentlichen Fernmeldenetzes auf der technischen Ebene eine Vielzahl von Unternehmen involviert sein können. Nach Art. 16a Abs.1 Bst. a E-VÜPF gilt aber auch als FDA, wer ein öffentliches Fernmeldenetz betreibt. Dies können für dasselbe Netz auch mehrere Unternehmen sein. Damit würde eine unnötige Duplizierung der Pflichten gemäss E-VÜPF für ein und dasselbe öffentliche Fernmeldenetz entstehen. Daher soll Art. 16a Abs. 1 Bst. a E-VÜPF ersatzlos gestrichen werden.

3.2. Teilnehmer- und Benutzeridentifikation (Art. 19 Abs. 1 E-VÜPF)

Neu soll eine Teilnehmer- und Benutzeridentifikation nicht nur für FDA, PZD sowie Wiederverkäuferinnen (Art. 2 Lit. f BÜPF) gelten, sondern auch für die neue Kategorie der AAKD mit reduzierten Pflichten. Da der Schwellenwert für diese AAKD mit 5'000 Benutzern sehr tief angesetzt ist, führt dies faktisch zu einer flächendeckenden Pflicht zur Identifikation von Teilnehmern und Benutzern bei den AAKD. Gemäss erläuterndem Bericht (S.30/31) kann diese mittelbare Identifikation beispielsweise mittels SMS-Zugangscode auf das Handy oder den Autorisierungsdaten bei Kreditkartenzahlungen erfolgen. Dabei erfolgt die Identifikation in der Regel nur bei der erstmaligen Aktivierung eines Dienstes und nicht laufend. Die aufgeführten Identifikationsmittel sind jedoch für viele abgeleitete Kommunikationsdienste nicht praktikabel oder werden von Benutzerinnen und Benutzern nicht geschätzt. Als Alternative schlägt der erläuternde Bericht daher eine Identifikation durch die Auskunftstypen IR_59_EMAIL_LAST und IR_60_COM_LAST vor. Dies hätte zur Folge, dass AAKD mit reduzierten Pflichten in ein Auskunftssystem investieren müssen, obwohl sie noch gar nicht der automatisierten Auskunftspflicht unterstehen. Zudem ist es nicht nachvollziehbar, dass bei Kreditkarten eine einmalige Identifikation des Teilnehmers ausreicht, bei der Identifikation über IR_59 und IR_60 hingegen eine permanente Identifikation notwendig ist.

Diese Ausführungen zeigen deutlich die Mängel, welche durch die Einführung der neuen Kategorie der AAKD mit reduzierten Pflichten entstehen. Daher soll in Art. 19 Abs. 1 die Pflicht für diese AAKD gestrichen werden. Entsprechend sollen die AAKD mit reduzierten Pflichten auch in Art. 21 Abs. 1 Bst. a gestrichen werden.

3.3. Auskunftstypen mit flexibler Namenssuche (Art. 27 Abs. 3 E-VÜPF)

Gemäss der heutigen Regelung ist die flexible Suchfunktion für Namen von natürlichen Personen möglich. Diese flexible Suchfunktion wurde eingeführt, um ein in der Praxis auftretendes Problem bei der Eingabe

von Personennamen zu beheben: Insbesondere bei komplizierteren Namen oder solchen mit anderen Zeichensätzen werden teilweise fehlerhafte bzw. nicht ganz korrekte Eingaben getätigt.

Die nun vorgeschlagene Erweiterung auf juristische Personen lässt sich nach Ansicht von asut demgegenüber nicht rechtfertigen. Erstens sind den FDA im Bereich der juristischen Personen keine ähnlichen, regelmässig auftretenden Probleme bei der Sucheingabe bekannt, und auch in den Erläuterungen wird hierzu nichts ausgeführt. Im Gegensatz zur Personensuche stehen den Strafverfolgungsbehörden bei der Firmensuche ausserdem öffentlich zugängliche Hilfsmittel zur Verfügung, mit denen flexibel gesucht werden kann (z.B. Zefix). Den Strafverfolgern kann durchaus zugemutet werden, eine entsprechende Kontrolle bzw. Suche bei Bedarf selbst durchzuführen. Vermutungsweise wird dies teilweise bereits gemacht. Die flexible («nice to have»-) Suchfunktion nunmehr auf die Mitwirkungspflichtigen abzuwälzen ist vor diesem Hintergrund unnötig und unverhältnismässig. Auch an dieser Stelle gibt asut zu bedenken, dass die Implementierung von neuen technischen Funktionen jeweils bei allen betroffenen Anbietern mit einem nicht unerheblichem Entwicklungsaufwand und entsprechenden Kosten verbunden ist.

asut stellt vor diesem Hintergrund den Antrag, auf die vorgeschlagene Änderung von Art. 27 Abs. 2 E-VÜPF zu verzichten.

3.4. IR_8_IP_NAT: Benutzeridentifikation bei IP Adressen mit NAT (Art. 38 Abs. 2 E-VÜPF)

Der Wortlaut von Art. 38 Abs. 2 VÜPF wird materiell nicht angepasst und auch gemäss den Erläuterungen soll bei diesem Auskunftstyp inhaltlich nichts geändert werden. In denselben Erläuterungen wird jedoch ergänzend angemerkt, dass die beauftragten Mitwirkungspflichtigen eine mögliche Toleranzabweichungen der Systemuhren bei der Suche und Identifikation der Benutzer, der Urheberschaft oder der Herkunft zu berücksichtigen haben.

Eine solche Berücksichtigung stellt nach Ansicht von asut eine materielle Änderung dar, die seitens der FDA in dieser Form jedoch nicht umgesetzt werden kann. Die Strafverfolger erhalten die Informationen für Aufträge dieses Auskunftstyps (öffentliche Source IP-Adresse, Source Port, Zeitpunkt) aus Logfiles, die ihnen von den Content-Anbietern im Internet (Chat-Services, Online-Shops, Webseiten etc.) zur Verfügung gestellt werden. Die Herkunft und Details zur Urheberschaft der Daten sind bei der Übermittlung des Auftrags an die Mitwirkungspflichtigen jedoch nicht vorgesehen. Ihnen ist die Herkunft der Daten, die dem Auftrag zu Grunde liegen, die dort vorhandene technische Infrastruktur und die für die Synchronisation der Zeit verwendeten Methoden und Funktionen somit nicht bekannt. Ohne diese Informationen ist eine Einschätzung von Toleranzabweichungen der Systemuhren bei den FDA jedoch nicht möglich.

Vor diesem Hintergrund ist diese Anmerkung in den Erläuterungen zu Abs. 2 («Ergänzend zu den Ausführungen [...] berücksichtigen hat») zu streichen.

3.5. IR_58_IP_Intersect: Benutzeridentifikation durch Schnittmengenbildung (Art. 38a E-VÜPF)

asut kann sich mit diesem neuen Auskunftstyp einverstanden erklären. Der Zweck des Auskunftstyps wird im Artikel allerdings aus Sicht asut nicht korrekt wiedergegeben. Die Schnittmengenberechnung kommt vor allem zur Anwendung, wenn die Strafverfolger von ihren Quellen keine Informationen zur öffentlichen Quell-Portnummer erhalten. In solchen Fällen kann eine Schnittmengenberechnung von mehreren Internetverbindungen das Fehlen der öffentlichen Quell-Portnummer kompensieren und trotzdem zu einem Resultat führen. Folgerichtig ist deshalb die Angabe der öffentlichen Quell-Portnummer, der öffentlichen Ziel-IP-Adresse und der Ziel-Portnummer nicht notwendig.

Weiter sieht asut Anpassungsbedarf bei zwei Anmerkungen in den Erläuterungen:

- In Absatz 2 der Erläuterungen wird darauf hingewiesen, dass wenn ein Auskunftsgesuch IR_7_IP nicht zu einem eindeutigen Ergebnis führt und auch ein Auskunftsgesuch IR_8_IP_NAT nicht erfolgreich ist, eine Schnittmengenbildung aus den Mehrfachergebnissen zu einer eindeutigen Identifikation führen kann. Dieser Text suggeriert eine nicht vorhandene Verbindung zwischen IR_7_IP und IR_8_IP_NAT. Der Zusammenhang, der hier dargestellt wird, existiert in dieser Form nicht und entsprechend sollte der Hinweis auf das Auskunftsgesuch IR_7_IP gestrichen werden. Darüber hinaus kommt die Schnittmengenberechnung wie oberhalb erwähnt vor allem zur Anwendung, wenn die Strafverfolger von ihren Quellen keine Informationen zur öffentlichen Quell-Portnummer erhalten. Es besteht also auch kein direkter Zusammenhang mit nicht erfolgreichen Auskunftsgesuchen IR_8_NAT. Darum sollte auch dieser Teil des Textes in der Erläuterung gestrichen und der Zweck

des IR_58_IP präzisiert werden.

- Analog zu den Ausführungen bei Art. 39 E-VÜPF fehlen den FDA auch hier die nötigen Informationen, um eine Einschätzung zu möglichen Toleranzabweichungen der Systemuhren berücksichtigen zu können. Deshalb ist auch hier der entsprechende Hinweis in den Erläuterungen zu Abs. 3 («Für diesen Zeitpunkt gilt, wie auch bei Artikel 38 Abs. 2 [...] zu berücksichtigen hat») zu streichen.

3.6. Entfernung von Verschlüsselungen (Art. 50a E-VÜPF)

Gemäss Art. 26 BÜPF sind FDA verpflichtet, im Rahmen von Überwachungen die von ihnen angebrachten Verschlüsselungen zu entfernen. Diese Pflicht kann auch AAKDs mit erweiterten Pflichten gemäss Art. 27 BÜPF auferlegt werden. Neu verlangt jedoch Art. 50a E-VÜPF, dass diese Verpflichtung auch für AAKD mit reduzierten Pflichten gilt. Damit müssten alle AAKD mit mehr als 5'000 Benutzern die Entfernung der von ihnen angebrachten Verschlüsselung vorsehen. Damit geht die E-VÜPF über den gesetzlichen Rahmen der BÜPF hinaus und es zeigt sich erneut, dass die neu geschaffene Kategorie der AAKD mit reduzierten Pflichten nicht gesetzeskonform ist.

Art. 50a verlangt von den AAKD, dass sie ihre Dienste so gestalten, dass die Verschlüsselung jederzeit entfernt werden kann. Da die Verschlüsselung heute ein zentrales Sicherheitselement vieler abgeleiteter Dienste ist, betrifft dies nicht nur die AAKD mit vollen oder reduzierten Pflichten, sondern in der Praxis alle AAKD. Denn kein Unternehmen würde einen Dienst ohne diese Anforderung gemäss Art. 50a konzipieren und einführen, nur um beim Überschreiten eines Schwellenwertens die Sicherheitsfunktionen des Dienstes grundlegend anzupassen. Da die Möglichkeit, eine Verschlüsselung zu entfernen, das Sicherheitsniveau eines Dienstes schwächen kann, führt Art. 50a insgesamt zu negativen Auswirkungen auf die Cyber-Security der Schweiz. Zudem bleibt ungeklärt, welche Auswirkungen Art. 50a auf Verschlüsselungen hat, die durch den AAKD gar nicht mehr entfernt werden können (z.B. asymmetrische Verschlüsselungen) und ob die Anwendung dieser Verschlüsselungen gemäss E-VÜPF überhaupt noch zulässig wären. Der Geltungsbereich von Art. 50a soll daher auf FDAs sowie AAKD mit vollen Pflichten beschränkt werden.

3.7. RT_61_NA_CC-Trunc_IRI: Echtzeitüberwachung von Randdaten und gekürzten Inhalten bei Netzzugangsdiensten (Art. 55a E-VÜPF)

Dieser neue Überwachungstyp ist grundsätzlich eine Nachbildung des bereits existierenden Überwachungstyps gemäss Art. 55 VÜPF mit dem einzigen Unterschied, dass die Mitwirkungspflichtigen einen Teil der in Echtzeit aufgezeichneten Inhaltsdaten wieder aussortieren müssen. Welche Daten bzw. IP-Pakete entfernt bzw. geliefert werden müssen, wird dabei von der anordnenden Strafverfolgungsbehörde bestimmt.

Diese vorgesehene Aussonderungspflicht durch die Mitwirkungspflichtigen ist problematisch und würde eine systemwidrige Zäsur in die bewährte, gesetzlich vorgegebene Aufgabenteilung darstellen.

Das grundsätzliche Anliegen der Strafbehörden, nicht immer sämtliche angefallenen Daten zu erhalten, ist nachvollziehbar und sachlich gerechtfertigt. Mitunter lassen sich bei grossen Datenmengen die tatsächlich relevanten Daten für die Strafverfolger nur schwer auswerten.

Dieses Anliegen ist jedoch bereits auf Gesetzesstufe klar und abschliessend adressiert. Gemäss Art. 17 Bst. g BÜPF gehört es nämlich zu den Aufgaben des Dienstes ÜPF, auf Ersuchen der anordnenden Behörde eine allfällige Sortierung vorzunehmen und bestimmte Daten aus dem Datenfluss herauszufiltern. Diese Aufgabe fällt somit und entgegen der in Art. 55a E-VÜPF vorgeschlagenen Regelung dem Dienst ÜPF und nicht den Mitwirkungspflichtigen zu. Aus den Gesetzesmaterialien geht zudem unmissverständlich hervor, dass es sich hierbei um einen bewussten und begründeten Entscheid handelte. Gemäss Botschaft zum BÜPF «muss die Sortierung, mit der bestimmte Datentypen aus dem Datenfluss ausgesondert werden, entgegen der Bestimmung, die im Vorentwurf vorgesehen war, grundsätzlich durch den Dienst erfolgen. Allein schon aus Fragen der Haftung für die Vollständigkeit der Daten ist es heikler, diese Aufgabe einer anderen Stelle zu übertragen, insbesondere den Fernmeldedienstanbieterinnen»⁴.

Eine Abwälzung der Filter- bzw. Kürzungspflicht auf die Mitwirkungspflichtigen verstösst mit anderen Worten gegen das Legalitätsprinzip. Die Mitwirkungspflichtigen sind von Gesetzes wegen gar *nicht berechtigt*,

⁴ Vgl. [Botschaft zum BÜPF, BBI 2013, S. 2727](#).

den im Rahmen einer angeordneten Überwachung aufgezeichneten Inhalt des Fernmeldeverkehrs herauszufiltern. Vielmehr gehört es zu den Aufgaben des Dienst ÜPF einer allfälligen Anordnung einer Strafbehörde auf Aussonderung von IP-Paketen nachzukommen. Er kann dies direkt gestützt auf Art. 17 Bst. g BÜPF tun. Entsprechend beantragt asut, Art. 55a E-VÜPF ersatzlos zu streichen.

Aus Sicht asut ist es zudem effizienter und sicherer solche Eingriffe in den originären Fernmeldeverkehr jeweils nur von einer zentralen, behördlichen Stelle vornehmen zu lassen.

3.8. HD_62_IP: rückwirkende Überwachung zum Zweck der Teilnehmeridentifikation bei Internetverbindungen (Art. 60a E-VÜPF)

Art. 60a E-VÜPF stellt eine klare Ausweitung dieses Überwachungstyps und damit einen nicht unerheblichen (zusätzlichen) Eingriff in die Grund- bzw. Persönlichkeitsrechte der betroffenen Personen dar.

Gemäss der heutigen Regelung müssen Mitwirkungspflichtige bei den sog. Schnittmengenberechnungen einzig dann Auskünfte erteilen, wenn die Ergebnisse eine eindeutige oder zumindest eine möglichst eindeutige Benutzeridentifikation zulassen. Neu müssten die Mitwirkungspflichtigen auf Verlangen der anordnenden Behörde auch bei nicht eindeutigen Ergebnissen, das heisst bei Mehrfachtreffern, die falsch-positiven Ergebnisse herausgeben. Dies kann eine sehr grosse Anzahl von Personen betreffen. Die Schnittmengenberechnung ist der Versuch, das Fehlen einer wichtigen Information durch den Vergleich mehrerer Ereignisse (d.h. mehrere Internetverbindungen) zu kompensieren. Die meisten dieser Internetverbindungen haben unbedenkliche Inhalte als Ziel. Es befinden sich darunter vielleicht nur wenige (wenn überhaupt), die kritische Inhalte als Ziel haben. Es ist möglich, dass die Strafverfolger aus Gründen, die sie nicht beeinflussen können, nicht in der Lage sind, aussagekräftige Informationen zu beschaffen. Dass aber mit Hilfe dieser nicht aussagekräftigen Informationen und der Schnittmengenberechnung in die Grund- bzw. Persönlichkeitsrechte von vielen betroffenen Personen eingegriffen werden soll, ist aus Sicht asut nicht verhältnismässig.

Mit anderen Worten führt dieser Überwachungstyp zu einer Datenbeschaffung auf Mutmassung zu generellen Abklärungszwecken (sog. fishing expeditions). Wie der Dienst ÜPF in den Erläuterungen richtigerweise ausführt, ist der Überwachungstyp daher in der Schwere des Grundrechtseingriffs mit dem Antennensuchlauf vergleichbar.

Aus Sicht asut, ist es mehr als fragwürdig, ob sich ein solch schwerer Eingriff für nur sehr beschränkt erfolgsversprechende Strafverfolgungszwecke (fishing expeditions) rechtfertigen lässt und inwiefern den Anforderungen aus dem Datenschutzgesetz Art. 25 Abs. 2 lit.c ff. Rechnung getragen werden kann. Die Grundpfeiler des Datenschutzrechts und EMRK Art. 8 scheinen damit tangiert. Fraglich ist zudem auch die genügende gesetzliche Grundlage im BÜPF, weil mit diesem neuen Überwachungstyp viel mehr als nur die Randdaten der überwachten Person im Sinne von Art. 26 Abs. 1 Bst. b BÜPF geliefert werden müssten.

Vor diesem Hintergrund stellt asut den Antrag, Art. 60a E-VÜPF ersatzlos zu streichen.

3.9. Übergangsbestimmungen (Art. 74c E-VÜPF)

Bei den Auskünften gemäss Art. 38a, 42a und 43a handelt es sich um neue, komplexe Auskunftstypen die von den FDA von Grund auf neu entwickelt, implementiert und erfolgreich getestet werden müssen. Die in Art. 74c E-VÜPF veranschlagte Umsetzungsfrist von 6 Monaten ist deshalb klarerweise zu kurz bemessen. Eine Übergangsfrist von 18 Monaten wäre vor diesem Hintergrund angemessen.

asut beantragt gemäss Pkt. 3.5 obenstehend eine ersatzlose Streichung von Art. 60a E-VÜPF. Sollte wider Erwarten diesem Antrag nicht entsprochen werden, so gilt es darauf hinzuweisen, dass dieser neue Überwachungstyp von Grund auf und in Zusammenarbeit im externen Lieferanten entwickelt werden müsste. Die dazu benötigte minimale Umsetzungsfrist beträgt 18 Monate.

asut beantragt gemäss Pkt. 3.4 obenstehend die ersatzlose Streichung von Art. 55a E-VÜPF. Sollte wider Erwarten diesem Antrag nicht entsprochen werden obliegt es den einzelnen Mitgliedern zu entscheiden, ob die Vorschrift trotz der fehlenden gesetzlichen Grundlage gleichwohl umgesetzt wird. Ungeachtet dessen müsste auch hier eine minimale Umsetzungsfrist von 18 Monaten gewährt werden, da auch dieser Echtzeitzeitüberwachungstyp in Zusammenarbeit mit externen Lieferanten von Grund auf neu entwickelt werden müsste.

4. Änderung der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (E-VD-ÜPF)

Mit den vorgeschlagenen Änderungen der VD-ÜPF kann sich asut einverstanden erklären.

Konkrete Änderungsanträge zu einzelnen Artikeln finden Sie im Anhang. Wir danken Ihnen bestens für die Berücksichtigung unserer Anliegen und stehen bei Fragen mit unseren Fachexpertinnen und Fachexperten gerne zur Verfügung.

Freundliche Grüsse



Judith Bellaiche
Präsidentin



Christian Gasser
Geschäftsführer

**Anhang zur Stellungnahme zur
Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)**

Vorentwurf E-VÜPF	Änderungsanträge asut (fett bzw. durchgestrichen markiert)
Art. 11 Abs. 1 Bst. a a. Erteilung von Auskünften gemäss den Artikeln 35–38, 39–43a, 48a–48c sowie gemäss Artikel 27 in Verbindung mit den Artikeln 35, 40, 42 und 43;	Art. 11 Abs. 1 Bst. a a. Erteilung von Auskünften gemäss den Artikeln 35–38, 39 40 –43a, 48a–48c sowie gemäss Artikel 27 in Verbindung mit den Artikeln 35, 40, 42 und 43;
Art. 16a FDA (neu) ¹ Als FDA gilt für den betreffenden Dienst, wer einen Fernmeldedienst erbringt. Fernmeldedienste sind: a. Betrieb eines öffentlichen Fernmeldenetzes; ...	Art. 16a FDA (neu) 1 Als FDA gilt für den betreffenden Dienst, wer einen Fernmeldedienst erbringt. Fernmeldedienste sind: a. Betrieb eines öffentlichen Fernmeldenetzes; ...
Art. 16b FDA mit reduzierten Pflichten (neu) ¹ Auf Gesuch erklärt der Dienst ÜPF eine FDA für bestimmte Fernmeldedienste zur FDA mit reduzierten Pflichten, wenn sie: .. b. keine der nachstehenden Grössen erreicht: 1. Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste; 2. Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren. ² Kontrolliert eine Anbieterin im Sinne von Artikel 963 Absatz 2 des Obligationenrechts ein oder mehrere rechnungslegungspflichtige Unternehmen, so sind bei der Bestimmung der Anzahl der Überwachungen und des Jahresumsatzes die Anbieterin und die kontrollierten Unternehmen als Einheit zu betrachten. ³ b. ihr Jahresumsatz die Grösse nach Absatz 1 Buchstabe b Ziffer 2 erreicht hat; die Mitteilung muss innerhalb von drei Monaten nach dem Abschluss des Geschäftsjahres erfolgen.	Art. 16b FDA mit reduzierten Pflichten (neu) 1 Auf Gesuch erklärt der Dienst ÜPF eine FDA für bestimmte Fernmeldedienste zur FDA mit reduzierten Pflichten, wenn sie: .. b. keine eine der nachstehenden Grössen nicht erreicht: 1. Überwachungsaufträge zu 10 20 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste ; 2. Jahresumsatz in der Schweiz des gesamten Unternehmens mit einem bestimmten Fernmeldedienst von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren. ² Kontrolliert eine Anbieterin im Sinne von Artikel 963 Absatz 2 des Obligationenrechts ein oder mehrere rechnungslegungspflichtige Unternehmen, so sind bei der Bestimmung der Anzahl der Überwachungen und des Jahresumsatzes die Anbieterin und die kontrollierten Unternehmen als Einheit zu betrachten. ³ b. ihr Jahresumsatz die Grösse nach Absatz 1 Buchstabe b Ziffer 2 erreicht hat; die Mitteilung muss innerhalb von drei Monaten nach dem Abschluss des Geschäftsjahres erfolgen.
Art. 16f AAKD mit reduzierten Pflichten (neu)	Art. 16f AAKD mit reduzierten Pflichten (neu)

Vorentwurf E-VÜPF	Änderungsanträge asut (fett bzw. durchgestrichen markiert)
<p>¹ Eine AAKD gilt für alle von ihr angebotenen abgeleiteten Kommunikationsdienste als AAKD mit reduzierten Pflichten, wenn im Durchschnitt der letzten 12 Monate (Stichtag: 30. Juni) die Anzahl der Teilnehmenden für alle von der Anbieterin angebotenen abgeleiteten Kommunikationsdienste mindestens 5000 betragen hat und sie die Voraussetzungen nach Artikel 16g Absatz 1 nicht erfüllt.</p> <p>² ...</p> <p>³ Kontrolliert eine Anbieterin im Sinne von Artikel 963 Absatz 2 des Obligationenrechts¹ ein oder mehrere rechnungslegungspflichtige Unternehmen, so sind bei der Bestimmung der Anzahl der Teilnehmenden und des Jahresumsatzes die Anbieterin und die kontrollierten Unternehmen als Einheit zu betrachten.</p> <p>...</p>	<p>¹ Eine AAKD gilt für alle bestimmte von ihr angebotenen abgeleiteten Kommunikationsdienste als AAKD mit reduzierten Pflichten, wenn im Durchschnitt der letzten 12 Monate (Stichtag: 30. Juni) die Anzahl der Teilnehmenden des betreffenden Dienstes für alle von der Anbieterin angebotenen abgeleiteten Kommunikationsdienste mindestens 5000 ANZAHL* betragen hat und sie die Voraussetzungen nach Artikel 16g Absatz 1 nicht erfüllt.</p> <p>² ...</p> <p>³ Kontrolliert eine Anbieterin im Sinne von Artikel 963 Absatz 2 des Obligationenrechts¹ ein oder mehrere rechnungslegungspflichtige Unternehmen, so sind bei der Bestimmung der Anzahl der Teilnehmenden für diesen bestimmten Dienst und des Jahresumsatzes die Anbieterin und die kontrollierten Unternehmen als Einheit zu betrachten.</p> <p>...</p> <p><i>*Kommentar: asut macht keinen Vorschlag für eine konkrete Anzahl. Diese soll durch eine Marktstudie abgeklärt werden.</i></p>
<p>Art. 16g AAKD mit vollen Pflichten (neu)</p> <p>¹ Der Dienst ÜPF erklärt eine AAKD für alle von ihr angebotenen abgeleiteten Kommunikationsdienste zur AAKD mit vollen Pflichten, wenn:</p> <ul style="list-style-type: none"> a. im Durchschnitt der letzten 12 Monate (Stichtag: 30. Juni) die Anzahl der Teilnehmenden für alle von der Anbieterin angebotenen abgeleiteten Kommunikationsdienste mindestens 1 Million betragen hat; oder b. der Jahresumsatz in der Schweiz des gesamten Unternehmens in den beiden vorhergehenden Geschäftsjahren mindestens 100 Millionen Franken betragen hat. <p>² Für die Bestimmung der Anzahl der Teilnehmenden und des Jahresumsatzes gilt Artikel 16f Absatz 3.</p> <p>...</p>	<p>Art. 16g AAKD mit vollen Pflichten (neu)</p> <p>¹ Der Dienst ÜPF erklärt eine AAKD für alle bestimmte von ihr angebotenen abgeleiteten Kommunikationsdienste zur AAKD mit vollen Pflichten, wenn beide der nachstehenden Größen erreicht werden:</p> <ul style="list-style-type: none"> a. im Durchschnitt der letzten 12 Monate (Stichtag: 30. Juni) die Anzahl der Teilnehmenden für den betreffenden Dienst für alle von der Anbieterin angebotenen abgeleiteten Kommunikationsdienste mindestens 1 Million betragen hat; oder und b. der Jahresumsatz in der Schweiz des gesamten Unternehmens mit einem bestimmten abgeleiteten Kommunikationsdienst in den beiden vorhergehenden Geschäftsjahren mindestens 100 Millionen Franken betragen hat. <p>²Für die Bestimmung der Anzahl der Teilnehmenden und des Jahresumsatzes gilt Artikel 16f Absatz 3</p> <p>...</p>
<p>Art. 19 Abs. 1 (in Verbindung mit Art. 21 Abs. 1 Bst. a)</p> <p>¹ Die FDA, die AAKD mit reduzierten Pflichten, die AAKD mit vollen Pflichten und die Wiederverkäuferinnen gemäss Artikel 2 Absatz 1 Buchstabe f BÜPF müssen sicherstellen, dass die Teilnehmenden mit geeigneten Mitteln identifiziert werden.</p>	<p>Art. 19 Abs. 1 (in Verbindung mit Art. 21 Abs. 1 Bst. a)</p> <p>¹ Die FDA, die AAKD mit reduzierten Pflichten, die AAKD mit vollen Pflichten und die Wiederverkäuferinnen gemäss Artikel 2 Absatz 1 Buchstabe f BÜPF müssen sicherstellen, dass die Teilnehmenden mit geeigneten Mitteln identifiziert werden.</p>

Vorentwurf E-VÜPF	Änderungsanträge asut (fett bzw. durchgestrichen markiert)
Art. 21 Abs. 1 Bst. a a. die FDA, die AAKD mit reduzierten Pflichten und die AAKD mit vollen Pflichten: die Angaben über die Dienste und die Angaben zum Zweck der Identifikation nach Artikel 19 Absatz 1;	Art. 21 Abs. 1 Bst. a a. die FDA, die AAKD mit reduzierten Pflichten und die AAKD mit vollen Pflichten: die Angaben über die Dienste und die Angaben zum Zweck der Identifikation nach Artikel 19 Absatz 1;
Art. 19 Abs. 2 ² Die FDA haben bei professionell betriebenen öffentlichen WLAN-Zugängen, bei denen sie den Internetzugang erbringen, sicherzustellen, dass alle Endbenutzerinnen und -benutzer mit geeigneten Mitteln identifiziert werden.	Art. 19 Abs. 2 ² Die FDA haben bei Bei professionell betriebenen öffentlichen WLAN-Zugängen, bei denen sie den Internetzugang erbringen, haben die Anbieterinnen der WLAN-Zugänge sicherzustellen, dass alle Endbenutzerinnen und -benutzer mit geeigneten Mitteln identifiziert werden.
Art. 27 Abs. 2 Das Auskunftsgesuch enthält bei natürlichen Personen jeweils das erste sowie mindestens ein weiteres Anfragekriterium des zugrundeliegenden Auskunftstyps, bei juristischen Personen jeweils den Namen und optional den Sitz.	Art. 27 Abs. 2 (bisher) Das Auskunftsgesuch enthält bei natürlichen Personen jeweils das erste sowie mindestens ein weiteres Anfragekriterium des zugrundeliegenden Auskunftstyps, bei juristischen Personen jeweils den Namen und optional den Sitz.
Art. 38a Abs. 2 Auskunftstyp IR_58_IP_INTERSECT: Benutzeridentifikation durch Schnittmengenbildung (neu) ³ Das Auskunftsgesuch enthält die folgenden Angaben über jede der angefragten Internetverbindungen: a. die öffentliche Quell-IP-Adresse; b. falls für die Identifikation notwendig: 1. die öffentliche Quell-Portnummer, 2. die öffentliche Ziel-IP-Adresse, 3. die Ziel-Portnummer, 4. den Typ des Transportprotokolls; ...	Art. 38a Abs. 2 Auskunftstyp IR_58_IP_INTERSECT: Benutzeridentifikation durch Schnittmengenbildung (neu) ³ Das Auskunftsgesuch enthält die folgenden Angaben über jede der angefragten Internetverbindungen: a. die öffentliche Quell-IP-Adresse; b. falls für die Identifikation notwendig: 1. die öffentliche Quell-Portnummer, 2. die öffentliche Ziel-IP-Adresse, 3. die Ziel-Portnummer, 4. den Typ des Transportprotokolls; ...
Art. 50a Die Anbieterinnen mit reduzierten Pflichten und die Anbieterinnen mit vollen Pflichten entfernen die von ihnen oder für sie angebrachten Verschlüsselungen. Sie erfassen und entschlüsseln dafür den Fernmeldeverkehr der überwachten Person an geeigneten Punkten, damit die Überwachungsdaten ohne die vorgenannten Verschlüsselungen geliefert werden. Die Ende-zu-Ende-Verschlüsselungen zwischen Endkunden sind davon nicht betroffen.	Art. 50a Die Anbieterinnen mit reduzierten Pflichten und die Anbieterinnen mit vollen Pflichten entfernen die von ihnen oder für sie angebrachten Verschlüsselungen. Sie erfassen und entschlüsseln dafür den Fernmeldeverkehr der überwachten Person an geeigneten Punkten, damit die Überwachungsdaten ohne die vorgenannten Verschlüsselungen geliefert werden. Die Ende-zu-Ende-Verschlüsselungen zwischen Endkunden sind davon nicht betroffen.

Vorentwurf E-VÜPF	Änderungsanträge asut (fett bzw. durchgestrichen markiert)
Art. 55a Überwachungstyp RT_61_NA_CC-TRUNC_IRI: Echtzeitüberwachung von Randdaten und gekürzten Inhalten bei Netzzugangsdiensten (neu) ...	Art. 55a ist ersatzlos zu streichen
Art. 60a Überwachungstyp HD_62_IP: rückwirkende Überwachung zum Zweck der Teilnehmeridentifikation bei Internetverbindungen (neu) ...	Art. 60a ist ersatzlos zu streichen
Art. 74c Abs. 2 Die FDA mit vollen Pflichten müssen Auskünfte gemäss den Artikeln 38a, 42a und 43a innerhalb von 6 Monaten nach Inkrafttreten dieser Änderung erteilen können.	Art. 74c Abs. 2 Die FDA mit vollen Pflichten müssen Auskünfte gemäss den Artikeln 38a, 42a und 43a innerhalb von -6- 18 Monaten nach Inkrafttreten dieser Änderung erteilen können.
Art. 74c Abs. 3	Art. 74c Abs. 3 Art. 74 Abs. 3 ist ersatzlos zu streichen. Eventualiter ist eine Umsetzungsfrist von mindestens 18 Monaten festzuschreiben.

Monsieur le Conseiller fédéral
Beat Jans
Chef du Département fédéral de
justice et police (DFJP)
3003 Berne

Par email :
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Genève, le 6 mai 2025

Consultation : Ordonnances sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT)

Monsieur le Conseiller fédéral,

Le 29 janvier, le Département fédéral a mis en consultation un projet de révision partielle de deux ordonnances sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT).

La Chambre de commerce, d'industrie et des services de Genève (CCIG) tient à faire part de sa position sur ce projet compte tenu de son importance pour une partie de ses membres, et pour l'économie suisse et genevoise.

D'une manière générale, la CCIG estime que les propositions contenues dans ce projet constituent une menace sérieuse pour le maintien ainsi que le développement du secteur technologique suisse. À ce titre, nous nous opposons, sur le principe, aux révisions partielles de l'OSCPT et de l'OME-SCPT. Il nous semble que l'adoption de ce projet, à tout le moins sans modifications substantielles, compromettrait gravement les perspectives de croissance du secteur technologique suisse de même que son maintien.

1. Menace sur la confiance des utilisateurs

L'élargissement massif de la surveillance étatique, couplé à une réduction des garanties judiciaires, met à mal la confiance accordée d'une manière générale par les clients, entreprises et particuliers, en Suisse et à l'étranger, des entreprises visées par cette révision. Le texte, dans sa formulation actuelle, est si large qu'il engloberait potentiellement l'ensemble des entreprises technologiques suisses, mettant en péril leur compétitivité à un moment où le secteur connaît une opportunité de croissance sans précédent en Europe.

Certaines mesures, telles que l'obligation généralisée de conservation des métadonnées, rapprocheraient la Suisse des standards en vigueur dans des régimes autoritaires plutôt que

de ceux de ses partenaires démocratiques européens ou nord-américains. Cela risquerait de porter un coup durable à la réputation de la Suisse en matière de confidentialité, de sécurité et de confiance – éléments clés de nombreux secteurs économiques.

2. Fragilisation de la compétitivité du secteur technologique suisse

La technologie est un moteur de croissance important. Pourtant, les mesures proposées dans cette révision mettraient un sérieux coup de frein à la compétitivité des entreprises technologiques situées en Suisse. Alors même que les consommateurs et les entreprises recherchent des produits technologiques sûrs, et que le contexte géopolitique favorise l'essor de solutions européennes, il importe que la Suisse préserve son industrie technologique.

Ce projet de révision menace directement cette dynamique : il imposerait un cadre réglementaire plus strict que celui de l'Union européenne ou des États-Unis. Certaines entreprises suisses et genevoises, à l'instar de protonmail, affirment déjà qu'elles ne seraient plus en mesure de proposer des services crédibles basés sur la confiance si elles étaient contraintes à des pratiques de surveillance plus étendues que celles requises aux États-Unis. Le seuil d'utilisateurs proposé pour déclencher des obligations lourdes est particulièrement problématique pour les startups et entreprises en croissance, qui seraient confrontées à des coûts de conformité élevés dès les premiers stades de leur développement, les empêchant d'innover ou de se développer. Aucune exigence similaire n'existe dans les législations européenne ou américaine.

3. Dégât d'image important pour la Suisse

La Suisse bénéficie depuis plus d'un siècle d'une réputation mondiale de neutralité, de stabilité, de sécurité et de respect de la vie privée. Cette image est au cœur de la compétitivité de nombreux secteurs économiques suisses. La révision proposée mettrait fin à cet avantage compétitif unique, en alignant la Suisse non plus sur ses pairs démocratiques mais sur des régimes autoritaires.

Le départ de quelques entreprises technologiques majeures pourrait suffire à ternir durablement l'image de la Suisse comme place sûre pour l'innovation et la protection des données.

4. Conclusion

Au vu des éléments précités, la CCIG considère que le projet de révision de l'OSCPT doit être abandonné. Il existe un intérêt public majeur à préserver le cadre légal actuel, qui garantit un équilibre entre sécurité nationale, compétitivité économique et droits fondamentaux.

En vous remerciant de l'attention que vous voudrez bien porter à ces observations, nous vous prions d'agréer, Monsieur le Conseiller fédéral, l'assurance de notre haute considération.

Chambre de commerce, d'industrie et des services de Genève



Vincent Subilia
Directeur général



Mohamed Atiek
Directeur du Département promotion et soutien à l'économie

La CCIG a pour objectif d'assurer une économie forte, permettant aux acteurs qui constituent le tissu économique local d'exercer leur activité de manière pérenne. Association de droit privé, indépendante des autorités politiques, la CCIG fait entendre la voix des entreprises, par exemple lors de consultations législatives cantonales et fédérales, et en formulant des propositions ayant trait aux conditions cadre. La CCIG compte 2 600 entreprises membres.

Consultation relative aux révisions partielles de l'OSCPT et de l'OME-SCPT

Formulaire pour la saisie de la prise de position

Date	6 mai 2025
Office	Département fédéral de justice et police (DFPJ)
Position de	Proton AG, route de la Galaise 32, 1228 Plan-les-Ouates (GE)
Personne de contact en cas de questions (Nom/tél./courriel)	Marc Alexander Loebekken, +41774273671, marc.loebekken@proton.ch

Merci d'envoyer votre prise de position par courrier électronique à aemterkonsultationen-uepf@isc-ejpd.admin.ch. Un envoi de **votre prise de position en format Word** par courrier électronique facilitera grandement notre travail. D'avance, merci beaucoup.

Remarques générales :

Nous approuvons en principe les révisions partielles de l'OSCPT et de l'OME-SCPT

OUI NON

Le rapport du Conseil fédéral sur la révision en cours indique que la révision vise essentiellement à adapter les ordonnances pour les rendre plus favorables pour les PME. Toutefois, un grand nombre des modifications proposées dépassent le cadre défini par le Conseil fédéral. Contrairement à l'objectif déclaré de « maintenir la charge financière des PME à un niveau bas », la proposition élève une grande majorité des PME à un niveau supérieur et les oblige désormais à participer activement et à grands frais dans des domaines où, jusqu'à présent, il n'existe qu'une obligation de tolérance qui leur était favorable. L'équilibre des intérêts entre les services de poursuite pénale et les fournisseurs concernés se trouve ainsi modifié au détriment de ces derniers. La révision élargit aussi considérablement la surveillance en général.

Les modèles d'affaires d'entreprises suisses bien connues telles que Proton sont remis en question par le projet, et sont même gravement menacés. En particulier, Proton risque d'être contrainte de quitter le pays en raison de l'obligation qui lui est faite d'identifier ses utilisateurs et de conserver les métadonnées de ses utilisateurs pendant 6 mois si l'entreprise veut maintenir sa forte position sur le marché dans le domaine de des communications sécurisées, tant un cadre législatif aussi draconien est unique en Europe. L'adoption de cette révision porte donc indirectement atteinte à l'intérêt de la Suisse pour les applications de haute sécurité exploitées localement.

En outre, le projet conserve les obligations de rétention de données secondaires de communication pour les fournisseurs de services de communication dérivés (FSCD), qui n'ont d'égal nulle part ailleurs en Europe (du fait notamment qu'elles sont illégales dans l'Union Européenne) et dans les démocraties occidentales, plaçant un fardeau sans précédent sur les FSCD ayant des obligations étendues. Le Conseil Fédéral devrait saisir l'opportunité de cette révision pour abolir ce principe pour les FSCD afin de ne pas sévèrement pénaliser l'industrie technologique suisse.

De manière générale, les modifications proposées, ainsi que la non-modification de dispositions problématiques existantes comportent des risques considérables pour la Suisse en tant que lieu d'innovation et d'affaires et ne répondent pas aux objectifs fondamentaux de la révision. La réputation de la Suisse en tant que juridiction propice aux fournisseurs de technologies de l'information dignes de confiance risque d'être sérieusement entachée par la révision.

Enfin, nous tenons à souligner que nous considérons que la technique législative du projet est limitée. Le texte est structuré de manière très confuse, avec un grand nombre de références croisées, et, sous cette forme, il est à peine compréhensible même pour les experts, et encore moins pour les PME, qui sont maintenant confrontées à des obligations beaucoup plus strictes. Le rapport qui l'accompagne est également difficile à lire. Il est difficilement envisageable que le texte puisse être compris par autre que des juristes hautement spécialisés dans cette matière spécifiquement.

Proton propose de rejeter le projet dans son intégralité et invite l'autorité en charge à produire un nouveau document prenant en compte les réalités techniques des services de communication dérivés ainsi que les intérêts stratégiques et économiques de la Suisse, selon les suggestions détaillées ci-après.

Remarques par rapport aux différents articles de l'OSCPT

Article	Proposition	Justification / Remarques
OSCPT		
16b, al. 1	Modifier l'al. 1 comme suit : « Sur demande, le service SCPT déclare un FST comme ayant des obligations restreintes pour un service de télécommunication qu'il offre lorsque ce service »	La nouvelle formulation renforce les critères pour les FST ayant des obligations réduites, ce qui se traduira par une réduction du nombre d'entreprises relevant de l'art. 16a OSCPT. En basant les critères sur le chiffre d'affaires de l'ensemble de l'entreprise au lieu des seules parties concernées, l'innovation des entreprises existantes qui dépassent déjà les seuils est activement entravée, puisqu'elles ne peuvent pas lancer de nouveaux services et de nouvelles fonctionnalités sur le marché sans avoir à remplir l'ensemble des obligations en tant que FST. Les entreprises existantes doivent donc soit renoncer complètement aux innovations, soit accepter des exigences disproportionnées. Les seuils d'application d'obligations supplémentaires doivent être calculés pour chaque service séparément.
16b, al. 1	Supprimer l'al. 1 let b ch. 1	Le seuil d'application basé sur les mandats de surveillance reçus au cours des douze derniers mois ne repose sur aucune base légale dans la LSCPT (art. 26 al. 6 LSCPT), dans la mesure où il est complètement décorrélé de l'importance économique du FST. Il n'est pas rare que de multiples mandats de surveillance soient émis pour une seule et même affaire pénale. Ce critère doit être supprimé au profit du chiffre d'affaires uniquement.
16c, al. 3	Supprimer l'al. 1 let. a	<p>La fourniture automatique d'informations, qui a une fois de plus été considérablement élargie par le nouveau règlement, prive le FST de la possibilité de se défendre contre des demandes erronées ou injustifiées. Cela porte atteinte aux principes de l'Etat de droit de deux manières : premièrement, le contrôle humain est éliminé et deuxièmement, les obstacles existants à l'obtention de ces informations sont abaissés. Les coûts et les efforts constituent des garanties naturelles contre l'utilisation abusive ou disproportionnée de ces mesures.</p> <p>La période de 12 mois envisagée pour la mise en œuvre conforme à la loi d'un système aussi complexe est tout à fait inadéquate. Une mise en œuvre hâtive augmente le risque de graves déficiences techniques et juridiques.</p> <p>En outre, le présent règlement étend considérablement les obligations d'automatisation à toutes les FSCD ayant des obligations complètes et crée plusieurs nouvelles requêtes problématiques telles que IR_59 et IR_60, qui peuvent être susceptibles d'exécution automatique. Le risque d'une élimination complète de l'examen humain des demandes formulées et de la perte de la protection des droits fondamentaux pour les particuliers et les entreprises augmente donc considérablement. Ce risque n'est ni acceptable ni nécessaire dans une démocratie comme la Suisse. La fourniture d'informations automatisées doit donc être supprimée sans remplacement.</p>

Article	Proposition	Justification / Remarques
16d	Supprimer les services de stockage en ligne et les VPN (réseaux privés virtuels) de cette interprétation	<p>Une définition plus claire du terme FSCD est la bienvenue, mais l'interprétation actuelle va bien au-delà de l'objectif légal. La couverture générale des services de stockage en ligne tels que iCloud, OneDrive ou Google Drive, qui sont souvent utilisés exclusivement pour le stockage privé (photos, mots de passe, etc.), est particulièrement problématique. L'art. 2 lit. c LSCPT définit expressément les FSCD comme des services qui « permettent une communication unidirectionnelle ou multidirectionnelle ». Cette définition ne s'applique pas aux services de stockage en nuage personnels, ce qui signifie que leur inclusion dépasse clairement le cadre juridique. Les services de stockage en ligne doivent donc être supprimés de l'art. 16d.</p> <p>En outre, il est admis dans le rapport explicatif que les VPN servent à rendre les utilisateurs anonymes, mais la combinaison avec la révision de l'art. 50a supprime effectivement cette possibilité. Cela empêcherait les services VPN de fournir leur service principal. Les fournisseurs de VPN devraient donc également être exclus de l'article 16d.</p>
16g al. 3 let. a ch. 2	Supprimer l'obligation faites aux FSCD à tout niveau d'obligation de conserver les données secondaires de communication aux fins d'exécuter les surveillance rétroactives	<p>L'obligation de conserver les données secondaires de télécommunications de l'art. 26 al. 5 LSCPT est l'obligation la plus lourde du dispositif de surveillance en Suisse. Si celle-ci découle d'une application directe de la LSCPT pour les FST, tel n'est pas le cas pour les FSCD. En effet, le Conseil fédéral a le pouvoir, et non l'obligation, de soumettre les FSCD à des obligations identiques ou similaires en vertu de l'art. 27 al. 3 LSCPT.</p> <p>Dans le projet soumis à consultation, le Conseil fédéral décide d'appliquer ces obligations de conservation mutatis mutandis aux FSCD, à savoir dans la même mesure qu'appliquées aux FST. Ceci est une grave erreur et une immense pénalité compétitive et concurrentielle pour les FSCD suisses pour les raisons suivantes :</p> <ol style="list-style-type: none"> 1. Contrairement aux autres obligations proportionnées et ciblées de l'OSCPT (p.ex. obligations de surveillance en temps réel), l'obligation de rétention des données secondaires pour une durée de 6 mois demande des ressources et des investissements constants sans rapport de proportionnalité ; ces données doivent être stockées, copiées et/ou préservées et des mesures doivent être prises afin d'en garantir l'intégrité. A titre d'exemple, pour un service comme Proton Mail, ceci devrait être fait pour plus de 100 millions de comptes d'utilisateurs, représentant un investissement en infrastructure de plusieurs millions, voire plusieurs dizaines de millions de francs suisses ; 2. Cette rétention de données représente un risque considérable pour la sécurité et le droit à la vie privée des utilisateurs ainsi que l'intégrité opérationnelle des fournisseurs ; même si l'accès légitime par les autorités pénales à ces données était subordonné à un ordre

Article	Proposition	Justification / Remarques
		<p>du tribunal des mesures de contrainte (ce qui n'est pas systématiquement le cas avec l'introduction des art. 42a et 43a), la rétention de ces données exigerait des FSCD concernés de devoir faire des investissements conséquents pour réduire les risques de cybersécurité associés à la rétention forcée de ces données ; dans une économie et une concurrence globalisée, cela représente un désavantage concurrentiel et réputationnel sérieux et ferait des FSCD suisses ayant des obligations étendues des cibles privilégiées des cyber-attaques ;</p> <p>3. Cette rétention de données indiscriminée a notamment été jugée illicite en 2016 par les autorités judiciaires de l'Union Européenne (CJUE) car considérée comme une violation disproportionnée du droit à l'auto-détermination informationnelle (C-203/15 et C-698/15, Tele2 Sverige and Watson and Others) ; en l'état, la Suisse serait un des uniques états d'Europe à soumettre ses fournisseurs à cette mesure reconnue comme ouvertement abusive chez ses voisins ; ceci consacrerait encore plus profondément le désavantage compétitif et réputationnel des FSCD suisses ; sous cet angle-là, le désavantage causé aux FSCD serait encore beaucoup plus grand que celui causé aux FST, dans la mesure où les FST tendent à délivrer des services ciblés pour la Suisse et entrer en compétition avec des acteurs suisses pour une clientèle principalement suisse;</p> <p>4. Au-delà de l'interdiction par les autorités judiciaires de l'UE de cette pratique, les sociétés américaines (Etats-Unis) ne sont notamment pas sujettes à des obligations similaires. Les FSCD suisses se trouveraient également sujet à un désavantage compétitif extrêmement sérieux vis-à-vis des grandes sociétés technologiques américaines, qui disposent de monopoles ou quasi-monopoles sur ces marchés ; ceci serait particulièrement préoccupant à l'heure où l'on voit émerger en Suisse et en Europe la nécessité d'alternatives viables aux grandes sociétés de technologie américaines (« Big Tech ») et un besoin de plus de souveraineté numérique;</p> <p>5. Il n'est pas démontré que la rétention des données en question causerait une amélioration du taux d'investigations réussies par les autorités de poursuite pénale ; en effet, l'implémentation de telles mesures de rétention devrait être faite de manière transparente par les FSCD, qui devraient informer leurs utilisateurs de ces mesures (obligation de transparence sur la base des lois de protection des données applicables, notamment RGPD et LPD) ; ces utilisateurs pourraient dès lors facilement prendre des mesures de précaution contre l'exploitabilité de ces données, particulièrement les utilisateurs ayant pour objectif de commettre des activités illicites ; pour le surplus, une certaine quantité de données secondaires existent déjà du simple fait de la fourniture du service à l'utilisateur et ces données secondaires sont déjà</p>

Article	Proposition	Justification / Remarques
		<p>fournies sur demandes aux autorités de poursuite pénale en réponse aux ordres de surveillance rétroactifs ;</p> <p>6. Le seul but de cette rétention de données secondaires est l'exécution des ordres de surveillance rétroactifs, qui représentent une quantité marginale des requêtes effectuées par les autorités pénales chaque année en Suisse ; à titre d'exemple, en 2024, sur un total de 410'451 commandes auprès des fournisseurs, le SCPT a ordonné seulement 6'601 ordres de surveillance rétroactives ; ceci correspond à seulement 1,6% de la surveillance effectuée en Suisse par les autorités ; lorsque ce chiffre est mis en perspective avec les implications opérationnelles, réputationnelles et liées à la cybersécurité d'une telle obligation, elle apparaît clairement disproportionnée et inopportun.</p> <p>En conséquence, le Conseil fédéral ne devrait pas faire usage de son pouvoir en vertu de l'art. 27 al. 3 LSCPT. Les FSCD ayant des obligations complètes devraient être soumis à des obligations similaires aux FST (utilisation du système de traitement centralisé, service de piquet, disponibilité à surveiller les communications en temps réel de manière ciblée pour les services pour lesquels un ordre RT existe) à l'exception des mesures de rétention des données. Les FSCD ayant des obligations complètes devraient livrer les données dont ils disposent uniquement en réponse aux ordres de surveillance rétroactifs, comme c'est le cas pour les FSCD avec des obligations minimales et restreintes.</p> <p>Au demeurant, l'existence dans le cadre légal actuel d'un arbitraire complet dans les différents types d'ordres de surveillance rétroactifs existants (HD) rend cette obligation hautement inégale dans son application. Une partie des FSCD (courrier électronique, VoIP, VPN) sont très durement touchés par la conservation des données découlant de l'obligation d'exécuter ces ordres HD en cas d'application, là où de nombreux modèles commerciaux n'en ont aucune (quand bien même le FSCD aurait des obligations étendues), à défaut de l'existence d'un ordre HD correspondant au service qu'ils fournissent.</p> <p>L'obligation pour les FSCD, quel que soit leur niveau d'obligation, de conserver les données secondaires de communication pour exécuter les surveillances rétroactives, devrait donc être supprimée sans remplacement.</p>
16e, 16f, et 16g	Supprimer les articles et adapter les critères existants de manière à ce qu'uniquement le chiffre d'affaires soit pertinent.	Selon le rapport explicatif, la révision prévue de l'OSCPT est destinée à rendre le cadre juridique plus favorable aux PME et à atténuer les requalifications arbitraires des FSCD. Or, le projet présenté est diamétralement opposé à cet objectif déclaré. Au lieu de respecter la proportionnalité, il soumet la grande majorité des PME ayant plus de 5000 utilisateurs mais

Article	Proposition	Justification / Remarques
	<p>Ajouter une exception d'application pour les projets pilotes (y compris de grandes sociétés) et les organisations sans but lucratif.</p>	<p>moins de 100 millions de chiffre d'affaires (ou 1 million d'utilisateurs) à des obligations nettement plus strictes.</p> <p>Selon nous, l'introduction de 5000 utilisateurs comme limite inférieure à évaluer séparément viole également l'Art. 27 para. 3 LSCPT, car 5000 personnes ne constituent en aucun cas un « grand nombre d'utilisateurs » pour lequel les nouvelles mesures de surveillance nettement plus strictes seraient justifiées.</p> <p>En outre, l'introduction d'une unité de groupe dans l'art. 16f para. 3 pose des problèmes considérables, car les produits ne doivent plus atteindre seuls une certaine taille. En particulier dans le cas d'entreprises ayant des sociétés associées en arrière-plan, tous les services et produits relèvent désormais automatiquement du niveau le plus élevé, qu'ils soient encore à un stade précoce ou non. Cela détruit la viabilité économique et entrave l'innovation, car chaque projet doit déjà être planifié avec des obligations de suivi complètes. Cette barrière d'entrée extrêmement élevée nuit durablement à la Suisse en tant que lieu d'innovation.</p> <p>Le postulat 19.4031 d'Albert Vitali, qui critiquait l'utilisation peu fréquente des déclassements, est en contradiction flagrante avec cet état de fait : «La situation des fournisseurs de services de communication dérivés est encore moins favorable. L'ordonnance considère en effet qu'ils sont soumis à la loi, alors que celle-ci ne dit rien de tel. Concrètement, toute entreprise qui propose des services en ligne est ainsi soumise à la LSCPT et doit donc mettre en oeuvre la surveillance. ». Selon le rapport explicatif, au lieu d'alléger le fardeau des PME, la révision conduit en fait à une « mise à niveau automatique par décret sans ordonnance ». Cette approche est manifestement disproportionnée et ne se contente pas de renforcer les exigences, mais oblige même les FSCD de peu d'importance à participer activement et à grands frais.</p> <p>Cette mise à niveau automatique est également source d'une grande insécurité juridique. Dans le système actuel, les normes généralement abstraites de l'OSCPT sont appliquées à un cas particulier par le biais d'une décision. Dans le système révisé, la décision n'est plus nécessaire et un FSCD est automatiquement requalifié dès qu'il atteint la valeur-seuil. Toutefois, la question de savoir si la valeur-seuil a été atteinte peut être difficile à trancher en cas de doute. Il ne fait aucun doute que les FSCD ont un intérêt digne de protection à savoir s'ils devront prendre les mesures supplémentaires étendues qu'ils devront prendre une fois qu'ils auront été re-qualifiés. Toutefois, le FSCD devrait se renseigner activement à ce sujet par le biais d'une décision déclaratoire. Le système actuel est cependant beaucoup plus conforme aux principes généraux de la procédure administrative. Pour des raisons de sécurité juridique, le FSCD ne devrait donc pas être automatiquement re-qualifié. En effet, les profanes et les</p>

Article	Proposition	Justification / Remarques
		<p>PME sensibles aux coûts qui ne disposent pas d'un service juridique spécialisé ne peuvent pas se faire une idée de leurs nouvelles obligations.</p> <p>Par rapport à l'ancienne OSCPT, la révision étend à nouveau de manière significative les obligations d'automatisation à toutes les FSCD ayant des obligations complètes et crée plusieurs nouvelles questions problématiques, telles que IR_59 et IR_60, qui peuvent désormais être interrogées automatiquement et sans intervention manuelle. Or, c'est précisément cette possibilité d'intervention manuelle qui est cruciale pour les fournisseurs afin d'éviter les abus, qui pourraient à leur tour violer les contrats avec leurs clients et le secret des télécommunications. L'automatisation augmente donc considérablement le risque d'utilisation abusive des instruments de surveillance et, partant, le risque pour les droits fondamentaux des personnes concernées. La fourniture d'informations automatisées doit donc être supprimée sans remplacement.</p> <p>La suppression du critère de la « majeure partie de l'activité commerciale » dans l'art. 16g para. 1 (par rapport à l'article 22, paragraphe 1, point b), de l'ancienne OSCPT) signifie qu'une entreprise n'a plus besoin d'offrir des services de communication dérivés en tant que « partie majeure de son activité commerciale » pour être considérée comme une FSCD. Cela signifie que les entreprises qui ne fournissent un outil en ligne qu'à titre expérimental ou pour des raisons caritatives sont également pleinement soumises à la loi. Les conséquences sont graves, car même un projet pilote public entraîne des obligations étendues, telles que les services de garde (article 16g, paragraphe 3, alinéa a, point 1) la fourniture automatisée d'informations (article 16g, paragraphe 3, alinéa b, point 1) et possiblement les obligations de conservation de données secondaires. Cela crée de nouveaux obstacles considérables pour l'innovation en Suisse.</p> <p>Les organisations à but non lucratif telles que la Fondation Signal (si celle-ci était en Suisse) seraient également soumises à ces exigences plus strictes. Alors qu'auparavant elles pouvaient rester soumises à des obligations de tolérance tant qu'elles n'entraient pas dans le champ d'application de l'art. 22 para. 1 OSCPT. Selon les nouveaux critères, le nombre d'utilisateurs est également pris en compte, ce qui signifie que Signal, par exemple, serait désormais enregistré comme une FSCD soumis à des obligations complètes. En Suisse, Signal pourrait ainsi être contraint de se retirer du marché ou s'exposer à des conséquences juridiques importantes, car Signal ne stocke pas les adresses IP et enfreint donc l'article 19 rev-OSCPT et l'art 43a rev-OSCPT. La proposition ignore également les réalités économiques. Un grand nombre d'utilisateurs ne signifie pas que les organisations à but non lucratif sont fi-</p>

Article	Proposition	Justification / Remarques
		<p>nancièrement viables pour mettre en place des mesures de surveillance étendues. Par conséquent, les solutions open source et à but non lucratif sont délibérément écartées du marché, tandis que les monopoles existants tels que WhatsApp (96 % de parts de marché en Suisse) sont renforcés. La nouvelle réglementation n'est donc pas viable d'un point de vue économique et le critère du nombre d'utilisateurs est inadapté et doit être supprimée.</p> <p>Enfin, l'ordonnance affaiblit également la sécurité nationale : surtout à une époque où les cyberattaques se multiplient, elle est contre-productive en termes de politique de sécurité. Aux États-Unis, par exemple, le ministère de la sécurité intérieure encourage délibérément l'utilisation de communications sécurisées et chiffrées de bout en bout et minimisant le traitement des données. La Suisse irait dans la direction opposée avec la réglementation proposée et refuserait effectivement à ses citoyens l'accès à des messageries sécurisées qui ont fait leurs preuves.</p> <p>Dans l'ensemble, l'introduction proposée d'un nouveau niveau d'obligation pour les FSCD ne soulagera pas les PME et n'atténuerà pas le problème de la mise à niveau, mais restreindra le marché, favorisera les monopoles existants, entravera l'innovation, affaiblira la sécurité intérieure et sera en contradiction directe avec le postulat 19.4031.</p> <p>Le système à trois niveaux proposé doit donc être rejeté et le système existant doit être conservé.</p>
16h al. 2	Supprimer la mention du rapport explicatif au profit du nombre d'utilisateurs simultanés	<p>L'art. 16h al. 2 définit l'accès Wi-Fi public comme professionnel si plus de 1 000 utilisateurs peuvent l'utiliser. Le rapport explicatif précise que « ce n'est pas le nombre réel d'utilisateurs de l'accès Wi-Fi concerné » qui est déterminant, mais « le nombre maximal (capacité) qui est pratiquement possible ». Cette interprétation est beaucoup trop large et crée des risques inacceptables pour le FST en combinaison avec l'art. 19 al. 2 rev-OSCPT.</p> <p>Techniquement parlant, il est trivial de configurer un réseau de manière à ce qu'il puisse potentiellement permettre 1000 utilisateurs simultanés, par exemple en utilisant plusieurs sous-réseaux (par exemple 192.168.0.0/24 à 192.168.3.0/24) ou en agrégant des plages d'adresses IP (par exemple 192.168.0.0/22). Même avec les routeurs disponibles dans le commerce pour le marché des particuliers, presque toutes les connexions Internet en Suisse pourraient tomber sous le coup de cette réglementation. Cela imposerait des obligations disproportionnées aux FST, car la distinction n'est plus basée sur la fonction du réseau. Un WLAN ouvert privé, qui ne tombe pas sous le coup de cette réglementation selon la fiche d'information précédente, pourrait désormais être classé comme réseau professionnel. Dans le cadre de la réglementation existante, un FST pouvait procéder à une évaluation sur la base</p>

Article	Proposition	Justification / Remarques
		<p>de l'emplacement (par exemple, une bibliothèque, un aéroport). La nouvelle définition, en revanche, l'obligerait à accéder à n'importe quel réseau privé pour inspecter le matériel et les installations, ce qui est inconstitutionnel et pratiquement impossible. Cette formulation vague entraîne une incertitude juridique permanente pour la FST.</p> <p>L'art. 16h para. 2 devrait donc être supprimé sans remplacement afin de conserver le règlement existant.</p> <p>En outre, la formulation de l'art. 16h pourrait également couvrir des technologies telles que TOR ou I2P. Celles-ci sont utilisées par les journalistes, les lanceurs d'alerte et les personnes vivant dans des états autoritaires pour protéger leur vie privée. Les opérateurs de ces nœuds ne peuvent techniquement pas déterminer quelle personne génère le trafic de données. Une obligation d'identification serait donc non seulement techniquement impossible, mais mettrait également en péril la sécurité de ces utilisateurs et remettrait fondamentalement en question ces systèmes inestimables. Il convient donc de préciser que l'exploitation de systèmes complets ou partiels tels que les nœuds de pont, d'entrée, de milieu et de sortie n'est pas couverte par le OSCPT révisé.</p>
19, al. 1	<p>Supprimer les mentions de « FSCD avec des obligations restreintes » et « FSCD avec des obligations complètes », ou modification en une obligation de fournir toute information collectée mais sans obligation d'identifier les utilisateurs</p>	<p>L'introduction d'une obligation d'identification des abonnés par le FSCD contredit la réglementation antérieure du LSCPT et son interprétation par le Conseil fédéral et les tribunaux de l'OSCPT, qui ne reconnaissent pas une telle obligation d'identification.</p> <p>L'introduction de l'identification obligatoire contredit également les principes de la loi suisse sur la protection des données, en particulier celui de la minimisation des données, en obligeant les entreprises à collecter plus de données que nécessaire, compromettant ainsi massivement la protection des clients suisses. Les entreprises respectueuses de la protection des données sont pénalisées, car leur modèle d'entreprise est compromis et leur argument de vente unique (USP), qui réside souvent précisément dans la minimisation des données et l'excellente protection des données, est invalidé.</p> <p>Au lieu d'une exigence d'identification, le transfert des données existantes doit rester suffisant. Cela permet non seulement de garantir la protection des données, mais aussi de protéger la compétitivité des PME et de renforcer la place de la Suisse en tant que lieu d'innovation.</p>
21 al. 6	<p>Supprimer l'obligation faites aux FSCD à tout niveau d'obligation de conserver les données secondaires de communication</p>	<p><i>Voir commentaire art. 16g al. 3 let. a ch. 2 OSCPT</i></p>

Article	Proposition	Justification / Remarques
	aux fins d'exécuter les surveillances rétroactives (al. 6)	
19, al. 2	Supprimer sans remplacement et maintenir les règles présentement applicables	Comme cela a déjà été mentionné à l'art. 16h al. 2, il n'est pas possible pour un FST de s'assurer juridiquement de la définition utilisée. Le paragraphe doit donc être supprimé sans être remplacé.
22	Supprimer sans remplacement	Comme cela a déjà été expliqué aux articles 16e à 16f, il convient de conserver la division en deux catégories existantes. La suppression de l'art. 22 devrait donc être abrogée.
11, al. 4	Supprimer sans remplacement	Comme cela a déjà été expliqué aux articles 16e à 16f, il convient de conserver la division en deux catégories existantes. L'art. 11 al. 4 devrait dès lors être abrogé sans remplacement.
16b	Supprimer sans remplacement	Comme cela a déjà été expliqué aux articles 16e à 16f, il convient de conserver la division en deux catégories existantes. L'art. 16b devrait dès lors être abrogé sans remplacement.
31, al. 1	Supprimer sans remplacement	Comme cela a déjà été expliqué aux articles 16e à 16f, il convient de conserver la division en deux catégories existantes. Tout ce qui va au-delà d'une obligation de tolérance est inacceptable pour les PME. Le FSCD avec des obligations réduites devrait donc être supprimée de toutes les obligations de l'art. 31 sans remplacement.
51 et 52	Abroger la suppression	Comme cela a déjà été expliqué aux articles 16 sexies à 16 septies, il convient de conserver la division en deux catégories existantes. La suppression des articles 51 et 52 devrait donc être abrogée.
60a	Supprimer sans remplacement	Selon les experts, les mesures rétroactives devraient déjà être considérées avec beaucoup de scepticisme. Selon les notes explicatives, la nouvelle mesure de l'article 60a permet également à une autorité ordonnatrice d'exiger délibérément des résultats faux positifs. Cela condamne objectivement des personnes innocentes et viole ainsi les piliers fondamentaux du système juridique suisse et la présomption d'innocence.
42a and 43a	Supprimer sans remplacement, alternativement supprimer les mentions des protocoles, adresses IP et port du client	<p>Les articles 42a et 43a exigent que le dernier accès à un service soit récupérable, y compris un identifiant de service unique, la date, l'heure et l'adresse IP. Non seulement la limite de 5 000 utilisateurs s'applique à nouveau ici, ce qui couvre donc la quasi-totalité du paysage FSCD en Suisse, mais de telles requêtes devraient désormais pouvoir être effectuées par une simple requête « IR_ », qui, contrairement aux requêtes « HD_ » et la surveillance « RT_ », peuvent être récupérées automatiquement sans autre contrôle juridique, bien que cela implique également la récupération d'une adresse IP dans le passé, tout comme pour les requêtes « HD_ », qui sont beaucoup plus strictement réglementées. Il est incompréhensible et, à notre avis, contraire à la LSCPT que les requêtes au titre de IR_59 et IR_60 soient soumises à des règles plus souples.</p> <p>En outre, le texte de l'ordonnance ne fixe pas de limite à la fréquence à laquelle ces informations automatisées peuvent être fournies. En l'absence de telles limites, une telle demande</p>

Article	Proposition	Justification / Remarques
		<p>pourrait donc être faite automatiquement toutes les 5 minutes, par exemple. Au mieux, cela entraînerait des coûts exorbitants et la ruine financière de l'FSCD concernée. Dans le pire des cas, cependant, les demandes sont envoyées à un système d'information également (facultativement) automatisé et une grande partie des informations qui étaient initialement obtenues via les types d'information/surveillance HD_ et RT_ juridiquement plus sûrs peuvent désormais être obtenues via le type IR_ juridiquement non sécurisé. IR_59 et IR_60 permettent alors de facto une surveillance en temps réel du système sans être soumis aux contrôles requis de ces types de surveillance invasifs.</p> <p>Les deux articles devraient donc être supprimés dans leur intégralité.</p>
50a	Supprimer sans remplacement	<p>L'art. 50a stipule désormais que les fournisseurs sont tenus de supprimer à tout moment le cryptage qu'ils ont eux-mêmes mis en place. Cette obligation ne s'applique plus uniquement aux FST (art. 26 LSCPT) ou, à titre exceptionnel, à certains FST d'une grande importance économique (art. 27 LSCPT), mais doit désormais être appliquée par défaut et sans distinction à tous les fournisseurs comptant plus de 5 000 abonnés. Cela représente une extension significative et problématique des obligations antérieures.</p> <p>Cette extension est non seulement disproportionnée, mais elle met activement en danger l'ensemble du paysage informatique suisse. En obligeant tous les fournisseurs à rendre leurs systèmes de cryptage déchiffrables par les autorités à tout moment, des risques énormes pour la sécurité sont créés : plus il est facile de supprimer le cryptage, plus les systèmes deviennent vulnérables aux attaques de pirates informatiques, à l'utilisation abusive des données et à l'espionnage. Cela est contraire à l'article 13 de la Constitution suisse et à la nouvelle loi suisse sur la protection des données, qui stipule explicitement la protection des données personnelles par des mesures techniques efficaces, en particulier le cryptage. Un cryptage qui peut être supprimé par le fournisseur réduit de toute façon l'efficacité du cryptage. C'est précisément un tel affaiblissement du cryptage qui a récemment été considéré comme une violation des droits fondamentaux par la Cour européenne des droits de l'homme dans l'affaire PODCHASOV c. Russie (33696/19). L'article 50a viole donc également le droit international applicable.</p> <p>Comme déjà mentionné à l'article 16d, l'article 50a empêche également la fourniture efficace de services VPN classiques. Pour un VPN, l'opérateur contrôle à la fois le point d'entrée et le point de sortie. Comme la communication entre le point de sortie et un site web ne peut pas être chiffrée de bout en bout en raison de la structure actuelle de l'Internet en général, même les petits VPN sont obligés de supprimer leur propre chiffrement et de surveiller leurs clients. Comme la protection de la vie privée des utilisateurs est un aspect essentiel de leur service,</p>

Article	Proposition	Justification / Remarques
		<p>cela les désavantage indûment sur le marché et les prive même de leur raison d'être.</p> <p>Mais surtout, le fournisseur d'une application de messagerie ou de courrier électronique doit nécessairement afficher le message dans l'application dans une version lisible par l'homme, et le cryptage de bout en bout est nécessairement déjà supprimé à ce stade. Le libellé de l'article 50a laisse encore ouverte la question de savoir s'il devrait également être possible d'exiger la suppression du cryptage à ce stade, contrairement à toutes les assurances données par le Service SCPT à l'occasion de la dernière révision de l'OSCPT. Compte tenu de la tendance manifeste des autorités de surveillance suisses, au fil des ans, à étendre continuellement le champ d'application de la loi sur la surveillance et à ne se laisser ralentir que par les tribunaux, il est nécessaire d'apporter une nouvelle fois des éclaircissements à ce sujet, selon lesquels la suppression du cryptage qui n'est installé que dans la sphère de l'utilisateur (bien que par le logiciel du fournisseur) ne peut être exigée.</p>
62 let. a et b	<p>Modifier les let. a et b comme suit : «</p> <p>a. pour chaque envoi et réception de courrier électronique : si ces données existent, la date, l'heure, le type d'événement, les identifiants d'usager, les éventuels alias de messagerie, les adresses de l'expéditeur et du destinataire, le protocole utilisé, le statut de remise du message, ainsi que les adresses IP, les numéros de port et les noms du serveur de courrier électronique expéditeur et destinataire ;</p> <p>b. pour chaque connexion ou déconnexion à la boîte de courrier électronique : si ces données existent, la date, l'heure, le type d'événement, les identifiants d'usager, les adresses IP et numéros de port du serveur et du client.</p>	<p>L'ordonnance est élaborée de manière que l'existence de types de surveillance HD détermine les données qui doivent être retenues par les fournisseurs soumis à des obligations de conserver les données secondaires pour la surveillance. Il est donc extrêmement important de bien définir les ordres HD car ceux-ci influencent directement les obligations des fournisseurs.</p> <p>En l'espèce, la let. a est construite de manière à exiger un certain type de données pour chacun des événements suivants : envoi, réception, connexion à la boîte de courrier électronique. Toutefois, certaines données demandées en lien avec chacun de ces événements ne font pas sens technique. Par exemple, il n'existera jamais d'adresse du destinataire pour un événement de connexion ou de déconnexion à la boîte de courrier électronique, puisque l'existence d'une adresse du destinataire implique nécessairement un envoi ou une réception de courrier électronique. D'autres incohérences existent et rendent extrêmement confus pour les fournisseurs le type de données qui devraient être retenues en cas d'obligations de rétention de données secondaires de surveillance. La structure de l'ordre HD_30_EMAIL doit être repensée intégralement dans afin d'être plus claire.</p> <p>L'exigence de la rétention de toutes les données en lien avec l'ordre HD_30_EMAIL telle qu'existant actuellement n'est pas raisonnable, si bien qu'elle ne pourrait être exécutée sans des investissements extrêmement conséquents pour le fournisseur et sans retenir une quantité de données absolument excessive de tous les utilisateurs (et notamment les données de géo-location pour chaque connexion au service ainsi que chaque courriel envoyé). En outre, l'ordre HD_30_EMAIL tel qu'il existe présentement exigerait d'un fournisseur ayant les obligations complètes de garder une copie de tous les courriers électroniques envoyés et reçus sur son service pour une durée de 6 mois (nonobstant leur suppression et/ou la suppression de</p>

Article	Proposition	Justification / Remarques
		<p>leur compte par l'utilisateur), un nombre extrêmement conséquent de données non-utiles d'un point de vue commercial en lien avec ces courriers électroniques, ainsi que de retenir les adresses IP de connexion et déconnexion d'absolument tous les utilisateurs pour chaque événement de connexion, instaurant un système de surveillance généralisé.</p> <p>A titre d'exemple, pour un fournisseur comme Proton pour son service Proton Mail, cela demanderait de retenir ces données pour plus de 100 millions de comptes existants, ce qui demanderait des développements techniques et infrastructurels estimés entre plusieurs millions plusieurs dizaines de millions de francs suisses (coûts de développement et coûts opérationnels récurrents), ce qui serait de nature à rendre Proton Mail inapte à demeurer compétitif face à ses concurrents internationaux, voire remettre en question la viabilité économique du service en tant que tel. Lorsque mis en perspective avec le fait qu'un service comme Proton Mail a seulement reçu 61 ordres HD_30_EMAIL des autorités suisses au cours de l'année 2024, le rapport entre l'obligation de conservation et son utilité pratique pour la poursuite des infractions pénales apparaît largement disproportionné. Ce d'autant plus qu'il est constaté que ces ordres, malgré l'absence d'obligations de rétention de données secondaires pour Proton Mail à ce jour, permettent déjà la transmission d'un nombre conséquent des données utiles aux forces de l'ordre sur la base des données existantes et nécessaires pour l'opération du service (les services de courrier électronique étant des services de communication écrite asynchrones, leur opération usuelle génère nécessairement déjà beaucoup de données secondaires qui sont disponibles).</p> <p>Pour le surplus, il est à noter que l'ordre HD_30_EMAIL est l'un des seuls ordres de surveillance rétroactif concernant un service de communication dérivé spécifique dans l'OSCPT. Il existe donc indéniablement un arbitraire total dans l'établissement de l'ordonnance dans la mesure où uniquement ce type de service serait seul sujet à ces obligations de rétention extrêmement intrusives là où de nombreux autres services de communication dérivés pouvant exister selon l'OSCPT, n'en auraient aucune, à défaut d'existence d'un ordre HD pour leur type de services. Il n'existe pas de justification pour la quasi-exclusivité des obligations de conservation extrêmement lourdes imposées aux fournisseurs de courrier électronique.</p> <p>Il est difficile d'expliquer pourquoi de telles disparités existent et pourquoi un nombre très faible de services dérivés ont des obligations extrêmement intrusives et coûteuses là où de nombreux autres n'en ont aucune ou n'en ont que des limitées. Il semblerait que l'ordre HD_30_EMAIL ait initialement été pensé par le législateur comme un ordre affectant un service de télécommunication et c'est donc dans cet esprit que des obligations extrêmement in-</p>

Article	Proposition	Justification / Remarques
		<p>trusives ont été imposées sur ce type de service (afin d'imposer un niveau d'obligation similaire à celui d'un fournisseur d'accès internet ou de téléphonie, qui sont des FST). Cette interprétation de la LSCPT a été depuis rejetée par le Tribunal Administratif Fédéral, qui a confirmé que les services de courrier électronique tels que Proton Mail n'étaient pas des fournisseurs de services de télécommunication (A-5373/2020). Il semblerait dès lors plus cohérent que leurs obligations soient à tout le moins moins intrusives afin d'être plus proches de celles des autres services de communication dérivés dans l'OSCPT.</p> <p>C'est la raison pour laquelle, en sus d'une refonte de la structure de l'article lui-même, il est impératif d'ajouter systématiquement « si ces données existent », afin que l'ordre HD_30_EMAIL ne crée pas d'obligations de conservation déraisonnables complètement décorrélées de ce qui est généralement pratiqué par les fournisseurs et exigé des autres services de communication dérivés. La suppression de l'obligation de rétention de données secondaires pour les services de communication dérivés, telle que proposée à l'art. 16g de la présente réponse, viendrait également rectifier cette discrimination arbitraire des services de courrier électronique.</p>

Remarques par rapport aux différents articles de l'OME-SCPT

Artikel Article Articolo	Antrag Proposition Richiesta	Begründung / Bemerkung Justification / Remarques Motivazione / Osservazioni
OME-SCPT		
14, al. 3 VD-ÜPF	Supprimer sans remplacement	Comme déjà mentionné dans l'art. 16e à 16f Rev. OSCPT, l'intervention active pour tous les FSCD (y compris ceux qui comptent plus de 5 000 utilisateurs) est disproportionnée et non viable économiquement. Le paragraphe doit donc être supprimé sans remplacement.
14, al. 4 VD-ÜPF	Modifier le terme «FSCD avec des obligations minimales» en «FSCD sans obligations complètes»	La formulation proposée élargit le champ d'application du paragraphe et augmente considérablement le nombre d'FSCD qui en font l'objet. La formulation « FSCD sans obligations complètes » devrait donc être utilisée pour éviter les problèmes déjà abordés dans les articles 16e à 16f de la révision de la LSCPT.
20, al. 1 VD-ÜPF	Supprimer la phrase «et les fournisseurs avec des obligations réduites»	Comme déjà mentionné dans les art. 16e à 16f de la révision de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT), l'intervention active pour tous les FSCD (y compris ceux qui comptent plus de 5 000 utilisateurs) est disproportionnée et économiquement non viable. La sous-clause devrait donc être supprimée sans remplacement.



L'association des
consommateur·rice·s

Département fédéral de justice et police
A l'attention de Monsieur le Conseiller
fédéral Beat Jans

Par courriel : ptss-aemterkonsultationen@isc-ejpd.admin.ch

Lausanne, le 6 mai 2025

Consultation sur la révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT)

Monsieur le Conseiller fédéral,
Madame, Monsieur,

La Fédération romande des consommateurs (ci-après : la FRC) vous remercie de l'avoir associée à la consultation visée sous référence.

Celle-ci a trait à des domaines spécifiques qui n'entrent pas directement dans le champ de compétences de la FRC ; néanmoins, elle touche à des questions extrêmement sensibles sous l'angle de la protection des données, de même que sous l'angle des services numériques qui sont et seront offerts en Suisse aux consommatrices et consommateurs. Ainsi, elle appelle de notre part les remarques générales et/ou questionnements suivants.

En premier lieu, il est indéniable que l'enregistrement et la conservation des données visées dans les ordonnances soumises à consultation peuvent porter atteinte aux droits fondamentaux des utilisateurs concernés, en particulier à leur droit au respect de la vie privée et à l'autodétermination informationnelle. En effet, c'est déjà le cas sous le régime actuel de la LSCPT et la validité des justifications concrètement invoquées jusqu'ici n'ont pas encore été tranchées définitivement par la Cour européenne des droits de l'homme, qui doit statuer sur l'affaire ayant donné lieu à l'ATF 144 I 126 (arrêt 1C_598/2016 du 2 mars 2018). Dans ce contexte, on peut légitimement douter de l'opportunité d'étendre le régime d'obligations existant.

Ensuite, la FRC s'inquiète de la réaction très vive de plusieurs entreprises suisses ou établies en Suisse et qui fournissent des services numériques par rapport au contenu des ordonnances soumises à consultation. En effet, il semble que plusieurs d'entre elles envisagent très sérieusement de s'établir à l'étranger si les projets d'ordonnances ici visés devaient entrer en vigueur, car cela menacerait leur modèle commercial. Cela est préoccupant à plusieurs titres. Cela questionne

FÉDÉRATION ROMANDE DES CONSOMMATEURS

Indispensable et indépendante, la FRC est la plus grande association de défense des consommateurs en Suisse

Rue de Genève 17 | CP 585 | 1001 Lausanne | Tél. 021 331 00 90 | frc.ch/contact | **frc.ch**

d'abord très sérieusement sur la proportionnalité des mesures envisagées. Une telle réaction laisse aussi craindre que les consommateurs puissent prochainement se retrouver avec des options très limitées, voire inexistantes, lorsqu'ils cherchent des alternatives aux grands fournisseurs de services numériques américains, dans un contexte géopolitique qui est particulièrement sensible actuellement et dans lequel la tendance va plutôt vers des tentatives de mieux protéger ses données et donc de réduire la dépendance vis-à-vis de fournisseurs établis outre-Atlantique.

A cela s'ajoute qu'à première vue, la quantité de données à conserver selon les nouvelles règles proposées sera véritablement massive, ce qui pose à la fois des questions d'empreinte écologique (auxquelles les consommateurs sont de plus en plus sensibles), mais aussi de sécurité des données. Il serait vraiment regrettable que l'adoption des nouvelles règles envisagées ait pour conséquence une exposition accrue des entreprises et autorités suisses concernées à des cyberattaques, surtout si le nombre de cas dans lesquels les données conservées sont utiles concrètement reste finalement très modeste.

En conclusion, la FRC invite le Département fédéral de justice et police à procéder à une réévaluation sérieuse et à une pesée des intérêts extrêmement minutieuse avant d'aller de l'avant avec les projets d'ordonnances concernés par la présente consultation. Si les risques d'atteinte aux droits de la personnalité et à la protection des données s'avèrent aussi élevés, voire supérieurs aux bénéfices escomptés concernant une minorité de personnes concernées, il est impératif de renoncer sans délai aux modifications envisagées.

Nous vous remercions d'avance de l'intérêt que vous porterez à ces lignes et nous vous adressons, Monsieur le Conseiller fédéral, Madame, Monsieur, nos salutations les meilleures.

Fédération romande des consommateurs



Sophie Michaud Gigon
Secrétaire générale



Aurélie Gigon
Responsable juridique

Par pli simple et e-mail

Département fédéral de justice et police (DFJP)
Monsieur Beat JANS
Conseiller fédéral
Palais fédéral ouest
3003 Berne

Genève, le 6 mai 2025

Consultation relative à la révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT et OME-SCPT) : Prise de position de l'Ordre des avocats de Genève

Monsieur le Conseiller fédéral,

Fort de ses 2'200 membres, l'Ordre des avocats de Genève (ODAGE) représente près de 80% des avocates et avocats exerçant dans le canton. Parmi ses buts, l'ODAGE veille notamment à garantir le respect de l'état de droit et des droits fondamentaux.

Nous avons pris connaissance avec attention du projet de révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication, soit l'Ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT) et l'Ordonnance sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT).

L'ODAGE soutient le principe d'une précision accrue des catégories de personnes tenues de collaborer, d'une gradation plus fine de leurs obligations et d'une adaptation du contenu des ordonnances aux évolutions du marché des fournisseurs de services de télécommunication (FST) et de services de communication dérivés (FSCD), respectivement aux avancées technologiques.

1.

Nous tenons toutefois à rappeler que l'art. 13 de notre Constitution fédérale garantit le droit fondamental à la protection de la sphère intime, y compris le droit pour toute personne d'être protégée contre l'emploi abusif des données qui la concernent. À Genève, le droit à l'intégrité numérique a été inscrit dans la Constitution cantonale (art. 21A). L'enjeu, du point de vue des droits fondamentaux, se situe donc sur le plan des obligations imposées aux FST et aux FSCD en matière de récolte et de conservation des données personnelles, dont le Tribunal fédéral a rappelé, dans son arrêt publié aux ATF 144 I 126 consid. 4.2., qu'elles emportent déjà une atteinte à la sphère privée (art. 8 al. 1 CEDH et 13 al. 1 Cst. féd.), voire à la liberté de réunion et de presse.

De nombreuses obligations imposées (ou précisées) dans le cadre de la révision de l'OSCPT et de l'OME-SCPT entrent en tension avec les droits fondamentaux susmentionnés, comme l'identification des utilisateurs par des moyens appropriés et la conservation des données relatives à la dernière adresse IP de connexion à un service à charge des FSCD comptant plus de 5'000 utilisateurs. De plus, la définition de la nouvelle catégorie des FSCD à obligations complètes (art. 16g P-OSCPT), qui remplace celle des FSCD ayant des obligations étendues en matière de fourniture de renseignements (art. 22 OSCPT) et les FSCD ayant des

obligations étendues en matière de surveillance (art. 52 OSCPT), est de nature à accroître le nombre d'usagers de FSCD dont les données sont recueillies et conservées de façon générale et indiscriminée.

Le Tribunal fédéral a considéré que le système de la LSCPT est conforme au droit supérieur (ATF 144 I 126). Toutefois, cet arrêt a fait l'objet d'un recours à la CourEDH, enregistré sous n° 47351/18. Ce recours s'appuie sur la jurisprudence de la Cour de justice de l'UE¹, qui considère que l'intérêt public à la surveillance des télécommunications pouvait être atteint par une mesure moins incisive qu'une collecte générale et indiscriminée de données de télécommunication. Dans un tel contexte, il y a lieu de revoir le projet de façon qu'il n'entraîne à tout le moins aucun accroissement de la collecte indiscriminée de telles données, qui sont des données personnelles.

2.

Nous relevons également que la légalité de la mise en œuvre des obligations, telles qu'elles sont actuellement rédigées, repose essentiellement sur l'interprétation que les FST et FSCD feront de l'étendue et des modalités desdites obligations. Cette architecture nous paraît imposer des obligations sortant du champ de compétences des FST et FSCD et crée d'importants risques pour le respect des droits fondamentaux.

Des exemples de risques liés à la mise en œuvre des ordonnances révisées se trouvent dans l'art. 19 OSCPT révisée, où l'identification des usagers par des « moyens appropriés » est en l'état laissée à l'appréciation des FST et FSCD, ou encore dans la transmission par les FST et FSCD de renseignements de manière automatisée (art. 16c, 16g et 18 P-OSCPT).

3.

Nous souhaitons également rappeler à votre attention, ainsi qu'à celle du Service de surveillance de la correspondance par poste et télécommunication, que les services de télécommunication sont utilisés par de nombreuses utilisatrices et nombreux utilisateurs soumis à des obligations de secret, y compris les avocates et avocats. Dans ce contexte, nous formulons une réserve fondamentale sur le principe même d'une transmission automatisée de renseignements par des FST.

À ce sujet, nous rappelons que la correspondance échangée par un avocat ou une avocate bénéficie d'un statut privilégié, sous l'angle de la protection de la sphère privée (art. 13 de la Cst. féd. ; art. 8 CEDH). Dans le récent arrêt *Bersheda et Rybolovlev c. Monaco*, 2024, la CourEDH a reconnu que la protection stricte de la correspondance entre une avocate ou un avocat avec son mandant ou sa mandante porte sur l'ensemble des « informations se rapportant à des conversations », soit notamment à toute donnée relative à l'existence, la date ou la durée d'un contact téléphonique ou l'envoi d'un courriel². La saisie et/ou l'exploitation de telles données par l'autorité constitue déjà une ingérence dans le droit au respect du secret de notre correspondance.

La CourEDH a reconnu que la protection de la confidentialité de ces correspondances exige des États la mise en place de garanties procédurales spécifiques, cela dans l'intérêt de protéger la relation de confiance entre l'avocate ou l'avocat et le client ou la cliente³, mais également de la bonne administration de la justice⁴.

Nous relevons que, au même titre que la LRens, l'OSCPT et l'OME-SCPT ne prévoient aucune garantie spécifique visant à protéger notre secret professionnel, ce qui nous paraît contraire au droit supérieur. Nous attirons l'attention de votre autorité que la problématique de l'absence de garanties spécifiques visant à

¹ CJUE, arrêt du 8 avril 2014 nos C-293/12 et C-594/12 Digital Rights Ireland, §§ 57 ss ; arrêt du 21 décembre 2016 nos C-203/15 et C-698/15 Tele2 Sverige, §§ 108 ss ; arrêt du 6 octobre 2020, causes C-623/17 Privacy International, C-511/18 La Quadrature du net et al., C-512/18 French Data Network et al. et C-520/18 .

² CourEDH arrêt du 6 juin 2024 nos. 36559/19 et 26570/19 Bersheda et Rybolovlev c. Monaco, § 73.

³ Cour EDH, arrêt du 21 janvier 2010 no. 43757/05 Xavier Da Silveira c. France, § 36 ; arrêt du 24 juillet 2008 no. 18603/03 André et autre c. France, § 41.

⁴ Cour EDH arrêt du 3 septembre 2015 no. 27013/10 Sérvulo & Associados – Sociedade de Advogados, RL et autres c. Portugal, § 77 ; arrêt du 16 octobre 2007 no. 74336/01 Wieser et Bicos Beteiligungen GmbH c. Autriche, §§ 65-66 ; arrêt du 16 décembre 1992 no. 13710/88 Niemietz c. Allemagne, 1992, § 37.

protéger le secret des avocates et avocats pouvant être indirectement affectés par des mesures de surveillance fait actuellement l'objet d'examen par le Tribunal administratif fédéral, dans le cadre d'un recours déposé par l'un de nos membres (A-4423/2024).



Nous vous remercions de l'attention que vous porterez à la présente et vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de notre très haute considération.



Stéphanie CHUFFART-FINSTERWALD
Présidente de la Commission Innovations
et modernisation du barreau



Sandrine GIROUD
Bâtonnière



Roxane SHEYBANI
Présidente de la Commission
des droits humains

digitalswitzerland | Waisenhausplatz 14 | 3011 Bern

zu Handen von
Bundesrat Beat Jans
Vorsteher, Eidgenössisches Justiz- und Polizeidepartement
Bundeshaus West
3003 Bern

ausschliesslich via E-Mail an ptss-aemterkonsultationen@isc-ejp.admin.ch

Vernehmlassungsantwort Teilrevision VÜPF, VD-ÜPF

Bern, 5. Mai 2025

Sehr geehrter Herr Bundesrat Jans
Sehr geehrte Damen und Herren,

Wir bedanken uns für die Möglichkeit, an der Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) teilzunehmen.

digitalswitzerland lehnt die in den beiden Erlassen enthaltenen Teilrevisionen ab und fordert eine Rückweisung an den Bundesrat zur umfassenden Überarbeitung.

Wir verweisen an dieser Stelle auf die Stellungnahmen unserer Partnerverbände **Swico, asut und SwissICT**, deren Argumentation wir vorbehaltlos unterstützen.

Allgemeine Bemerkungen

Die vorliegende Verordnung verfolgt ein nachvollziehbares Ziel - die Kategorien von mitwirkungspflichtigen Organisationen bei der Fernmeldeüberwachung klarer zu definieren. Derart einschneidende Änderungen, wie sie die vorliegende Verordnung vorsieht und die den betroffenen Unternehmen signifikante neue Pflichten auferlegen, sollten aber nur auf Gesetzesstufe eingeführt werden. Sie müssen verhältnismässig sein und um Rechtssicherheit herstellen. Das Vorgehen über den Verordnungsweg ist hierfür nicht adäquat und schmälernt das Vertrauen der Wirtschaft und der Bevölkerung in den Staat, was für eine nachhaltige, bürgerzentrierte und innovationsfreundliche Digital- und Infrastrukturpolitik schädlich ist. ***Die Vorlage ist daher umfassend zu überarbeiten.***

Erläuterungen

digitalswitzerland unterstreicht, in Anlehnung an die Schreiben der Verbände Swico und asut, bei den folgenden Punkten den Handlungsbedarf:

1. Wirtschaftliche Auswirkungen:

Die Revisionen führen zu negativen Auswirkungen auf den Wirtschaftsstandort Schweiz. Die neuen Regelungen schrecken IT-Anbieter ab, was zu Standortverlagerungen und Innovationshemmung führen könnte. Es bestehen zusätzlich Wettbewerbsnachteile für Schweizer Unternehmen, da ausländische Anbieter weniger betroffen wären. Wir fordern, dass die Wirtschaft bei der Überarbeitung der Vorlage eng einbezogen wird.

2. Eingriff in Grundrechte und Datenschutzbedenken:

Die Revisionen stellen einen starken Eingriff in die informationelle Selbstbestimmung und den Datenschutz dar. Im Zusammenhang mit der Identifikation von Teilnehmern ergeben sich erhebliche rechtliche Bedenken. Insbesondere Art. 19 Abs. 1¹ und Art 50 a² VÜPF sehen wir kritisch. Wir fordern, dass Änderungen mit derartiger Tragweite auf Gesetzesstufe verhandelt und beschlossen werden.

3. Rechtsunsicherheit:

Wir befürchten Rechtsunsicherheit aufgrund unklarer Definitionen von AAKD und der auf unverhältnismässigen Schwellenwerten basierenden automatischen Hochstufung in verschiedene Pflichtstufen. Unternehmen können schwer abschätzen, welche Pflichten für sie gelten. Wir fordern, dass:

- die jeweiligen Dienste FDA und AAKD, bei Unternehmen, die beides anbieten, unabhängig voneinander betrachtet werden (Unterscheidung der Business-Units);
- die Differenzierung der Pflichten für alle Dienste einzeln zu erfolgen hat, d.h., dass auch die wirtschaftliche Bedeutung und die Benutzerschaft pro Dienst berücksichtigt werden (einerseits für alle Fertmeldedienste einer Unternehmung und andererseits separat für alle abgeleiteten Dienste);
- die Kriterien zwingend kumulativ wirken müssen, dass also die volle Überwachungspflicht (mit Ausnahmen - siehe Punkt 4) nur dann zulässig ist, wenn alle Kriterien zutreffen. So soll auch das Kriterium Anzahl Auskunftsgesuche / Überwachungsaufträge - neben Umsatz und Benutzerschaft - mit einbezogen werden, da dies die Relevanz für die Strafverfolgung widerspiegelt.

4. Unverhältnismässige Pflichten für Unternehmen:

Die geplanten Überwachungspflichten, insbesondere die Vorratsdatenspeicherung und die 24/7-Pikettdienste, sind gerade für KMU unverhältnismässig und wirtschaftlich nicht tragbar. Die Kosten und der bürokratische Aufwand würden den Nutzen übersteigen. Wir fordern, dass AAKD von der aktiven Überwachungspflicht ausgenommen und die Pflicht zur Vorratsdatenspeicherung gestrichen wird.

¹ **Art. 19 Abs. 1 VÜPF:** Die Einführung einer Identifikationspflicht ist ein Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 BV) und hält einer Grundrechtsprüfung nach Art. 36 BV (Verhältnismässigkeit) nicht stand. Die Identifikationspflicht widerspricht dem Grundsatz der Datensparsamkeit, da Unternehmen gezwungen werden, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig. Die Einführung einer Identifikationspflicht für die grosse Mehrheit der AAKD widerspricht auch der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht.

² **Art. 50a VÜPF:** Die Schwächung der Verschlüsselung ist als unverhältnismässig im Sinne von Art. 36 BV zu betrachten, da das Resultat nicht in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördendarbeit steht. Außerdem ist sie mit dem Schutz der Privatsphäre (Art. 13 BV) unvereinbar. Eine rückwirkende Aufhebung von Verschlüsselungen würde auch eine Vorratsdatenspeicherung verschlüsselter Inhalte und Keys darstellen, die mit dem Prinzip der Datenminimierung (Art. 6 Abs. 3 DSG) unvereinbar ist. Auch die Ausdehnung der Pflicht zur Aufhebung von Verschlüsselungen auf AAKD stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar, da Art. 27 Abs. 3 BÜPF fordert, dass AAKD "Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten" müssen.



Wir danken Ihnen sehr für die Berücksichtigung unserer Stellungnahme. Für Fragen oder Anregungen sind wir jederzeit zur Stelle.

Freundliche Grüsse,

Franziska Barmettler
Managing Director digitalswitzerland
franziska@digitalswitzerland.com

Guillaume Gabus
Policy & Foresight
guillaume@digitalswitzerland.com

Über digitalswitzerland

Die Dachorganisation digitalswitzerland bringt Wirtschaft, Wissenschaft, Zivilgesellschaft und Behörden zusammen, um eine verantwortungsvolle Grundlage für den digitalen Wandel zu schaffen, dessen Chancen zu nutzen, Risiken zu erkennen und diese zu steuern.

Über einen offenen Dialog und die Schaffung gemeinsamer Rahmenbedingungen will digitalswitzerland zu vertrauenswürdigen digitalen Ökosystemen beitragen und flächendeckende digitale Kompetenz für Gesellschaft und Wirtschaft fördern. Unter Einbezug seiner diversen Mitgliederbasis treibt digitalswitzerland wirkungsvolle Initiativen an, ermöglicht sektorübergreifende und öffentlich-private Zusammenarbeit und schafft so Raum für Innovation.

digitalswitzerland sieht die Digitalisierung als transformative Kraft, die den Menschen in den Mittelpunkt stellt und Ressourceneffizienz, Lebensqualität und Wettbewerbsfähigkeit steigert. Gemeinsam mit Wirtschaft, Wissenschaft, Zivilgesellschaft und Behörden setzt sich digitalswitzerland dafür ein, dass die Schweiz zu den Chancen einer datenbasierten Zukunft beiträgt

digitalswitzerland | Waisenhausplatz 14 | 3011 Bern

à l'attention de
Conseiller fédéral Beat Jans
Chef du Département fédéral de justice et police
Palais fédéral, l'aile ouest
3003 Bern

exclusivement par e-mail à ptss-aemterkonsultationen@isc-eipd.admin.ch

Réponse à la consultation sur la révision partielle de l'OSCPT, OME-SCPT

Berne, 5 Mai 2025

Monsieur le Conseiller fédéral Jans
Mesdames et Messieurs

Nous vous remercions de nous avoir donné la possibilité de participer à la consultation sur la révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT).

digitalswitzerland rejette les révisions partielles contenues dans ces deux ordonnances d'exécution et demande leur renvoi au Conseil fédéral pour une révision complète.

Nous nous permettons de faire référence ici aux prises de position de nos associations partenaires Swico, asut et SwissICT, dont nous soutenons sans réserve l'argumentation.

Remarques générales

La présente ordonnance poursuit un objectif compréhensible - définir plus clairement les catégories d'organisations tenues de coopérer dans le cadre de la surveillance des télécommunications. Des modifications aussi radicales que celles prévues par la présente ordonnance et qui imposent de nouvelles obligations significatives aux entreprises concernées ne devraient toutefois être introduites qu'au niveau de la loi. Elles doivent être proportionnées et viser à établir une sécurité juridique. La procédure par voie d'ordonnance n'est pas adéquate à cet effet et diminue la confiance de l'économie et de la population dans l'État, ce qui est contraire à une politique numérique et d'infrastructure durable, centrée sur le citoyen et favorable à l'innovation. Le projet doit donc être révisé en profondeur.

Explications

digitalswitzerland souligne, en s'appuyant sur les lettres des associations Swico et asut, la nécessité d'agir sur les points suivants :

1. les conséquences économiques :

Les révisions entraînent des conséquences négatives pour la place économique suisse. Les nouvelles réglementations découragent les fournisseurs informatiques, ce qui pourrait entraîner des délocalisations et freiner l'innovation. Il existe en outre des désavantages concurrentiels pour les entreprises suisses, car les fournisseurs étrangers seraient moins touchés. Nous demandons que l'économie soit étroitement associée à la révision du projet.

2. atteinte aux droits fondamentaux et préoccupations en matière de protection des données :

Les révisions représentent une forte atteinte à l'autodétermination en matière d'information et à la protection des données. En ce qui concerne l'identification des abonnés, des doutes juridiques importants se font jour. Nous sommes particulièrement critiques à l'égard de l'art. 19, al. 1¹ et de l'art. 50 a OSCPT.² Nous demandons que des modifications d'une telle portée soient négociées et adoptées au niveau de la loi.

3. l'insécurité juridique :

Nous craignons une incertitude juridique due au manque de clarté des définitions de l'FSCD et à la réévaluation automatique des différents niveaux d'obligation sur la base de seuils disproportionnés. Les entreprises peuvent difficilement évaluer les obligations qui leur sont applicables. Nous demandons que

- les services respectifs FST et FSCD, pour les entreprises qui proposent les deux catégories de services, soient considérés indépendamment les uns des autres (distinction des business units) ;
- la différenciation des obligations doit être effectuée séparément pour chaque service, c'est-à-dire que l'importance économique et le nombre d'utilisateurs par service doivent également être pris en compte (d'une part pour tous les services de télécommunication d'une entreprise et d'autre part séparément pour tous les services dérivés) ;
- les critères doivent impérativement avoir un effet cumulatif, c'est-à-dire que l'obligation de surveillance complète (avec des exceptions - voir point 4) n'est autorisée que si tous les critères sont applicables. Ainsi, le critère du nombre de demandes de renseignements / de mandats de surveillance - en plus du chiffre d'affaires et du nombre d'utilisateurs - doit également être pris en compte, car il reflète la pertinence pour la poursuite pénale.

4. obligations disproportionnées pour les entreprises :

Les obligations de surveillance prévues, notamment la conservation des données et les services de piquet 24h/24 et 7j/7, sont disproportionnées et économiquement insupportables, en particulier pour les PME. Les coûts et la charge bureaucratique dépasseraient les avantages. Nous demandons que les FSCD soient exemptés de l'obligation de surveillance active et que l'obligation de conservation des données soit supprimée.

¹ **Art. 19, al. 1, OSCPT** : l'introduction d'une obligation d'identification constitue une atteinte au droit à l'autodétermination en matière d'information (art. 13 Cst.) et ne résiste pas à un examen des droits fondamentaux au regard de l'art. 36 Cst. L'obligation d'identification est contraire au principe de minimisation des données, car les entreprises sont contraintes de collecter plus de données que nécessaire pour leur activité commerciale. L'introduction d'une obligation d'identification pour la grande majorité des FSCD est également contraire à la réglementation de la LSCPT, qui ne prévoit une telle obligation que pour un très petit nombre des FSCD.

² **Art. 50a OSCPT** : l'affaiblissement du cryptage doit être considéré comme disproportionné au sens de l'art. 36 Cst., car le résultat n'est pas proportionné à la simplification du travail des autorités visée. En outre, il est incompatible avec la protection de la sphère privée (art. 13 Cst.). Une suppression rétroactive des cryptages constituerait également une conservation des données des contenus et clés cryptés, incompatible avec le principe de minimisation des données (art. 6, al. 3, LPD). De même, l'extension de l'obligation de supprimer les cryptages aux FSCD constitue une extension considérable des obligations actuelles, non couverte par la loi, puisque l'art. 27 al. 3 LSCPT exige que les FSCD « offrent des services d'une grande importance économique ou à un grand nombre d'utilisateurs ».

Nous vous remercions vivement d'avoir pris en compte notre avis. Nous restons à votre disposition pour toute question ou suggestion.

Meilleures salutations,



Franziska Barmettler
Managing Director digitalswitzerland
franziska@digitalswitzerland.com



Guillaume Gabus
Policy & Foresight
guillaume@digitalswitzerland.com

A propos de digitalswitzerland

digitalswitzerland réunit le secteur privé, la science, la société civile et les autorités afin de créer une base responsable pour la transformation numérique, d'exploiter ses opportunités ainsi que d'identifier et gérer ses risques.

Par le dialogue et la création de conditions-cadres communes, digitalswitzerland veut contribuer à la mise en place d'écosystèmes numériques fiables et promouvoir la compétence numérique à tous les niveaux de la société et de l'économie. Avec l'aide de ses membres, digitalswitzerland mène à bien des initiatives efficaces, facilite la collaboration intersectorielle, privilégie la participation publique-privée et crée ainsi un espace pour l'innovation.

digitalswitzerland considère la numérisation comme une force de transformation qui place l'être humain au centre. Dans ce cadre, la numérisation est considérée comme un moyen d'améliorer l'efficacité, la qualité de vie et la compétitivité. En collaboration avec le secteur privé, la science, la société civile et les autorités, digitalswitzerland s'engage pour que la Suisse contribue aux opportunités d'un avenir basé sur les données.

c/o Orchis consulting,
av. de la gare 5,
1950 Sion

Genève, le 6 mai 2025

Concerne : Consultation sur les deux ordonnances d'exécution de la surveillance de la correspondance par poste et télécommunication (OSCPT et OME-SCPT).

Introduction

Swiss Respect est une association de droit suisse, comptant 250 membres, qui a pour vocation d'intervenir dans le débat public sur des sujets peu discutés, lorsqu'ils ont trait aux suivants :

1. La sphère et à la propriété privée,
2. Les conditions-cadres économiques,
3. La sécurité du droit
4. Le fédéralisme.

Pour faire part de notre point de vue, nous intervenons dans la presse et sur les réseaux sociaux, à la manière d'un média, et nous interpellons directement nos élus.

Initialement constituée pour défendre la sécurité du droit envers les employés de banques suisses dans la protection de leur sphère privée, SwissRespect a porté nombre d'autres combats comme la défense des forfaits fiscaux, l'opposition à la ratification de la convention de double imposition en matière de succession avec la France ou le rétablissement de la formule magique pour l'élection du Conseil Fédéral.

Analyse du projet soumis

Après examen, notre Comité a estimé que la Loi sur la surveillance des télécommunications (LSCPT) touche de près l'article 13 Cst. relatif au respect de la vie privée, de la correspondance, et des relations postales et de télécommunications ; elle rentre dans le cadre de la mission de l'association SwissRespect. C'est donc sous les aspects de la **protection de la vie privée**, de la **sécurité du droit** et

des **conditions-cadre de l'économie** que nous allons traiter la proposition de modification de l'Ordonnance de surveillance de la correspondance par la poste et télécommunication.

Celle-ci pose à notre avis un problème de forme. En effet l'introduction du rapport explicatif (paragraphe 1.1) indique que l'objectif est de préciser les personnes chargées de collaborer en vertu de l'art. 2 de la loi.

La longueur inhabituelle de ce texte (56 pages) suggère que l'Ordonnance poursuit des objectifs qui vont au-delà de l'objectif annoncé (la clarification des rôles des opérateurs). Celle-ci nous apparaît comme une profonde refonte de l'esprit et du fonctionnement du *reporting* des opérateurs de télécommunication, dans le sens d'une extension des pouvoirs de surveillance de la police.

À notre avis, le texte de la refonte de l'OSCPT n'est pas rédigé de façon suffisamment claire pour que des tiers (même juristes ou spécialistes en télécommunications) puissent comprendre son champ d'action et les mesures prises, et répondre aux questions légitimes qu'ils peuvent se poser.

Pour l'aspect de la constitutionnalité (5.1 du rapport explicatif) nous relevons que les articles 5 et 13 de la Cst., la seule référence est la suivante « Le présent projet en tient compte comme il se doit ».

Arguments et recommandations

Caractère personnel des métadonnées

Le Comité de notre Association a été alerté notamment par les réactions des opérateurs ProtonMail et Infomaniak qui ont jugé les dispositions du projet d'ordonnance trop contraignantes (notamment l'article 38 nouvelle teneur et art. 50a.), à propos de l'*obligation de facto* faite à des opérateurs de fournir des « **backdoors** » aux autorités fédérales, même s'il ne s'agirait que de fournir des **métadonnées**, qui contiennent pour la plupart des informations que la nLPD considère comme relevant incontestablement de la sphère privée. À notre avis, l'ordonnance introduit arbitrairement une divergence entre le droit public et le droit privé sur la définition des données privées.

Cette mesure pourrait compromettre ainsi l'intégrité technique, et potentiellement le fonctionnement des mesures de sécurité dites « end-to-end-encryption », pour **l'ensemble de la population suisse**. Notre préoccupation est que cette exigence compromettrait fatallement les mesures prises par les entreprises et les particuliers pour assurer leur propre sécurité contre un certain nombre de risques tels que : violation de la vie privée par des tiers, espionnage industriel, harcèlement, vol de données, phishing, ou rançonnement.

Caractère exceptionnel et restreint des limitations des droits fondamentaux

En tout état de cause, la limitation du commentaire à propos des articles 5 et 13 Cst. à ce que « Le présent projet en tient compte comme il se doit » n'est pas suffisante, considérant que **la protection de la vie privée et du secret des télécommunications est un principe supérieur qui gouverne la surveillance des télécommunications**.

Une ordonnance ne peut constituer qu'une liste raisonnée **d'exceptions** à ce principe constitutionnel motivées par le principe de proportionnalité : étant entendu que **les exceptions prévues par la LSCPT devraient toujours être interprétées de la façon la plus restreinte possible**.

C'est donc à dessein avons mentionné le **caractère hermétique du texte** qui ne permet pas de distinguer si les exceptions que le projet d'ordonnance introduirait à l'article 13 Cst. seraient bien justifiées, proportionnées et restreintes dans leur **application quotidienne**.

En outre, le **principe de bonne foi** de l'administration repose traditionnellement sur la prémissse que la loi et ses règlements d'application soient clairs et compréhensibles. La contrepartie du principe que « personne n'est censé ignorer la loi » est donc une exigence de **technique législative** : que la loi et les ordonnances soient formulées de façon à être autant que possible compréhensibles par tout citoyen qui fasse un effort raisonnable pour la lire.

En raison de son opacité, la teneur de l'article 50a et en l'absence d'explications satisfaisantes qui soient de nature à dissiper nos préoccupations, il découle du devoir de vigilance de notre Association qu'il nous faut présumer l'hypothèse la plus défavorable : c'est-à-dire que le projet d'Ordonnance, dans son état actuel, viole le droit à la vie privée, ainsi que l'article 8 de la Convention européenne des droits de l'homme, et l'art. 12 de la Déclaration des droits de l'homme, résultant potentiellement en des recours judiciaires en Suisse au auprès de la CEDH.

Maintien des conditions-cadres de l'économie

Notre compréhension est que l'exigence de communiquer des métadonnées ou d'introduire des *backdoors* à la cryptographie causerait une perte d'affaires voire le départ d'opérateurs de télécommunications à l'étranger ce qui constituerait une péjoration de **conditions-cadre de l'économie** de notre pays.

Modifications au texte de l'ordonnance

Indépendamment des exigences de clarification, le projet d'ordonnance devrait être modifié pour expliciter les points suivants.

1. La fourniture de métadonnées, doit être limitée à une liste d'exception dûment listés et en se limiter à une liste de types données non extensible ; et *pour autant qu'elles ne soient pas cryptées de façon à ce que l'opérateur lui-même n'en ait pas connaissance*.
2. En effet, exiger le **décryptage de métadonnées qui ne sont connues que des clients** reviendrait à forcer les opérateurs d'introduire des « backdoors » gouvernementaux dans les systèmes de cryptographie de leurs clients, à leur insu.
3. Dans l'état actuel du droit, **toute intrusion dans la cryptographie d'une personne (même si cette cryptographie est garantie ou exploitée par un opérateur)** doit être **autorisée par un juge**, conformément aux lois sur la protection des données et à la procédure pénale.

En tout état de cause, dans le système juridique suisse fondé sur l'État de droit, il est impératif **d'assurer la clarté des textes**, afin de garantir la prévisibilité des décisions du pouvoir exécutif, et permettre leur examen rigoureux par les pouvoirs judiciaire et politique, ainsi que par les citoyens.

Conclusion

Notre Association estime que le projet d'Ordonnance manque de clarté et contient trop de détails ; cela nous apparaît comme une indication d'une faiblesse de ses principes généraux.

Nous sommes d'avis que ce projet devrait être reformulé pour répondre aux exigences suivantes :

1. Être clairement intelligible, dans ses principes, son application et ses conséquences, par des personnes autres que les rédacteurs eux-mêmes ou des personnes

intimement proches du sujet ; notamment par des membres du Parlement et des citoyens ordinaires (et à fortiori des juristes).

2. Être accompagnée d'un rapport explicatif assorti d'un contexte suffisant, définissant les termes utilisés.
3. Répondre de façon détaillée et factuelle aux questions de fond sur la conformité aux articles 5 et 13 Cst, en donnant des exemples de comment ces dispositions seraient respectées, et susceptibles d'être vérifiées, auditées et sujettes à des recours.
4. Limiter strictement le champ de l'ordonnance aux objectifs énoncés (écartier d'emblée toute suspicion de *hidden agenda*).
5. Viser à la brièveté et à l'énonciation de règles claires ; et déléguer des détails techniques qui ne relèvent pas de principes généraux ou de droits fondamentaux, à des directives d'application ainsi qu'à des circulaires destinées aux spécialistes.
6. Supprimer l'article 50a : la compromission des clés cryptographiques entre personnes et l'autorisation de *backdoors* insérées à l'insu de l'usager constitue un sujet de société, beaucoup trop profond pour être laissé à une Ordonnance émise du pouvoir exécutif. Notre Comité estime la question de l'intrusion dans la cryptographie des personnes touchant de très près à la sphère intangible de l'individu et la Constitution, ne devrait relever que du pouvoir législatif, c'est-à-dire d'un vote des Chambres fédérales, à propos de LSCPT, ce qui la rendrait le cas échéant soumise au référendum populaire.

Dans tous les cas, notre préoccupation est d' assurer le strict respect des clés cryptographiques entre individus et à interdire les backdoors de la cryptographie chez les opérateurs à l'insu des usagers ; réservant aux seuls tribunaux le droit de limiter ou lever les droits fondamentaux garantis par la Constitution.

Pour ce qui est du respect de la bonne foi de l'Administration, la **volonté d'extension des pouvoirs de surveillance sur les télécommunications**, qui nous semble **l'objectif sous-jacent** de cette modification de l'ordonnance devrait être annoncée ouvertement au public et au média, avec la plus grande transparence, afin qu'un large débat politique puisse avoir lieu.

Notre position est que, dans l'esprit de la démocratie helvétique, toute extension des pouvoirs de surveillance de la police sur la vie privée des Suisses devraient compensés, par souci d'équilibre, par un renforcement de la transparence de l'Administration, une plus grande clarification de quelles informations peuvent légitimement être rassemblées ou non et dans quelles conditions, l'assurance d'une surveillance efficace de cette activité par le pouvoir judiciaire, la clarification des droits de recours des usagers et la garantie d'un traitement rapide et équitable ; ainsi de toutes autres mesures prises pour assurer le respect des droits fondamentaux garantis par la Constitution et les traités internationaux.

Swiss Respect

Pour le Comité :



Laurent Franceschetti

Vice-Président

Eidgenössisches Justiz- und Polizeidepartement EJPD
ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 6. Mai 2025

Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF): Vernehmlassung

Sehr geehrter Herr Bundesrat

Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar 2025 wurde die Vernehmlassung zur Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) eröffnet. Gerne nehmen wir hiermit die Möglichkeit wahr, uns zu diesem Gesetzesentwurf zu äussern.

Glasfasernetz Schweiz ist die Interessens- und Informationsplattform der in den Ausbau der Glasfaserinfrastruktur investierenden Unternehmen.

Wir begrüssen grundsätzlich die vorgeschlagene Teilrevision der Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF), sehen jedoch in drei Punkten Klärungs- beziehungsweise Anpassungsbedarf:

- Erstens empfehlen wir die Kategorisierung der Mitwirkungspflichtigen aufgrund der Bedeutung der Dienste, die sich für uns aus der Anzahl der Teilnehmenden, ergibt.
- Zweitens sehen wir die Identifikationspflicht im Bereich WLAN-Zugängen klar bei den eigentlichen Betreibern des WLAN-Zugangs anzusiedeln, nicht bei den Internetzugangsanbietern. Letztere sind nicht in der Lage, Endnutzerinnen und Endnutzer eines WLAN-Zugangs zu identifizieren.
- Drittens regen wir an die Anpassungen zur Benutzeridentifikation, Echtzeitüberwachung und rückwirkender Überwachung zu streichen oder die Umsetzungsfristen praxisnah zu verlängern.

In allen obengenannten Punkten stimmen wir mit der Stellungnahme des asut überein und unterstützen deren entsprechende Ausführungen.

Wir danken für die gebotene Möglichkeit zur Stellungnahme und bitten Sie freundlich, unsere Argumente in der Entscheidfindung zu berücksichtigen.

Freundliche Grüsse



Hans Wicki, Ständerat
Präsident



Lorenz Jaggi
Geschäftsführer

Trust Valley

Fondation EPFL Innovation Park
Bâtiment C
CH-1015 Lausanne
info@trustvalley.swiss

Monsieur le Conseiller fédéral

Beat Jans

Chef du Département fédéral de
justice et police (DFJP)
Palais fédéral ouest
CH-3003 Berne

Lausanne, le 6 mai 2025

Objet : Consultation relative à la révision partielle des ordonnances OSCPT et OME-SCPT

Monsieur le Conseiller fédéral,

Nous avons pris connaissance avec grande attention de la révision partielle des deux ordonnances d'exécution de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (OSCPT et OME-SCPT).

En tant que centre de compétences Suisse en matière de confiance numérique et de cybersécurité de l'arc lémanique, et après consultation de nos partenaires des secteurs public, académique et privé, la Trust Valley reconnaît la nécessité d'adapter les outils de surveillance aux évolutions technologiques et souligne l'importance de protéger les droits fondamentaux et de garantir la sécurité numérique. Toutefois, nous tenons à exprimer nos réserves quant aux modifications proposées et quant aux impacts potentiels sur l'écosystème de la confiance numérique.

Suite à un examen approfondi des textes soumis à consultation, nous souhaitons partager nos réflexions autour de ce que nous percevons comme trois enjeux majeurs :

Premièrement, l'élargissement significatif du dispositif de surveillance étatique, combiné à une évolution du cadre du contrôle judiciaire, soulève des interrogations quant à son potentiel impact sur l'exercice des droits fondamentaux liés à la vie privée et à la sécurité numérique en Suisse. Il nous semble important de veiller à maintenir un équilibre respectueux des valeurs de liberté individuelle qui fondent notre société.

De plus, la portée potentiellement très large des propositions pourrait impliquer un nombre important d'entreprises technologiques suisses, y compris des acteurs clés de l'innovation tels que les startups, les scale-ups et les PMEs. Ceci pourrait avoir des répercussions considérables sur la dynamique de compétitivité d'un secteur stratégique pour l'économie nationale en pleine croissance.

Finalement, certaines orientations envisagées, notamment en matière de conservation des métadonnées, pourraient potentiellement créer un écart entre les pratiques suisses et les normes en vigueur dans les démocraties occidentales, ce qui pourrait avoir des conséquences sur la perception de la Suisse en tant que territoire de confiance, attaché à la sécurité et à la protection de la vie privée.

En alignment avec les positions exprimées par les cantons de Genève et Vaud, la Trust Valley recommande vivement l'ouverture d'un dialogue constructif et inclusif avec les acteurs économiques concernés afin de préserver un environnement propice au développement du secteur de la confiance numérique, élément véritablement stratégique pour l'avenir de la Suisse.

Nous serions ravis d'ouvrir un dialogue avec vous, et par la présente, je me permets de vous inviter à venir visiter la Trust Valley et ses partenaires au sein de l'EPFL Innovation Park et du Campus Unlimitrust dédié à l'économie de la confiance.

Nous restons à votre entière disposition pour toute information complémentaire et nous vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de notre respectueuse considération.

CEO, Trust Valley

Lennig Pedron

Lennig Pedron

Internet Society Schweiz (ISOC-CH)
c/o Ucom Standards Track Solutions GmbH
Heinrich-Wolff-Str. 17
CH-8046 Zürich



Eidgenössisches Justiz- und Polizeidepartement EJPD
Vorsteherin
Herr BR Beat Jans

ptss-aemterkonsultationen@isc-ejpd.admin.ch

Zürich/Genf, 6. Mai 2025

Vernehmlassungsantwort zur Revision VÜPF und VD-ÜPF

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir bedanken uns für Ihr Schreiben vom 29. Januar 2025, in dem Sie uns zu einer Stellungnahme im Rahmen der laufenden Vernehmlassung zur Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) einladen.

Die Internet Society Schweiz (ISOC-CH) ist die anerkannte Schweizer Vertretung (Chapter) der Internationalen Internet Society (ISOC). ISOC wurde 1992 gegründet und hat weltweit über 80'000 Mitglieder, davon mehr als 600 in der Schweiz. ISOC setzt sich seither für technische, soziale und politische Aspekte des Internets und dessen Nutzer ein.

<http://www.internetsociety.org/who-we-are/mission>

Auf nationaler Ebene verfolgt ISOC-CH ähnliche Ziele wie ISOC auf globaler Ebene.

Die Internet Society Schweiz hat sich speziell zum Ziel gesetzt, die Zukunft des Internets hierzulande und weltweit aktiv mitzugestalten, den Informationsaustausch zwischen Internet Benutzern und Experten zu fördern, als Bindeglied zwischen Politik, Internet Benutzern sowie Experten zu agieren, die Schweizer Internet Community auf politischer Ebene zu vertreten sowie bei der Weiterentwicklung von Dienstleistungen und Technologien zu unterstützen.

<http://www.isoc.ch/about/description>

Wir nehmen gerne die Gelegenheit wahr, uns im Rahmen der Vernehmlassung zur Revision der Verordnungen VÜPF und VD-ÜPF zu äussern.

Die Internet Society Schweiz (ISOC-CH) lehnt die vorliegenden Entwürfe zur Revision der Verordnungen VÜPF und VD-ÜPF in Gänze ab.

Die ISOC-CH hat grösste Bedenken im Bezug die Einschränkung des Grundrechte, vor allem des Grundrechts auf Privatsphäre. Grundrechte werden buchstäblich der Überwachung geopfert. Die überaus zahlreichen Überwachungspflichten für die Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD) und die massive Ausweitung der mitwirkungspflichtigen AAKD sind unverhältnismässig. Die geplanten Änderungen gefährden auch die Sicherheit von Verschlüsselung. Insbesondere VPN und andere verschlüsselte Kommunikationsdienste stehen im Fokus – mit potenziell verheerenden Folgen für Bürger und Unternehmen.

Die Pflichten zur Vorratsdatenspeicherung und Identifikation von Nutzern greifen tief in die Grundrechte der Bürger ein. Die Privatsphäre von unbescholtenen Bürgern und insbesondere auch das Arzt-Geheimnis oder der journalistische Quellschutz werden kompromittiert.

Jedes zusätzliche Speichern von Daten erhöht das Risiko für deren Missbrauch. Metadaten können detaillierte Einblicke in Kommunikationspartner, Standorte und Gewohnheiten geben. Die verpflichtende Vorratsdatenspeicherung von Metadaten über sechs Monate ermöglicht nicht nur eine Massenüberwachung, sondern grundsätzlich auch andere unrechtmässige Zugriffe von Dritten, wie Hackern, Kriminellen oder Mitarbeitern der FDA bzw. AAKD. Wenn solche Daten beispielsweise in die Hände von Kriminellen geraten, könnten diese für Erpressung, Telefonbetrug, Phishing, Identitätsdiebstahl oder andere Formen von Missbrauch verwendet werden.

Die vorgeschlagene Pflicht, angebrachte Verschlüsselungen zu entfernen, kompromittiert die Sicherheit der Verschlüsselung. Anbieterinnen würden gezwungen, Hintertüren anzubringen oder andere Methoden einzusetzen, welche die Verschlüsselung bewusst schwächen, um unverschlüsselte Inhalte den Behörden ausliefern zu können. Das Anbringen solcher Sicherheitslücken ermöglicht nicht nur den Behörden, sondern potenziell auch Hackern, Kriminellen oder anderen Unbefugten den Zugriff auf vertrauliche Daten.

Die britische Regierung hat kürzlich ähnliche Vorschriften beschlossen, worauf Apple entschied, diese nicht umzusetzen. Stattdessen kündigte Apple den Rückzug der verschlüsselten Dienste für ihre Kunden in Grossbritannien an.

Zitat: «*Apple und viele IT-Sicherheitsexperten argumentieren, dass eine Hintertür jede Verschlüsselung ad absurdum führt. Sobald ein Weg existiert, um verschlüsselte Daten zu entschlüsseln, ist es nur eine Frage der Zeit, bis Kriminelle oder autoritäre Regime ihn ausnutzen. End-to-End-Verschlüsselung bedeutet genau das: Niemand außer dem Nutzer selbst – nicht einmal Apple – kann auf die Daten zugreifen. Eine Hintertür ist daher immer eine massive Sicherheitslücke.*»¹

In der Schweiz haben Dienste mit Privatsphäre-freundlichen Lösungen traditionell eine starke Stellung. Schweizer Anbieterinnen wie Proton, NymVPN, PVY.swiss oder Threema sind durch die neue Regulierung besonders betroffen. Proton hat bereits angekündigt, die Schweiz zu verlassen, wenn sie hier keine ordnungsgemässen Geschäfte mehr tätigen kann.²

1 <https://www.gizmodo.de/apple-sagt-nein-zu-uk-backdoor-end-to-end-verschlüsselung-faellt-weg-2000014910>

2 <https://www.watson.ch/digital/wirtschaft/517198902-proton-schweiz-chef-andy-yen-zum-ausbau-der-staatlichen-ueberwachung>

Die ISOC-CH teilt auch die Bedenken, Einwände und Vorschläge der Piratenpartei Schweiz und unterstützt hiermit die Vernehmlassungsantwort der Piratenpartei Schweiz.

Wir bedanken uns für die Prüfung und Berücksichtigung unserer Anmerkungen und Vorschläge.

Bei Fragen oder Unklarheiten dürfen Sie jederzeit gerne auf uns zukommen.

Freundliche Grüsse

Internet Society Schweiz (ISOC-CH)
B. Höneisen, Head of Public Policy

Kontakt

Internet Society Schweiz (ISOC-CH)
c/o Ucom Standards Track Solutions GmbH
Bernie Höneisen
Heinrich-Wolff-Str. 17
CH-8046 Zürich

Telefon: +41 44 500 52 40

E-Mail: bernie.hoeneisen@isoc.ch

Internet: <http://www.isoc.ch/>

Von: Sebastian Bürgel
Gesendet: Dienstag, 6. Mai 2025 22:02:35 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Vernehmlassungsantwort zu den Teilrevisionen der VÜPF und der VD-ÜPF gemäss Schreiben des EJPD vom 29. Januar 2025

Datum: 6. Mai 2025

Verfasser: HOPR

Kontaktperson: Dr. Sebastian Bürgel, sebastian.buergel@hoprnet.org, 078 223 02 02

Sehr geehrte Damen und Herren

Im Rahmen des Vernehmlassungsverfahrens zur Teilrevision der VÜPF und der VD-ÜPF reichen wir hiermit unsere Stellungnahme ein. Wir danken Ihnen für die Gelegenheit, uns an diesem Verfahren beteiligen zu dürfen.

HOPR ist ein Schweizer Verein (CHE-244.032.710), der Technologien entwickelt, um private und sichere Datenübertragung zu gewährleisten. Wir sind Teil des florierenden Schweizer Sektors für Privacy-Technologien, der darauf ausgerichtet ist, Nutzerinnen und Nutzern mehr Autonomie über ihre Datensicherheit im Internet zu verschaffen. Zu diesem Umfeld gehören auch international führende Schweizer Unternehmen wie Proton und Threema – ein Sektor, der durch die vorliegende Revision in seiner heutigen Form irreversibel geschädigt würde.

Die vorgeschlagenen Änderungen stehen in direktem Widerspruch zur langjährigen Schweizer Tradition der Förderung und des Schutzes von Grundfreiheiten. Sie führen eine überzogene Überwachung ein, welche die Rechte aller Einwohnerinnen und Einwohner der Schweiz untergräbt. Die Schweiz würde sich dadurch in einen Überwachungsstaat verwandeln, dessen Massnahmen selbst von der EU – die nicht gerade dafür bekannt ist, bürgerliche Freiheiten über staatliche Überwachung zu stellen – als rechtswidrig angesehen würden (vgl. EuGH, C-203/15 und C-698/15 "Tele2/Watson" sowie zahlreiche weitere). Das erfüllt uns mit grosser Besorgnis, denn die Schweiz galt bislang als Bollwerk gegen den weltweiten Trend zur Aushöhlung fundamentaler Rechte auf Autonomie und Privatsphäre – online wie offline.

Darüber hinaus sind diese Revisionen auch aus strategischer Sicht höchst kurzsichtig. Wenn das Ziel darin besteht, datenschutzorientierte Projekte wie Proton, Threema und weitere in diesem innovativen Sektor zu regulieren oder einzuschränken, wird dieses Ziel verfehlt. Diese Projekte werden sich einfach in Länder mit günstigeren gesetzlichen Rahmenbedingungen verlagern – gemeinsam mit ihren Nutzerinnen und Nutzern samt erheblichen Einnahmen. Zurück bleiben Schweizer Bürgerinnen und Bürger sowie Unternehmen, die nicht in der Lage sind, einfach das Land zu verlassen, und die nun mit den Folgen dieser Verordnung leben müssen. Entgegen der Behauptung, die Änderungen würden KMU entlasten, wären die tatsächlichen Auswirkungen kostspielig, tiefgreifend und invasiv.

Wir lehnen die vorgelegten Revisionen in aller Deutlichkeit und mit Nachdruck ab. Allerdings erscheint es angesichts des Umfangs der vorgesehenen zusätzlichen Überwachungsbefugnisse unwahrscheinlich, dass Argumente auf Grundlage des grundrechtlichen Schutzes der Privatsphäre Gehör finden werden.

Deshalb konzentriert sich unsere weitere Stellungnahme auf die neuen Pflichten für Fernmeldedienstanbieterinnen (FDA) und Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD), auf die Schwellenwerte, die zur Auslösung dieser Pflichten vorgesehen sind, sowie auf die (nicht vorhandenen) Definitionen, auf denen diese Schwellen basieren. Entgegen dem erklärten Ziel, KMU zu entlasten und für Klarheit zu sorgen, sind die vorgeschlagenen Pflichten äusserst belastend und unklar formuliert. Die angesetzten Schwellen sind vollkommen willkürlich, praktisch nicht überprüfbar und so vage formuliert, dass sie jeglicher Bedeutung entbehren.

Artikel 16h verpflichtet FDA, die WLAN-Zugang anbieten, zur Umsetzung bestimmter Massnahmen, wenn ein Zugangspunkt als «professionell betrieben» gilt – was dann der Fall sein soll, wenn die «maximale Kapazität» über 1'000 Nutzerinnen und Nutzer beträgt, unabhängig davon, ob diese Zahl jemals erreicht wird. HOPR hat hierzu sein internes Entwicklerteam konsultiert – und selbst unseren erfahrenen Fachleuten ist völlig unklar, was damit gemeint ist. Nicht-technische Anbieter von WLAN-Zugängen dürften noch weniger in der Lage sein, ihre Pflichten zu erkennen.

Wenn die Kapazität als die blosse Fähigkeit zur Verbindung definiert wird, dann überschreitet jeder WLAN-Zugangspunkt diese Schwelle problemlos. Jeder Gastronomiebetrieb, jedes Hotel oder Café mit öffentlichem WLAN wäre betroffen – ebenso wie privat betriebene Router mit offenem Zugang.

Wenn man hingegen versucht, Kapazität über die tatsächliche Nutzung zu definieren – was im Entwurf nicht einmal ansatzweise unternommen wird –, dann würden vermutlich nur sehr wenige Netze als «professionell betrieben» gelten. Beide Auslegungen dürften kaum im Sinne der Revision sein – aber in der vorliegenden Form ist nicht erkennbar, was eigentlich gemeint ist. Eine fundierte rechtliche Einschätzung, ob ein WLAN-Zugang als «professionell betrieben» einzustufen ist, ist auf dieser Grundlage schlicht nicht möglich.

Auch wenn die Pflichten für AAKD gemäss Artikeln 16e–16g etwas präziser erscheinen, bleiben die zugrunde liegenden Schwellenwerte ebenfalls völlig willkürlich. Die Schwelle von 5'000 Nutzerinnen und Nutzern, die angeblich eine «grosse Nutzerzahl» darstellen soll, ist geradezu absurd niedrig. Darüber hinaus ist es mit erheblichem technischen Aufwand verbunden – oder schlicht unmöglich – zu beurteilen, ob diese Schwelle überschritten wurde und damit zusätzliche Meldepflichten ausgelöst werden. Gängige Sicherheitstechniken machen es oft unmöglich zu erkennen, ob verschiedene Nutzungsvorgänge von einer oder mehreren Personen stammen. Daraus ergibt sich, dass AAKD ihre Nutzerinnen und Nutzer identifizieren müssen – unabhängig davon, ob sie die Schwelle überschreiten oder nicht –, da dies die einzige Möglichkeit ist zu bestimmen, welcher Kategorie sie angehören und welche Pflichten für sie gelten. Diese Zirkularität macht das gesamte Kategoriensystem sinnlos.

In der vorliegenden Fassung ist diese Revision nicht rechtskonform umsetzbar. Die vorgesehenen Schwellenwerte sind unzureichend definiert und führen zu Pflichten, die faktisch nicht erfüllbar sind. Die Verantwortung für diese unlösbare Situation wird volumnäiglich den KMU aufgebürdet – also Unternehmen, die in der Regel nicht über das nötige technische Know-how verfügen, um solche Regelungen korrekt zu interpretieren. Dies

widerspricht fundamental dem erklärten Ziel der Revision, die Belastung von KMU zu reduzieren.

Wir sind überzeugt, dass diese Mängel im Rahmen des aktuellen Vernehmlassungsverfahrens nicht behoben werden können. Daher fordern wir, dass die Revisionen abgelehnt werden, und regen an, dass ein neuer Anlauf unternommen wird – unter Einbezug von Unternehmen aus dem schweizerischen Privacy-Tech-Sektor, die genau wissen, wie man die Gratwanderung zwischen dem Schutz individueller Rechte und der Integrität des Gesamtsystems der Kommunikationsinfrastruktur erfolgreich meistert. HOPR wäre gerne bereit, sich in diesen Dialog einzubringen.

Zum Schluss noch ein Warnhinweis: Uns ist bewusst, dass der Ausbau der Datenerhebung auf den ersten Blick verlockend erscheint. Es scheint einleuchtend, dass mehr Informationen zu mehr Sicherheit, besserer Entscheidungsfindung und höherer Vorbereitung führen.

Doch das ist eine Illusion – ähnlich jener, der sich die Regierungen der USA und des Vereinigten Königreichs während ihrer fehlgeleiteten «Kriege gegen den Terror» hingegeben haben. Die Schweiz war nie ein Überwachungsstaat und sollte es auch niemals werden. Helfen Sie nicht dabei, sie zu einem solchen zu machen. Diese Revisionen werden die Datensicherheit der Schweizer Bevölkerung nicht verbessern – sie werden sie aktiv gefährden. Die vorgeschlagene Verordnung verpflichtet dazu, grosse Mengen an personenbezogenen Daten von Schweizer Bürgerinnen und Bürgern zu sammeln und zu speichern – und überträgt diese Aufgabe an Unternehmen und Einzelpersonen, die weder über die Ressourcen noch das Fachwissen verfügen, um diese Daten sicher zu verarbeiten. Die bisherige Erfahrung zeigt eindeutig: Kein Staat, kein Unternehmen und kein Individuum hat je gezeigt, dass sich die mit solchen Datensammlungen verbundenen Risiken effektiv beherrschen lassen. Der einzige sichere Weg, die Daten der Schweizer Bevölkerung zu schützen, ist: So wenige Daten wie möglich zu erheben und zu speichern.

Wir gehen davon aus, dass diese Einwände ungehört verhallen werden. Unser Gewissen verpflichtet uns dennoch, sie vorzubringen.

Mit freundlichen Grüßen
HOPR

--
Dr. Sebastian Bürgel
Founder
[@SCBuerge1](https://twitter.com/SCBuerge1)

Piratenpartei Schweiz, 3000 Bern

Stellungnahme der Piratenpartei Schweiz zu den Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat Jans

Sehr geehrte Damen und Herren

Bezugnehmend auf Ihre Vernehmlassungseröffnung vom 29.01.2025 nehmen wir gerne Stellung.

Vorab, wir Piraten finden es sehr bedenklich, dass Sie für die Stellungnahme auf eine proprietäre Software verweisen (Word der Firma Microsoft), wo es doch heute zahlreiche offene und freie Dateiformate gibt. Wir entsprechen ihrem Wunsch mit einer docx-Datei, welche auch in neueren Word Versionen geöffnet werden kann.

Die Piratenpartei Schweiz setzt sich seit Jahren für eine humanistische, liberale und progressive Gesellschaft ein. Dazu gehören die Privatsphäre der Bürger, die Transparenz des Staatswesens, inklusive dem Abbau der Bürokratie, Open Government Data, den Diskurs zwischen Bürgern und Behörden, aber auch die Abwicklung alltäglicher Geschäfte im Rahmen eines E-Governments. Jede neue digitale Schnittstelle und Applikation bedingt aber eine umfassende

Piratenpartei Schweiz, 3000 Bern

Risikoanalyse und Folgeabschätzung.

Gerne nehmen wir wie folgt Stellung:

Allgemein:

Die Piratenpartei lehnt das BÜPF mit den dazugehörigen Verordnungen weiterhin in Gänze ab. Das Gesetz greift unverhältnismässig in das Recht auf Schutz der Privatsphäre ein und trägt zum chilling effect bei der Meinungs- und Informationsfreiheit bei. Es sollte in dieser Form nicht existieren.

Es zeigt sich ausserdem in dieser Vorlage erneut, was seit Beginn gesehen worden ist: Der Überwachungsstaat wird schleichend aber stetig nach mehr Kontrolle verlangen. So haben sich zuletzt die Überwachungen durch den Staat in nur einem Jahr verdoppelt.¹ Die vorliegende Revision der Verordnungen wird diesen Ausbau weiter beschleunigen und ist entsprechend abzulehnen.

Insbesondere und mindestens die automatisierte Abfrage der Daten bei den FDA und AAKD (Art. 18 Abs. 2 u. Abs. 4 VÜPF bzw. VE-VÜPF), die Vorratsdatenspeicherung (Art. 26 Abs. 5 BÜPF) sowie die Entfernung von Verschlüsselungen (Art. 26 Abs. 2 Bst. c BÜPF) sollten aus den schon in Kraft getretenen Texten vollständig gestrichen statt nun weiteren Personen aufgedrängt werden (vgl. unten Art. 16b i.V.m. Art. 16c VE-VÜPF).

Nach dem erläuternden Bericht zu den Teilrevisionen der VÜPF und VD-ÜPF sollen die Änderungen eine Revision des FMG umsetzen, welche dem Bundesrat eine feinere Unterteilung der Mitwirkungspflichtigen (MWP) ermöglichen soll. Ausserdem soll das VÜPF KMU-freundlicher werden, indem klarere Definitionen für die Einstufung der MWP gegeben werden.²

¹ Überwachungen durch den Staat haben sich verdoppelt - das sind die Gründe, <https://www.tagesanzeiger.ch/ueberwachungen-durch-den-staat-sind-in-einem-jahr-um-das-doppelte-gestiegen-das-sind-die-gruende-165465973955>.

² Erläuternder Bericht, S. 3f.

Es ist leider leicht zu erkennen, dass vielen Unternehmen das genaue Gegenteil widerfahren wird. Statt einer Vereinfachung oder Minderbelastung ist mit einer massenhaften Mehrbelastung zu rechnen. Ja, der Übergang für Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD) zwischen «ohne weitergehende Auskunftspflichten» und «weitergehenden Auskunftspflichten» (Art. 22 VÜPF) sowie AAKD mit oder ohne «weitergehenden Überwachungspflichten» (Art. 52 VÜPF) wird abgefertigt mit einer Zwischenstufe. Aber jene Zwischenstufe ist leicht erreicht – der Anbieter braucht lediglich 5000 «Teilnehmende» –, so dass am Ende mehr in der mittleren Kategorie landen werden, während sie nach den aktuellen Kriterien in der Kategorie ohne weitergehende Pflichten verbleiben würden. Für Unternehmen wird dies zu einem Mehraufwand und für die Bevölkerung zu mehr Überwachung durch die Hintertür führen.

Die Schweiz geniesst bisher, trotz einigen Läderungen (z.B. das BÜPF an sich), in den Bereichen Privatsphäre und Datenschutz ein positives Ansehen, weil sie jene als hohes Gut verteidigt. Dies nicht nur bei den eigenen Bürgerinnen und Bürgern sondern auch international. Das beschert den direkt involvierten Unternehmen bessere Umsätze und trägt auch zum guten Ruf der Schweiz als Ganzes bei. Dieses vertrauenswürdige Image würde mit der Annahme der VÜPF Vorlage schlüssig in Flammen gesetzt. So wird neu selbst der mittleren Kategorie der AAKD die Entschlüsselung nach Art. 50a VE-VÜPF auferlegt, was bisher den grossen Fernmeldedienstanbietern (FDA) und einigen wenigen riesigen AAKD vorbehalten war. Davon wären nicht nur VPN Anbieter betroffen, sondern u.a. auch Cloudspeicher-, E-Mail- oder Messenger-Anbieter.³ Art. 19 Abs. 1 VE-VÜPF verlangt neu auch die Nutzeridentifikation durch mehr Anbieter, was die Privatsphäre online zusätzlich aushebelt. Jegliches Vertrauen in schweizerische Dienste müsste also schlüssig eingestellt werden.

³

Erläuternder Bericht, S. 19f.

Piratenpartei Schweiz, 3000 Bern

Zu den einzelnen Artikeln:

Art. 16a-h

Grundsätzlich ist eine klarere Auflistung der betroffenen Dienste sowie die Kriterien zur Kategorisierung an einer Stelle zu begrüssen. Aber die neue Kategorie mit reduzierten Pflichten sollte gänzlich gestrichen werden.

Art. 16b

Anregung 1: Streichung von Art. 16 Abs. 1 Bst. b Ziff. 1

Anregung 2: Streichung der Änderung von Umsatz mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten zu Gesamtumsatz

Begründung:

Gemäss Art. 16b Abs. 1 Bst. b VE-VÜPF können sich FDA zu Diensten mit reduzierten Pflichten herunterstufen lassen, wenn sie (Ziff. 1) keine Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten hatten und (Ziff. 2) das gesamte Unternehmen in der Schweiz einen geringeren Jahresumsatz als 100 Millionen hat.

1

Das Kriterium in Ziffer 1 lehnen wir ab und die Chance zur Streichung im

Piratenpartei Schweiz, 3000 Bern

Rahmen der Revision sollte genutzt werden. Die Anfragen bzw. Überwachungsmassnahmen nehmen tendenziell zu⁴, was i.V.m. Ziffer 1 zu einer automatischen Zunahme von FDA mit vollen Überwachungspflichten führen wird. Dieses Kriterium belohnt geradezu den Ausbau des Überwachungsstaates mit vereinfachter und noch mehr Überwachung.

2

Die bisherige Regelung in Art. 51 VÜPF spricht aber noch von einem «Jahresumsatz in der Schweiz mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten von 100 Millionen». Neu soll also nicht mehr nur der Umsatz mit solchen Diensten sondern der gesamte Umsatz eines Unternehmens zur Hand genommen werden.

Im erläuternden Bericht wird dies mit einer Vereinfachung begründet, da es sich in der Praxis gezeigt habe, dass der gesamte Umsatz viel einfacher zu ermitteln und belegen sei (Bericht S. 16). Wer hätte es gedacht. Man möge es dem Dienst ÜPF bitte zumuten, diese Abgrenzung vorzunehmen oder alternativ die Herunterstufung zur FDA mit reduzierten Pflichten ungesehen zu akzeptieren - diese Variante würde es wesentlich mehr Personen erlauben, die propagierte «Vereinfachung» zu erleben. Denn damit wären nicht nur die Angestellten des Dienstes ÜPF sondern auch die Unternehmen entlastet. Was «Vereinfachung» angeht, ist die ungesehene Herabstufung auch klar der Vorlage überlegen, da die Entlastung der Angestellten beim Dienst ÜPF nochmals höher wäre.

Mit dieser neuen Definition erschwert man es ausserdem grösseren Unternehmen, in diesen Bereich zu investieren, wenn sie bisher nichts damit zu tun hatten. Sie würden sofort in die Kategorie mit vollen Pflichten fallen, was

⁴ Statistik zur Fernmeldeüberwachung: Mehr Überwachungsmassnahmen, <https://www.news.admin.ch/de/nsb?id=94661>; Überwachung im Internet: Wen dürfen die Behörden wann überwachen?, <https://blog.init7.net/de/ueberwachung-im-internet/>.

Piratenpartei Schweiz, 3000 Bern

den Einstieg erheblich unattraktiver macht. Selbes gilt auch für FDA, die die Schwelle von 100 Millionen noch nicht erreicht haben, aber gerne in andere Bereiche investieren würden.

Nicht zuletzt ist es schlicht nicht akzeptabel, dass eine kompliziertere Abgrenzung dazu benutzt wird, weitere Unternehmen in die Definition der FDA mit vollen Pflichten hereinzu ziehen und damit die ständige (automatisierte) Überwachung der Bevölkerung auszubauen.

Art. 16c

Anregung: Streichung von Abs. 3 Bst. a. (sowie Art. 18 Abs. 2, Abs. 3 Bst. c, Abs. 4 1. Satz und Art. 18a Abs. 3 letzter Teilsatz (VE-)VÜPF)

Begründung:

In Art. 16c Abs. 3 Bst. a wird von FDA mit vollen Pflichten verlangt, dass sie verschiedene Auskünfte nach Art. 18 Abs. 2 automatisiert liefern müssen. Art. 17 Abs. 3 Bst. c ermöglicht das gleiche freiwillig für Anbieterinnen mit reduzierten Pflichten. Jegliche Automatisierung sollte vollständig aus der Vorlage gestrichen werden. Die Automatisierung trivialisiert ein Verfahren, das bewusst mühsam sein muss. Es geht hier um schwere Eingriffe in die Grundrechte der betroffenen Personen. Solche Eingriffe sollen sowohl finanziell als auch Aufwand-mässig zu spüren sein, damit sie auch in dieser Hinsicht ein seltenes Mittel bleiben, statt eine Zunahme zu verzeichnen (vgl. Fussnote 1). Ausserdem schadet es mitnichten, wenn die Anfragen durch eine weitere Person genau kontrolliert werden können.

In Kombination mit der Änderung in Art. 16b Abs. 1 Bst. b Ziff. 2 fallen ausserdem noch mehr Anbieter unter die Automatisierung, was das Problem zusätzlich verschärft.

Piratenpartei Schweiz, 3000 Bern

Art. 16d

Anregung: Einschränkung der AAKD Definition

Begründung:

Gemäss Art. 16d Abs. 1 gilt als AAKD «wer für Dritte einen Einweg- oder Mehrwegkommunikationsdienst oder einen indirekten Zugangsdienst zu einem öffentlichen Fernmeldenetz erbringt, der unabhängig vom Netzzugangsdienst funktioniert.»

Man möchte es nicht meinen, aber, wie im allgemeinen Teil erwähnt, zählen laut erläuterndem Bericht auch «Onlinespeicherdiene, wie Cloud Storage, File Hosting, Share Host, Online Storage, File Sharing» dazu.⁵ Dies, weil man teilweise gemeinsam Dateien bearbeiten könne. Plötzlich fällt unter AAKD also auch etwas, das mit Kommunikation nichts zu tun hat - die private Ablage von Dateien. Damit fallen u.U. iCloud und Google Drive plötzlich darunter. Diese Interpretation von AAKD ist ausufernd und sollte so nicht umgesetzt werden.

Unternehmen wie Proton verlangen zu recht auch die Exklusion von VPNs, deren Sinn gerade darin besteht, ihre Nutzer zu anonymisieren - ein legitimer Anwendungszweck. Diese der Entschlüsselung (Art. 50a VE-VÜPF) und der Vorratsdatenspeicherung (Art. 16g Abs. 3 Bst. a Ziff. 2 VE-VÜPF) zu unterstellen, wäre der Todesstoss für diese Unternehmen in der Schweiz.⁶

Art. 16e

⁵ Erläuternder Bericht, S. 19f.

⁶ Proton-Chef: «Diese Entscheidung ist wirtschaftlicher Selbstmord für die Schweiz», <https://www.watson.ch/digital/wirtschaft/517198902-proton-schweiz-chef-andy-yen-zum-ausbau-der-staatlichen-ueberwachung>.

Piratenpartei Schweiz, 3000 Bern

Anregung 1: Änderung zu AAKD ohne Pflichten

Anregung 2: Ausnahme für nicht-kommerzielle Anbieter, Bildung und Forschung

Begründung:

1

Es fehlt leider eine Kategorie für AAKD (und FDA), die keine Pflichten haben. Eine solche wäre zu begrüßen. Überwachung ist kein Muss.

2

Art. 16e definiert die Kategorie "AAKD mit minimalen Pflichten" mit der Nicht-Erfüllung der Kriterien der anderen Kategorien. Es wäre sinnvoll nicht-kommerzielle Anbieter ebenfalls grundsätzlich in diese Kategorie aufzunehmen. Es gibt in Art. 16b bereits die Herabstufung für FDA, wenn sie ihren Dienst nur im Bereich Bildung und Forschung anbieten. Eine gleiche Ausnahme sollte auch hier geschaffen werden. Im Bereich der AAKD gibt es aber zusätzlich viele Projekte, die nicht-kommerziell sind. Eine plötzliche Überwachungspflicht nach Art. 16f würde diese einer ungebührlichen Mehrbelastung aussetzen und sie in ihrer Existenz bedrohen (siehe Begründung Art. 16f).

Diese Anbieter können auch wichtige Dienste für demokratische Bewegungen weltweit stellen. Tor-Anbieter⁷, also Anbieter, die z.B. für Dissidenten in autokratischen Ländern wichtige Zugänge ins freie Internet bereitstellen, könnten plötzlich die Teilnehmer identifizieren und die Verschlüsselung aufheben müssen.

Nicht-kommerzielle Anbieter sollten entsprechend in der Kategorie mit minimalen Pflichten verbleiben können.

⁷ [https://de.wikipedia.org/wiki/Tor_\(Netzwerk\)](https://de.wikipedia.org/wiki/Tor_(Netzwerk)).

Piratenpartei Schweiz, 3000 Bern

Art. 16f

Anregung: Streichung

Begründung:

Mit Art. 16f wird die neue mittlere Stufe «AAKD mit reduzierten Pflichten» eingeführt.

Laut Bericht wird «auf diese Weise [...] eine ausgewogenere und dem Grundsatz der

Verhältnismässigkeit besser entsprechende Abstufung der Verpflichtungen der verschiedenen Unterkategorien der AAKD erreicht.»⁸

Was harmlos klingt, unterstellt in Wirklichkeit die AAKD schon ab 5000 Teilnehmenden z.B. der Pflicht, Verschlüsselungen zu entfernen nach Art. 50a VE-VÜPF. Die Zahl ist klein genug, dass selbst Projekte wie «Freifunk»⁹ (gemeinschaftliche WLAN-Zugänge), Tor-Anbieter oder andere gemeinnützige Vereine darunter fallen.

Die Unternehmen und Vereine, die in diese Kategorie fallen, haben von der «ausgewogeneren» Abstufung entsprechend nichts ausser Mehrkosten und Pflichten. Darauf können nicht nur sie gut verzichten.

Die Kategorie «mit reduzierten Pflichten» wird ausserdem in Art. 19 Abs. 1 VE-VÜPF auch der Identifikationspflicht der Nutzer unterstellt, was bisher nicht der Fall war. Das bedeutet u.U. eine starke Steigerung der anfallenden Daten, was dem Grundsatz der Datensparsamkeit direkt zuwiderläuft und angesichts der Grösse kaum verhältnismässig ist (Art. 6 Abs. 2 DSG).

Die mittlere Kategorie dient letztlich lediglich dem Ausbau der Überwachung und der weiteren Einschränkung der Grundrechte der Schweizer Bevölkerung

⁸ Erläuternder Bericht, S. 4.

⁹ <https://freifunk.net/>.

Piratenpartei Schweiz, 3000 Bern

und sollte somit gestrichen werden.

Weniger aber dennoch relevant, erhöht die mittlere Stufe «reduzierte Pflichten» auch für kleinere Unternehmen (und Vereine/Einzelpersonen) die Kosten, Anbieter eines abgeleiteten Dienstes zu werden. Das hat eine abschreckende Wirkung auf die Entwicklung in der Schweiz.

Zuletzt wird im BÜPF explizit von AAKD, "die Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten" (Art. 22 Abs. 4 u. Art. 27 Abs. 3 BÜPF), gesprochen, welche weiteren Pflichten unterstellt werden können. Das kann mit der Anforderung von lediglich 5000 Teilnehmenden nur leidlich als erfüllt angesehen werden.

Eventualiter sollte mindestens die Einstufung an massiv höhere Anforderungen als 5000 Teilnehmende geknüpft werden. 5000 ist eine auffällig kleine Zahl, wenn die nächste Stufe bei 1 Million angesetzt wird.

Art. 16g

Anregung 1: Streichung als Kriterium oder Erhöhung der Teilnehmendenzahl

Anregung 2: Streichung der Änderung von 100 Millionen Umsatz, «wobei grosser Teil ihrer Geschäftstätigkeit im Anbieten abgeleiteter Kommunikationsdienste besteht» zu Gesamtumsatz

Anregung 3: Streichung der Vorratsdatenspeicherung

Anregung 4: Streichung der Automatisierung

Begründung:

Piratenpartei Schweiz, 3000 Bern

1

Zunächst begrüssen wir die Änderung, dass neu die Einstufung «mit vollen Pflichten» bei den AAKD nicht mehr auf die Anzahl der Überwachungsaufträge bzw. Auskunftsgesuche (Art. 22 Abs. 1 Bst. a bzw. Art. 52 Abs. 1 Bst. a VÜPF) abgestellt wird. Siehe Begründung Art. 16b.

Aber die neue Anforderung von 1 Million Nutzer darf gerne massiv erhöht werden. Der Erfolg eines Anbieters bzw. eines Angebots, viele Personen anzusprechen, sollte nicht allein als Begründung reichen, mehr Teilnehmende der automatisierten und erweiterten Überwachung auszusetzen.

2

Analog Begründung Art. 16b 2: Der Dienst ÜPF soll sich diese Arbeit gerne machen oder ganz bleiben lassen und nicht hochstufen, statt die Anzahl AAKD mit vollen Pflichten mit fragwürdiger Begründung zu erhöhen.

Eventualiter sollte der erforderliche (Gesamt-)Umsatz massiv erhöht werden.

3

Gemäss Art. 16g Abs. 3 Bst. a Ziff. 2 sollen die AAKD mit vollen Pflichten neu ebenfalls zur Vorratsdatenspeicherung verpflichtet werden, wie es die FDA bereits sind. Es sollen also Daten wie die IP und andere Randdaten für 6 Monate aufbewahrt werden müssen. Die Vorratsdatenspeicherung im Falle der FDA ist bereits äusserst bedenklich, diese aber auf AAKD auszuweiten geht weit über das Mass anderer Staaten hinaus. Die anhaltslose Massenüberwachung und Speicherung der Daten aller ist ein extremer Eingriff in die garantierten Rechte und wurde entsprechend auch schon vom EuGH abgewiesen.¹⁰ Für die Schweiz hat dies natürlich keinen direkten Einfluss, aber

¹⁰ Vgl. z.B. EuGH Pressemitteilung Nr. 58/22; NLMR 5/2018-EGMR.

Piratenpartei Schweiz, 3000 Bern

es darf festgehalten werden, dass unsere Menschenrechte in unseren Nachbarländern bereits als verletzt gelten würden.

Die Aufbewahrung von Randdaten auf AAKD auszuweiten, ist allerdings eine Eskalationsstufe die schlicht nicht mehr akzeptabel ist. Es wäre praktisch nicht mehr möglich, online sein Recht auf Privatsphäre wahrzunehmen, ohne auf ausländische Dienste zurückzugreifen. Die Rechte der eigenen Bürgerinnen und Bürger nur noch durch Dienste im Ausland gewährleisten zu können, kann nicht Ziel dieser Revision sein.

Ironischerweise könnte dies auch dazu führen, dass die Überwachungspflichten nutzloser werden, weil die zu Überwachenden alle schweizerischen AAKD meiden werden.

Wirtschaftlich betrachtet, wird das von Proton-Chef Andy Yen vollkommen zurecht als «Selbstmord für die Schweiz» bezeichnet.¹¹ Wird dieser Vorschlag umgesetzt, wird die Schweiz das letzte Land sein, in dem eine AAKD ihren Sitz haben wollen wird. Der Nachteil ist zu gross für Unternehmen, die darauf angewiesen sind, dass ihre Kunden ihnen vertrauen können, ihre Rechte ernstzunehmen – fast jedes andere Land wäre fortan besser dafür geeignet. Von den zusätzlichen Kosten gar nicht zu sprechen.

Nicht zuletzt muss für die Vorratsdatenspeicherung auch ein System her, welches diese Funktion sicherstellt. Die Speicherung setzt die Daten jedoch nicht nur den Behörden aus, sondern erhöht auch das Risiko, dass andere Zugriff erlangen können. Damit schafft man bei den betroffenen Anbieterinnen unnötig Angriffspunkte, die statt zur Bekämpfung zur Förderung von Delikten u.ä. beitragen können.

Ein weiterer Blick ist auch die Frage des Zusammenspiels zwischen

¹¹ Proton-Chef: «Diese Entscheidung ist wirtschaftlicher Selbstmord für die Schweiz», <https://www.watson.ch/digital/wirtschaft/517198902-proton-schweiz-chef-andy-yen-zum-ausbau-der-staatlichen-ueberwachung>.

Piratenpartei Schweiz, 3000 Bern

Vorratsdatenspeicherung und legitimer Geheimnisbewahrung wert. Arzt- und Anwaltsgeheimnis sowie Quellschutz und Whistleblower sind alle gleichsam von der ausgeweiteten massenhaften Überwachung betroffen. Es ist wohlbekannt, dass der Inhalt häufig gar nicht so wichtig ist, weswegen die Randdaten genügen, um relevante Einsichten bekommen zu können. Mit der Vorratsdatenspeicherung setzt man diese Daten zusätzlichem Risiko aus.

4

Siehe Begründung Art. 16c.

Art. 16h

Anregung: Änderung der Voraussetzung bzgl. professionellem Betrieb

Begründung:

Nach Art. 16h Abs. 2 VE-VÜPF soll ein öffentlicher WLAN-Zugang als professionell betrieben gelten, «wenn kumuliert maximal mehr als 1000 Endbenutzerinnen und -benutzer alle von der gleichen Person gemäss Absatz 1 zur Verfügung gestellten öffentlichen WLAN-Zugänge nutzen können.» Im Bericht steht dazu, dass die Kapazität für tausend Zugänge schon genüge und nicht auch tatsächlich tausend Nutzer (gleichzeitig) vorhanden sein müssen.¹² Wenn also jemand schon nur 1-2 «Prosumer» Produkte - beispielsweise bietet Ubiquiti APs an, die 500+ Connections versprechen - öffentlich zugänglich macht, gilt das WLAN dieser Person als professionell betrieben. Der Bericht geht davon aus, dass dies der Verhältnismässigkeit genüge tue, was definitiv bezweifelt werden muss.

Ebenfalls davon betroffen wären z.B. Konferenzen. Wenn normale Konsumenten-Hardware schon die Voraussetzungen erfüllen kann, gilt dies umso mehr für die Hardware, die für Konferenzen bereitgestellt wird.

¹² Erläuternder Bericht, S. 26.

Piratenpartei Schweiz, 3000 Bern

Die FDA, die die Zugänge sowohl hinter den Privatpersonen als auch hinter Konferenzen stellt, müsste dann bei einer solchen Konstellation gemäss Art. 19 Abs. 2 VÜPF alle Nutzer des WLANs identifizieren können. Wie sie dies anstellen soll, ist gänzlich unklar, wird aber verlangt – absurd. Angesichts dessen wäre es sinnvoll, wesentlich höhere Hürden anzusetzen oder den Absatz gleich zu streichen.

Alternativ könnte die Identifikationspflicht davon abhängig gemacht werden, ob die Nutzer separat für das WLAN bezahlen müssen oder nicht.

Art. 18

Anregung: Streichung der Automatisierung

Begründung: Siehe Begründung Art. 16c

Art. 18a

Anregung: Streichung der Automatisierung

Begründung: Siehe Begründung Art. 16c

Art. 19

Anregung 1: Streichung der Identifikationspflicht durch die AAKD

Anregung 2: Streichung der Endbenutzeridentifikation bei professionell betriebenen öffentlichen WLAN-Zugängen

Begründung:

1

Gemäss Art. 19 Abs. 1 VE-VÜPF sollen neu auch die AAKD mit reduzierten

Piratenpartei Schweiz, 3000 Bern

Pflichten ihre Nutzer mit geeigneten Mitteln identifizieren. Wie bei Art. 16f bereits erwähnt, läuft dieses Vorhaben direkt wichtigen Prinzipien wie der Datensparsamkeit entgegen. Durch die Erweiterung um AAKD mit reduzierten Pflichten, bzw. der Inklusion von AAKD überhaupt, wird es der eigenen Bevölkerung praktisch unmöglich sein, schweizerische Unternehmen zu nutzen, wenn sie auf ihre Daten und ihr Recht auf Privatsphäre acht geben wollen. Personen von ausserhalb werden selbstverständlich schweizerische Anbieter sowieso meiden. Beide Umstände sollten nicht wünschenswerte Auswirkungen einer Verordnungsrevision sein.

Wie Alexis Roussel, COO von NymVPN, ausserdem zu bedenken gibt, bedeuten mehr verfügbare Daten und weniger Anonymität online auch automatisch mehr Daten, die ausgenutzt werden können:

«For example, enforcing identification of all these small services will eventually push to leaks, more data theft, and more attacks on people.»¹³ Was man sich hier vielleicht an besserer Überwachungsmöglichkeit und damit (vermeintlich) besserer Bekämpfung von Verbrechen etc. erhofft, könnte in Wirklichkeit zu mehr erfolgreichen Delikten dank mehr stehlbaren Daten führen - Hacker, Personen mit kriminellen Absichten (z.B. Erpresser) oder gar vereinzelte Mitarbeiter könnten sich den neuen Daten ermächtigen und diese ausnutzen.

2

Wie schon bei Art. 16h beschrieben, ist es äusserst leicht, als Person mit professionell betriebenem öffentlichem WLAN-Zugang eingestuft zu werden. Art. 19 Abs. 2 VE-VÜPF verlangt nun die Nutzeridentifikation durch die FDA. Es ist absolut korrekt, dass der Betreiber selbst nicht identifizieren muss, aber dies den FDA aufzubürden ist keine Lösung. Um die Kontrolle sicherzustellen, müssten diese entweder einen enormen Aufwand betreiben oder starke

¹³ Secure encryption and online anonymity are now at risk in Switzerland – here's what you need to know, <https://www.techradar.com/vpn/vpn-privacy-security/secure-encryption-and-online-anonymity-are-now-at-risk-in-switzerland-heres-what-you-need-to-know>.

Piratenpartei Schweiz, 3000 Bern

Einschränkungen bei ihren Kunden vornehmen. Beides ist unverhältnismässig angesichts der sehr tiefen Hürde, als professionell zu gelten.

Art. 21

Anregung 1: Streichung AAKD in Abs. 1 Bst. a.

Anregung 2: Streichung der Vorratsdatenspeicherung, besonders für AAKD in Abs. 6

Begründung:

1

Siehe Begründung Art. 19, Anregung 1

2

Siehe Begründung Art. 16g, Anregung 3

Art. 42a, Art. 43a

Anregung: Streichung

Begründung:

Die verschiedenen Auskunfts- und Überwachungstypen sind leider reichlich unübersichtlich. Aber, sofern richtig interpretiert, gibt es bei AAKD bisher, ausser im Rahmen als Netzzugangsdienst i.S.v. Art. 35 VÜPF, keine «Information Requests» (IR-Abfragen), also die Stufe mit den niedrigsten Anforderungen, die die Herausgabe des «verwendeten Protokolls sowie IP-Adresse und Portnummer» (Art. 42a Abs. 1 Bst. c und Art. 43a Abs. 1 Bst. c) verlangen. Jetzt hingegen sollen plötzlich auch andere AAKD (ohne Netzzugangsdienst), wie Messenger oder E-Mail-Dienste die IPs, Protokolle und Ports mit einer IR-Abfrage (automatisch) herausgeben. Dies war bisher sonst scheinbar nur als Teil der «Historical Data» (HD) Abfragen und der «Real Time»

Piratenpartei Schweiz, 3000 Bern

(RT) Überwachung der Fall, welche höheren Anforderungen zur Ausführung unterliegen.

Da auch die AAKD mit reduzierten Pflichten darunterfallen, wird die Abfrage auch noch massiv ausgeweitet, was schlicht insgesamt unverhältnismässig und damit abzulehnen ist.

Die Schaffung dieser neuen Auskunftstypen schafft für die AAKD ausserdem einen unnötigen Mehraufwand. Mit der für viele AAKD bevorstehenden Einstufung zu AAKD mit reduzierten Pflichten (oder gar vollen Pflichten) wird die Belastung weiter erhöht.

Art. 50a

Anregung: Streichung (auch im BÜPF)

Begründung:

Nach Art. 50a VE-VÜPF soll die Entfernung von Verschlüsselungen nach Art. 26 Abs. 2 Bst. c BÜPF konkretisiert werden. Die Regelung schliesst die Ende-zu-Ende-Verschlüsselung von der Entfernung aus, da dies zu schwerer Kritik geführt hatte und Befürchtungen wie Chatkontrolle hochkommen liess.¹⁴ Das ist sicherlich eine begrüssenswerte Konkretisierung. Aber umgekehrt legt der Artikel immer noch fest, dass alle Anbieterinnen mit reduzierten und vollen Pflichten alle anderen von ihnen oder für sie angebrachten Verschlüsselungen entfernen müssen, um die unverschlüsselte Daten liefern zu können. «Wenn [...] ein Schlüssel der Anbieterin bei der Verschlüsselung verwendet wird, das heisst wenn die Anbieterin in der Lage ist, verschlüsselten Fernmeldeverkehr der überwachten Person zu entschlüsseln, dann muss sie dies auch tun.»¹⁵

Das bedeutet, dass jegliche Verschlüsselung, die eine Person nicht selbst

¹⁴ Oberster Schweizer Datenschützer spricht sich gegen Aufweichung der Verschlüsselung aus, <https://www.watson.ch/digital/schweiz/528820964-schweizer-datenschuetzer-ist-gegen-aufweichung-der-verschluesselung>.

¹⁵ Erläuternder Bericht, S. 43.

Piratenpartei Schweiz, 3000 Bern

angebracht hat (ausser z.B. E2EE in Messengern) muss auch entfernt werden.

Es ist unklar, ob davon selbst Dienste wie iCloud betroffen sein werden, aber Cloudspeicher-Anbieter gehören zu den AAKD, womit sie grundsätzlich dazu zählen. Und jede AAKD, die bisher im Auftrag eines Nutzers, Daten verschlüsselt hat, muss denselben Schlüssel nun benutzen, um die Daten herauszugeben. Theoretisch könnte dies selbst die Ausnahme der Ende-zu-Ende-Verschlüsselung umgehen, da die Verschlüsselung quasi vom Anbieter angebracht wird.

Das alles gilt, wie gesagt, schon ab 5000 Teilnehmenden. Die Zahl der Dienste, die von der Entschlüsselung betroffen sind, springt also zusätzlich massiv an.

Damit die Verschlüsselung jederzeit aufgehoben werden kann, muss zudem wiederum ein System her, welches diese Funktion sicherstellt. Diese Vereinfachung der Entschlüsselung setzt die Daten dahinter jedoch nicht nur den Behörden aus, sondern erhöht auch das Risiko, dass andere Zugriff erlangen können. Wie schon bei der Nutzeridentifikation schafft man damit unnötig Angriffspunkte, die statt zur Bekämpfung zur Förderung von Delikten u.ä. beitragen können. Zusätzlich könnte auch hier die Sicherheit des Arzt- und Anwaltsgeheimnisses sowie der Schutz von Quellen und Whistleblowern in Gefahr sein, insbesondere da eben auch kleine Anbieter in die Pflicht genommen werden.

Der Schaden für Wirtschaft, Image, Sicherheit und Privatsphäre ist schlicht unverhältnismässig im Vergleich zum fraglichen Nutzen.

Art. 60a

Anregung: Streichung

Piratenpartei Schweiz, 3000 Bern

Begründung:

Gemäss Art. 60a Abs. 1 soll eine rückwirkende Überwachung (HD-Abfrage) zum Zweck der Teilnehmeridentifikation stattfinden und dafür a. «alle Angaben über die mutmassliche Urheberschaft oder Herkunft einer Internetverbindung» und b. «die Schnittmenge aus allen Angaben über die mutmassliche Herkunft von zwei oder mehreren Internetverbindungen im Falle von zu vielen Ergebnissen (Art. 38a Abs. 4)» übermittelt werden.

Im erwähnten Art. 38a VE-VÜPF wird kein Ergebnis geliefert, wenn mehr als ein einziger Treffer vorliegt, weil dies Daten unbeteiligter Dritter liefern würde. Hier soll dies nun akzeptabel sein, weil die rückwirkende Überwachung (zu recht) höheren Anforderungen unterliege.¹⁶ Die Kombination aus der extrem fragwürdigen Praxis der Vorratsdatenspeicherung und der Lieferung von «falsch-positiven Ergebnissen» scheint allerdings generell unverhältnismässig.

Auf die Massenüberwachung aufbauend werden damit plötzlich Daten zu unbescholtene Usern ausgelesen - eine klare Verletzung der Privatsphäre, die kaum mit dem Nutzen abgewogen werden kann. Da es sich eben genau um Mehrfachtreffer handelt, die keine eindeutige Zuteilung erlauben, ist der Nutzen der Auskunft gering, die Gefahr für Fehler in der Folge eher hoch.

% Schlussbemerkungen

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht unsererseits auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Regelungen, ist damit keine Zustimmung durch die Piraten zu solchen Regelungen verbunden.

¹⁶ Erläuternder Bericht, S. 45.



piratenpartei

www.piratenpartei.ch

Piratenpartei Schweiz, 3000 Bern

Kontaktdetails für Rückfragen finden Sie in der Begleit-E-Mail.

Piratenpartei Schweiz, Arbeitsgruppe Vernehmlassungen, 05. Mai 2025

Swiss Industry Calls for Strong Commitment to Defend Swiss Competitiveness in Trust and Security

(Official German and French translation below)

6 May 2025

Dear Federal Councilor Jans,

We, the undersigned, are writing to you to raise significant concerns about the proposed draft of the second revision of the Ordinance on the Surveillance of Correspondence by Post and Telecommunication (SPTO), currently under consultation by the Federal council. As representatives of Switzerland's technology sector, legal community, academic community and investment community, we firmly believe that the proposals represent an existential threat to Switzerland's reputation internationally and future economic prosperity, and as such, we oppose in principle the partial revisions of the SPTO and OME-PTSS.

We are speaking out today because we believe passing the current proposal will sabotage Switzerland's future growth prospects. While the signatories of this letter come from vastly different industries, we are unified in sharing concerns around three areas.

1. We are concerned that the proposal to massively expand state surveillance with reduced judicial oversight threatens the basic rights of Swiss citizens for communication-privacy as well as our customers internationally.
2. The proposal is so broadly written that it can put in scope practically all Swiss tech businesses and risk undermining the competitiveness of the Swiss technology sector at a time when there is an unprecedented opportunity for growth in this sector in Europe.
3. We believe some of the proposals, like mandatory metadata retention applied broadly, put Switzerland so far behind European and American norms and closer to Russian or Chinese norms that they risk permanently damaging Switzerland's reputation of trust, security, and privacy, to the detriment of a wide range of present and future industries.

Undermining the privacy and security of Swiss citizens

Switzerland's existing surveillance framework and corresponding obligations represents a balanced approach that makes the country superior to the European Union and the US, and therefore globally competitive. The proposed revision unfortunately destroys this balance by dramatically expanding surveillance while removing judicial oversight at the same time.

Under this proposal, Swiss service providers can be obliged to automatically share data with no possibility to check the correctness of the data requests to ensure there is no abuse of the system. It also increases massively the amount of data that is required to be retained, and expands the scope of companies that can be eligible for these obligations. These mandatory metadata retention obligations are considered to be so onerous and contrary to the principle of basic privacy rights that they have been repeatedly deemed illegal in the European Union. In pursuing these proposals, Switzerland is seeing to introduce a form of surveillance that none of our democratic peer nations have today.

Forcing Swiss companies to retain sensitive data which European and American companies are not obliged to do, will also make Swiss companies more attractive targets for cyberattacks, attracting both cybercriminals, and state backed adversaries from countries like Russia, China, and North Korea to carry out attacks against Swiss businesses and infrastructure. Furthermore, mandating automated "backdoor" access for Swiss government

services to automatically access data held by Swiss tech companies, will also make the Swiss government an even higher profile target. In fact, the ISC-FDJP, the federal department that would be responsible for maintaining this backdoor, was subject to a data breach in 2023. If passed, this proposal would make the inevitable future breach much worse, by giving attackers backdoor access to a wide range of Swiss tech companies, exponentially magnifying the threat to Swiss citizens.

Hurting the competitiveness of the Swiss technology sector

Technology has been the largest driver of economic growth globally for the past three decades, but by adopting these proposals, the Federal Council will in practice ensure that this opportunity is lost to Switzerland. At a time when consumers and businesses all over the world are looking for technology products that offer greater security and geopolitical events are driving increased demand for European technology, Switzerland has an opportunity to build a vibrant and successful native technology industry. Indeed, there are signatories to this letter that in the past 10 years, have amassed hundreds of millions of customers from around the world, showing that Switzerland can successfully capitalize on this opportunity.

However, the proposed second SPTO revision draft threatens to undermine the competitiveness of these companies and the country as a whole. The proposals would create a legal framework that is not just worse than the European Union, but it would impose obligations that even the US does not have. Numerous Swiss companies have already stated that they would not be able to compete and offer credible services based on trust and security if they are forced to engage in surveillance on behalf of the state that goes even beyond what is required by American law. This would result in already established and successful companies leaving Switzerland. It would also discourage future founders from establishing technology businesses in Switzerland - especially when these founders realise they could be obligated to comply once they reach a mere threshold of 5'000 users - preventing future economic growth, employment and tax revenue in Switzerland. Even the higher proposed threshold of 1 million users is insignificant when considering tech companies that export successfully, which is a necessity given the limited size of Switzerland's domestic market. No such thresholds exist in the US and Europe, and tech startups are not subjected to mandatory data retention, meaning there are no artificial barriers to growth. By setting these thresholds, this proposal seeks to punish Swiss companies for their international success, and artificially caps the long term potential of our tech ecosystem.

By subjecting tech startups and scale-ups to the possibility of having the same obligations as large telecommunication companies with billions of revenue just from the Swiss market, the proposed revision would subject these companies to compliance costs that could run into the tens of millions of Swiss Francs, creating an unacceptable financial burden on scale ups with limited resources. For companies in the early stages of their growth and with limited financial reserves, the prospect of diverting cash and engineering capacity to these surveillance measures rather than innovating and competing is fatal. The tech industry is the most competitive industry in the world. Businesses will choose a legal jurisdiction that makes it as easy as possible to compete, and these proposals would ensure that Switzerland is not even considered.

Permanent reputational damage to Switzerland

Switzerland has built a global reputation for stability, privacy and security over a century. This has greatly benefited many sectors of the Swiss economy over the past century, and continues to be one of Switzerland's strongest competitive advantages. For over one

hundred years, this has been backed up by a legal framework that was superior to the US and the EU. By giving up this advantage and going further in the other direction than any other European democracy, this revision is an unfortunate act of self-sabotage.

A reputation that is built up over many years can be destroyed in an instant, requiring only the departure of a few key companies to permanently damage Switzerland's reputation globally. Even if it is deemed unnecessary to be better than the US and the EU, we must at the very least be equivalent, and never worse.

The proposed revision to the SPTO should be abandoned

In light of the concerns expressed above, we believe that the proposed revision of the SPTO should be abandoned and that there is an overriding public interest in preserving the current status quo.

Yours sincerely,

Schweizer Unternehmen fordern ein klares Bekenntnis zur Verteidigung der Schweizer Wettbewerbsfähigkeit in Sachen Vertrauen und Sicherheit

6. Mai 2025

Sehr geehrter Herr Bundesrat Jans,

Wir, die Unterzeichnenden, wenden uns an Sie, um ernsthafte Bedenken gegen den vorgeschlagenen Entwurf der zweiten Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) zu erheben, der sich derzeit in der Vernehmlassung des Bundesrates befindet. Als Vertreter der Schweizer Technologiebranche, der Rechtswissenschaft, der akademischen Gemeinschaft und von Investorenkreisen sind wir der festen Überzeugung, dass die Vorschläge eine existentielle Bedrohung für den internationalen Ruf der Schweiz und für den künftigen wirtschaftlichen Erfolg darstellen, weshalb wir die Teilrevisionen des VÜPF und VD-ÜPF grundsätzlich ablehnen.

Wir sind der Meinung, dass die Verabschiedung des aktuellen Vorschlags künftige Wachstumschancen der Schweiz gefährden wird. Obwohl die Unterzeichner dieses Briefes aus sehr unterschiedlichen Branchen kommen, teilen wir unsere Bedenken in folgenden drei Bereichen:

1. Dieser Vorschlag, der eine massive Ausweitung der staatlichen Überwachung mit eingeschränkter gerichtlicher Kontrolle vorsieht, verletzt das Grundrecht auf Privatsphäreschutz in der Kommunikation, welches den Schweizer Bürgerinnen und Bürger sowie unseren internationalen Kunden zusteht.
2. Der Vorschlag ist so weit gefasst, dass er praktisch alle Schweizer Technologieunternehmen betreffen kann und die Wettbewerbsfähigkeit des Schweizer Technologiesektors zu einem Zeitpunkt untergraben könnte, an dem sich in Europa einmalige Wachstumschancen bieten.
3. Wir sind der Meinung, dass einige der Vorschläge, wie z.B. die obligatorische Vorratsdatenspeicherung, die Schweiz so weit hinter die europäischen und amerikanischen Standards zurückfallen lassen und sich russischen oder chinesischen Standards annähern, dass sie den Ruf der Schweiz in Bezug auf Vertrauen, Sicherheit und Schutz der Privatsphäre dauerhaft schädigen könnten, und zwar zum Nachteil zahlreicher gegenwärtiger und künftiger Branchen.

Die Privatsphäre und Sicherheit der Schweizer Bevölkerung werden untergraben

Der bestehende Überwachungsrahmen in der Schweiz und die damit verbundenen Verpflichtungen stellen einen ausgewogenen Ansatz dar, der dem Land gegenüber der Europäischen Union und den USA einen Vorteil verleiht und es dadurch international wettbewerbsfähig macht. Die vorgeschlagene Revision zerstört diese Balance, indem sie die Überwachung drastisch ausweitet und gleichzeitig die gerichtliche Kontrolle abschafft.

Der Vorschlag sieht vor, dass Schweizer Dienstleistungserbringer verpflichtet werden können, automatisch Daten weiterzugeben – ohne die Möglichkeit, die Richtigkeit der Datenanfragen zu überprüfen und so sicherzustellen, dass das System nicht missbraucht wird. Zudem wird die Menge der Daten, die gespeichert werden müssen, massiv erhöht, und der Kreis der Unternehmen erweitert, die für diese Verpflichtungen in Frage kommen. Diese obligatorische Vorratsdatenspeicherung gilt als so schwerwiegender und unvereinbar mit dem Grundsatz der grundlegenden Rechte auf Privatsphäre, dass sie in der Europäischen Union wiederholt als rechtswidrig eingestuft worden ist. Mit dem Vorschlag will die Schweiz eine Form der Überwachung einführen, wie sie heute kein anderes demokratisches Land kennt.

Wenn Schweizer Unternehmen gezwungen werden, sensible Daten aufzubewahren (wozu europäische und amerikanische Unternehmen nicht verpflichtet sind), werden sie zu attraktiveren Zielen für Cyberangriffe, was sowohl Cyberkriminelle als auch staatlich unterstützte Akteure aus Ländern wie Russland, China und Nordkorea anzieht, Angriffe auf Schweizer Unternehmen und Infrastrukturen auszuüben. Die Einführung einer «Hintertür» für Schweizer Regierungsdienste, die den automatisierten Zugriff auf die Daten von Schweizer Technologieunternehmen erlaubt, macht auch die Schweizer Regierung zu einem noch interessanteren Ziel. Das Bundesdepartement ISC-EJPD, welches zusammen mit dem Eidgenössischen Justiz- und Polizeidepartement für diese Hintertür zuständig wäre, war im Jahr 2023 von einem Datenleck betroffen. Sollte der Vorschlag angenommen werden, würde damit eine unvermeidliche Datenpanne noch verschlimmert, da Angreifer durch die Hintertür Zugang zu einer Vielzahl von Schweizer Technologieunternehmen erhalten, was die Bedrohung für Schweizer Bürgerinnen und Bürger drastisch vergrössert.

Die Wettbewerbsfähigkeit des Schweizer Technologiesektors ist gefährdet

In den letzten drei Jahrzehnten war die technologische Entwicklung weltweit die wichtigste Triebkraft des Wirtschaftswachstums. Mit der Annahme des Vorschlags wird der Bundesrat jedoch dafür sorgen, dass diese Chance für die Schweiz verloren geht. Angesichts der Tatsache, dass Verbraucher und Unternehmen auf der ganzen Welt nach Technologieprodukten verlangen, die mehr Sicherheit bieten, und dass geopolitische Ereignisse die Nachfrage nach europäischen Lösungen ankurbeln, bietet sich für die Schweiz die Chance, eine starke und erfolgreiche lokale Technologiebranche aufzubauen. Die Unterzeichner dieses Schreibens haben in den letzten zehn Jahren Hunderte von Millionen von Kunden aus der ganzen Welt gewonnen, was zeigt, dass die Schweiz diese Chance erfolgreich nutzen kann.

Der vorgeschlagene Entwurf der zweiten VÜPF-Revision droht jedoch die Wettbewerbsfähigkeit dieser Unternehmen und des Landes insgesamt zu untergraben. So würde der Vorschlag einen Rechtsrahmen schaffen, der nicht nur schlechter ist als derjenige der Europäischen Union, sondern auch Verpflichtungen auferlegt, die nicht einmal die USA haben. Zahlreiche Schweizer Unternehmen haben bereits erklärt, dass sie nicht in der Lage wären, konkurrenzfähig zu sein und glaubwürdige, auf Vertrauen und Sicherheit basierende Dienstleistungen anzubieten, wenn sie zu staatlichen Überwachungsmassnahmen gezwungen würden, die sogar über den Gesetzesrahmen in den USA hinausgehen. Dies würde dazu führen, dass bereits etablierte und erfolgreiche Unternehmen die Schweiz verlassen. Ebenso würde es Unternehmer davon abhalten, Technologieunternehmen in der Schweiz zu gründen – vor allem, wenn sie sehen, dass die Vorschriften schon ab einem Schwellenwert von 5'000 Nutzern gelten. Künftiges Wirtschaftswachstum, Beschäftigung und Steuereinnahmen in der Schweiz würden somit verunmöglich. Selbst der vorgeschlagene höhere Schwellenwert von einer Million Nutzern ist unbedeutend, wenn man Technologieunternehmen miteinbezieht, die erfolgreich exportieren (was angesichts der begrenzten Grösse des Schweizer Binnenmarktes eine Notwendigkeit ist). In den USA und in Europa gibt es keine solchen Schwellenwerte, und Tech-Startups unterliegen keiner obligatorischen Vorratsdatenspeicherung; es gibt also keine künstlichen Wachstumsbarrieren. Durch die Festlegung solcher Schwellenwerte sollen Schweizer Unternehmen für ihren internationalen Erfolg bestraft und das langfristige Potenzial unseres Tech-Ökosystems künstlich begrenzt werden.

Die vorgeschlagene Revision würde Tech-Startups und Scale-ups denselben Verpflichtungen unterwerfen wie grosse Telekommunikationsunternehmen (die allein auf dem Schweizer Markt Milliardenumsätze machen), was sie mit Compliance-Kosten in zweistelliger Millionenhöhe belasten würde. Für Scale-ups mit begrenzten Ressourcen stellt dies eine unzumutbare finanzielle Belastung dar. Auch für Unternehmen in der frühen Wachstumsphase und mit begrenzten finanziellen Reserven ist die Aussicht, Kapital und technische Ressourcen in Überwachungsmassnahmen statt in Innovation und Wettbewerbsfähigkeit zu investieren, fatal.

Die Technologiebranche ist die wettbewerbsintensivste Branche der Welt. Unternehmen entscheiden sich für einen Rechtsstandort, die den Wettbewerb möglichst wenig behindern. Die geplante Revision würde dafür sorgen, dass die Schweiz gar nicht erst in Betracht gezogen wird.

Dauerhafter Reputationsschaden für die Schweiz

Die Schweiz hat sich über ein Jahrhundert hinweg weltweit einen guten Ruf für Stabilität, Privatsphäre und Sicherheit aufgebaut, wovon viele Bereiche der Schweizer Wirtschaft profitieren konnten. Dies gehört bis heute zu den stärksten Wettbewerbsvorteilen der Schweiz und wird seit über hundert Jahren durch einen Rechtsrahmen gestützt, der den USA und der EU überlegen ist. Wird dieser Vorteil aufgegeben und ein Schritt in die entgegengesetzte Richtung anderer europäischer Demokratien gemacht, ist die Revision nichts anderes als ein bedauerlicher Akt der Selbstsabotage.

Ein über viele Jahre aufgebautes Image kann im Handumdrehen zerstört werden: Es braucht nur den Wegzug einiger weniger wichtiger Unternehmen, um den Ruf der Schweiz weltweit dauerhaft zu schädigen. Selbst wenn es nicht erforderlich ist, besser zu sein als die USA oder die EU, müssen wir mindestens gleichwertig sein – und niemals schlechter.

Die vorgeschlagene Überarbeitung der VÜPF soll verworfen werden

In Anbetracht der oben geäusserten Bedenken sind wir der Ansicht, dass die vorgeschlagene Überarbeitung der VÜPF nicht umgesetzt werden sollte und dass ein überwiegendes öffentliches Interesse an der Beibehaltung des Status quo besteht.

Mit freundlichen Grüßen.

L'industrie suisse appelle à un engagement fort pour défendre la compétitivité suisse dans les domaines de la confiance et de la sécurité

6 mai 2025

Cher Conseiller fédéral Jans,

Nous, soussignés, vous écrivons pour vous faire part de nos vives préoccupations concernant le projet de deuxième révision de l'ordonnance sur la surveillance de la correspondance postale et des télécommunications (OSCPT), actuellement en procédure de consultation conduite par le Conseil fédéral. En tant que représentants du secteur technologique, de la communauté juridique, du monde universitaire et des investisseurs en Suisse, nous sommes fermement convaincus que ces propositions constituent une menace existentielle pour la réputation internationale et la prospérité économique future de la Suisse. À ce titre, nous nous opposons par principe aux révisions partielles de l'OSCPT et de l'OME-SCPT.

Nous prenons aujourd'hui la parole car nous estimons que l'adoption de la proposition actuelle sans révision substantielle compromettra les perspectives de croissance future de la Suisse. Bien que les signataires de cette lettre proviennent de secteurs très différents, nous partageons les mêmes préoccupations dans trois domaines:

1. Nous sommes préoccupés par le fait que les propositions visant à étendre massivement la surveillance étatique tout en réduisant le contrôle judiciaire menacent les droits fondamentaux des citoyens suisses ainsi que ceux de nos clients à l'échelle internationale.
2. La proposition est rédigée en des termes si généraux qu'elle pourrait s'appliquer à pratiquement toutes les entreprises technologiques suisses et risquer de nuire à la compétitivité du secteur technologique suisse à un moment où celui-ci connaît une opportunité de croissance sans précédent en Europe.
3. Nous estimons que certaines propositions, telles que la conservation obligatoire des métadonnées appliquée de manière générale, éloignent la Suisse des normes européennes et américaines et la rapprochent des normes russes ou chinoises, au risque de nuire de manière permanente à la réputation de la Suisse en matière de confiance, de sécurité et de protection de la vie privée, au détriment d'un large éventail d'industries actuelles et futures.

Atteinte à la vie privée et à la sécurité des citoyens suisses

Le cadre de surveillance existant en Suisse fait déjà l'objet d'abus généralisés, largement relayés par les médias. La proposition actuelle, qui vise à étendre la surveillance tout en supprimant le contrôle judiciaire, ne fera qu'aggraver le problème. En vertu de cette proposition, les fournisseurs de services suisses pourraient être contraints de partager automatiquement des données sans possibilité de vérifier l'exactitude des demandes afin de s'assurer qu'il n'y a pas d'abus du système. À cela s'ajoute une augmentation massive de la quantité de données à conserver, ainsi qu'un élargissement du champ d'application des entreprises pouvant être soumises à ces obligations. Ces obligations de conservation des métadonnées sont considérées comme si lourdes et contraires au principe des droits fondamentaux à la vie privée qu'elles ont été jugées illégales à plusieurs reprises dans l'Union européenne. En poursuivant ces propositions, la Suisse s'apprête à introduire une forme de surveillance qui n'existe aujourd'hui dans aucun autre pays démocratique comparable.

Obliger les entreprises suisses à conserver des données sensibles, ce que les entreprises européennes et américaines ne sont pas tenues de faire, rendra également les entreprises suisses plus attractives pour les cyberattaques, attirant à la fois les cybercriminels et les acteurs étatiques tels que la Russie, la Chine et la Corée du Nord, qui mèneront des attaques contre les entreprises et les infrastructures suisses. En outre, le fait d'imposer aux services gouvernementaux suisses un accès automatisé par une « porte dérobée » aux données détenues par les entreprises technologiques suisses rendra également le gouvernement suisse une cible encore plus importante.

En effet, le CSI-DFPJ, le département fédéral qui serait chargé de maintenir cette porte dérobée, a lui-même été piraté et victime d'une fuite de données en 2023. Si elle était adoptée, cette proposition aggraverait considérablement les violations inévitables à l'avenir, en donnant aux attaquants un accès dérobé à un large éventail d'entreprises technologiques suisses, ce qui multiplierait de manière exponentielle la menace pour les citoyens suisses.

Attaque contre la compétitivité du secteur technologique suisse

La technologie est le principal moteur de la croissance économique mondiale depuis trois décennies, mais en adoptant ces propositions, le Conseil fédéral fera en sorte que la Suisse passe à côté de cette opportunité de croissance.

À l'heure où les consommateurs et les entreprises du monde entier recherchent des produits technologiques offrant une plus grande sécurité et où les événements géopolitiques stimulent la demande en technologies européennes, la Suisse a l'opportunité de développer une industrie technologique locale dynamique et prospère. Certains signataires de cette lettre ont d'ailleurs convaincu des centaines de millions de clients à travers le monde au cours des dix dernières années, démontrant ainsi que la Suisse est en mesure de tirer parti de cette opportunité.

Toutefois, le deuxième projet de révision de l'OSCPT menace de nuire à la compétitivité de ces entreprises et du pays dans son ensemble.

Les propositions créeraient un cadre juridique non seulement pire que celui de l'Union européenne, mais imposeraient également des obligations que même les États-Unis n'ont pas. De nombreuses entreprises suisses ont déjà déclaré qu'elles ne seraient pas en mesure de fournir des services crédibles basés sur la confiance et la sécurité si elles étaient contraintes de se livrer à des activités d'espionnage d'État allant même au-delà de ce qu'exige la législation américaine. Cela entraînerait le départ de la Suisse d'entreprises déjà bien établies et prospères. Cela dissuaderait également les futurs créateurs d'entreprises technologiques de s'implanter en Suisse, surtout lorsqu'ils se rendraient compte qu'ils pourraient être obligés de se conformer à cette réglementation dès qu'ils atteindraient le seuil de 5'000 utilisateurs, ce qui freinerait la croissance économique, l'emploi et les recettes fiscales en Suisse. Même le seuil le plus élevé proposé de 1 million d'utilisateurs est insignifiant si l'on considère les entreprises technologiques qui exportent avec succès, ce qui est une nécessité compte tenu de la taille limitée du marché intérieur suisse. Aucun seuil de ce type n'existe aux États-Unis et en Europe, et les startups technologiques ne sont jamais soumises à une obligation de conservation des données, ce qui signifie qu'il n'existe aucun obstacle artificiel à leur croissance. En fixant ces seuils, cette proposition vise à punir les entreprises suisses pour leur succès international et à limiter artificiellement le potentiel à long terme de notre écosystème technologique.

En soumettant les startups et les scale-ups technologiques à la possibilité d'avoir les mêmes obligations que les grandes entreprises de télécommunications qui réalisent des milliards de

chiffre d'affaires rien qu'sur le marché suisse, la révision proposée imposerait à ces entreprises des coûts de mise en conformité pouvant atteindre plusieurs dizaines de millions de francs suisses, ce qui créerait une charge financière inacceptable pour les scale-ups disposant de ressources limitées.

Pour les entreprises en phase de croissance et disposant de réserves financières limitées, la perspective de devoir consacrer des liquidités et des capacités d'ingénierie à ces mesures de surveillance plutôt qu'à l'innovation et à la concurrence est fatale. Le secteur technologique est le plus concurrentiel au monde. Tout chef d'entreprise doté d'un minimum de sens des affaires choisirait une juridiction qui facilite autant que possible la concurrence, et ces propositions feraient en sorte que la Suisse ne soit même pas prise en considération.

Dommage irréparable à la réputation de la Suisse

La Suisse s'est forgée au cours d'un siècle une réputation mondiale en matière de stabilité, de protection de la sphère privée et de sécurité. Cela a grandement profité à de nombreux secteurs de l'économie suisse au cours du siècle dernier et continue d'être l'un des principaux avantages concurrentiels de la Suisse.

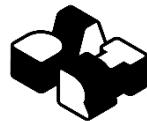
Pendant plus de cent ans, cette réputation a été soutenue par un cadre juridique supérieur qualitativement à celui des États-Unis et de l'Union européenne. En renonçant à cet avantage et en faisant ce qu'aucune autre démocratie occidentale n'a osé faire, la révision proposée constitue un acte d'autosabotage qui ferait de la Russie le plus proche voisin européen de la Suisse.

Une réputation bâtie en un siècle peut être détruite en un instant, il suffirait que quelques entreprises clés quittent le pays pour nuire de manière irréversible à la réputation de la Suisse à l'échelle mondiale. Même s'il n'est pas jugé nécessaire de faire mieux que les États-Unis et l'UE, nous devons au moins être équivalents, et jamais pires.

La révision proposée de l'OSCPT doit être abandonnée

Compte tenu des préoccupations exprimées ci-dessus, nous estimons que la révision proposée de l'OSCPT doit être abandonnée et qu'il existe un intérêt public supérieur à préserver le statu quo actuel.

Veuillez agréer l'expression de nos salutations distinguées.



Fondation Genevoise pour l'Innovation Technologique



THE PERFECT SETTING TO INNOVATE



ACE & Company SA

ACE & Company is a private equity and venture capital firm based in Geneva with over 1.8 billion CHF in assets under management.

ACE & Company ist eine Private-Equity- und Risikokapitalgesellschaft mit Sitz in Genf, Schweiz, und verwaltet ein Vermögen von über 1,8 Milliarden CHF.

ACE & Company est une société de capital-investissement et de capital-risque basée à Genève qui gère plus de 1,8 milliard de francs suisses d'actifs.

ACE Ventures

ACE Ventures is an early-stage VC fund with over \$400 million in assets under management, based in Zurich, Geneva and London. Their latest fund, ACE Swiss Tech Outliers, backs early-stage stage Swiss tech founders.

ACE Ventures ist ein Early-Stage-Risikokapitalfonds mit einem verwalteten Vermögen von über 400 Millionen US-Dollar und Sitz in Zürich, Genf und London. Ihr neuester Fonds, ACE Swiss Tech Outliers, unterstützt Schweizer Tech-Gründer in der Frühphase.

ACE Ventures est un fonds de capital-risque spécialisé dans les entreprises en phase de démarrage, avec plus de 400 millions de dollars d'actifs sous gestion, basé à Zurich, Genève et Londres. Son dernier fonds, ACE Swiss Tech Outliers, soutient les fondateurs suisses de startups technologiques en phase de démarrage.

Association Innovaud

Innovaud is the innovation and economic promotion agency of the canton of Vaud supporting more than 2'000 technology companies that employ together over 50'000 people.

Innovaud ist die Innovations- und Wirtschaftsförderungsagentur des Kantons Waadt und unterstützt mehr als 2'000 Technologieunternehmen, die über 50'000 Mitarbeiter beschäftigen.

Innovaud est l'agence pour l'innovation et la promotion économique du canton de Vaud qui soutient plus de 2'000 entreprises technologiques employant au total plus de 50'000 personnes.

ANYbotics AG

ANYbotics is an ETHZ spinoff which develops robotic solutions to automate industrial inspection. ANYbotics is a fast-growing scaleup that has raised over 130 million CHF and employs more than 200 people.

ANYbotics ist ein Spin-off der ETHZ, das Roboterlösungen für die Automatisierung industrieller Inspektionen entwickelt. ANYbotics ist ein schnell wachsendes Scale-up-Unternehmen, das über 130 Millionen CHF eingeworben hat und mehr als 200 Mitarbeiter beschäftigt.

ANYbotics est un spin-off de l'ETH qui développe des solutions robotiques pour automatiser l'inspection industrielle. ANYbotics est une scale-up en pleine croissance qui a levé plus de 130 millions de francs suisses et emploie plus de 200 personnes.

Chambre de commerce, d'industrie et des services de Genève (CCIG)

With some 2'600 member companies, CCIG is the leading business association within the Canton of Geneva and has been representing the Geneva business community since 1865.

Mit rund 2'600 Mitgliedsunternehmen ist die CCIG der führende Wirtschaftsverband im Kanton Genf und vertritt die Genfer Wirtschaft seit 1865.

Avec quelque 2'600 entreprises membres, la CCIG est la principale association commerciale du canton de Genève et représente la communauté économique genevoise depuis 1865.

Chambre vaudoise du commerce et de l'industrie (CVCI)

With some 3'300 member companies, CVCI is the leading business association within the Canton of Vaud and has been representing the Vaud business community since 1898.

Mit rund 3'300 Mitgliedsunternehmen ist die CVCI der führende Wirtschaftsverband im Kanton Waadt und vertritt seit 1898 die Waadtländer Wirtschaft.

Comptant environ 3'300 entreprises membres, la CVCI est la principale association commerciale du canton de Vaud et représente la communauté économique vaudoise depuis 1898.

DART Ventures AG

DART is a Swiss venture capital firm focusing on helping early-stage Swiss and European companies successfully export into the US and other international markets.

DART ist eine Schweizer Risikokapitalgesellschaft, die sich darauf fokussiert, Schweizer und europäische Unternehmen in der Frühphase ihres Bestehens beim erfolgreichen Eintritt in die USA und andere internationale Märkte zu unterstützen.

DART est une société suisse de capital-risque qui aide les entreprises suisses et européennes en phase de démarrage à réussir leur exportation vers les États-Unis et d'autres marchés internationaux.

DreamLab Technologies AG

DreamLab is a cutting-edge cybersecurity firm specializing in offensive and defensive security, cyber intelligence, and digital risk protection for governments, critical infrastructure and private enterprises worldwide.

DreamLab ist ein innovatives Cybersicherheitsunternehmen, das sich auf offensive und defensive Sicherheit, Cyber-Intelligenz und den Schutz vor digitalen Risiken für Regierungen, kritische Infrastrukturen und private Unternehmen weltweit spezialisiert hat.

DreamLab est une entreprise de cybersécurité de pointe spécialisée dans la sécurité offensive et défensive, le renseignement cybérétique et la protection contre les risques numériques pour les gouvernements, les infrastructures critiques et les entreprises privées du monde entier.

EPFL Innovation Park

EPFL Innovation Park is a dynamic hub for deep-tech innovation situated on the campus of the Ecole Polytechnique Fédérale de Lausanne (EPFL). It serves as a bridge between cutting-edge academic research and the commercial world, having fostered the development of more than 500 startups and scaleups over the last 30 years.

Der EPFL Innovation Park ist ein dynamischer Hub für Deep-Tech-Innovationen auf dem Campus der Ecole Polytechnique Fédérale de Lausanne (EPFL). Er fungiert als Brücke zwischen Spitzenforschung und Wirtschaft und hat in den letzten 30 Jahren die Entwicklung von mehr als 500 Start-ups und Scale-ups gefördert.

L'EPFL Innovation Park est un pôle dynamique dédié à l'innovation deep tech situé sur le campus de l'École polytechnique fédérale de Lausanne (EPFL). Il sert de passerelle entre la recherche universitaire de pointe et le monde commercial, ayant favorisé le développement de plus de 500 startups et scale-ups au cours des 30 dernières années.

Exoscale (Akenes AG)

Exoscale is a cloud infrastructure provider with its headquarters in Lausanne. The company specialized in offering Infrastructure-as-a-Service (IaaS) solutions tailored for developers, startups and data scientists, emphasizing privacy, scalability and European data sovereignty.

Exoscale ist ein Cloud-Infrastruktur-Anbieter mit Hauptsitz in Lausanne. Das Unternehmen hat sich auf Infrastructure-as-a-Service (IaaS)-Lösungen spezialisiert, die auf Entwickler, Startups und Datenwissenschaftler zugeschnitten sind und besonderen Wert auf Datenschutz, Skalierbarkeit und europäische Datenhoheit legen.

Exoscale est un fournisseur d'infrastructure cloud dont le siège social est situé à Lausanne. L'entreprise est spécialisée dans l'offre de solutions d'infrastructure en tant que service (IaaS) adaptées aux développeurs, aux startups et aux scientifiques des données, en mettant l'accent sur la confidentialité, l'évolutivité et la souveraineté européenne des données.

Fédération Suisse des Entreprises / Der Gewerberein

The Swiss Federation of Enterprises brings together more than 1'000 SMEs from all over Switzerland with a shared commitment towards economic prosperity through sustainable entrepreneurship.

Der Gewerberein vereint mehr als 1'000 KMU aus der ganzen Schweiz mit einem gemeinsamen Engagement für wirtschaftlichen Wohlstand durch nachhaltiges Unternehmertum.

La Fédération Suisse des Entreprises regroupe plus de 1'000 PME de toute la Suisse qui partagent un engagement commun en faveur de la prospérité économique grâce à un entrepreneurat durable.

Fondation digiVolution

digiVolution is a digital space observatory serving political, academic and economic decision-makers. digiVolution contributes to the public dialog in Swiss politics on security and digital aspects of society.

digiVolution ist eine Beobachtungsstelle für den digitalen Raum im Dienste von politischen, akademischen und wirtschaftlichen Entscheidungsträgern. digiVolution leistet einen Beitrag zum öffentlichen Dialog in der Schweizer Politik über Sicherheit und digitale Aspekte der Gesellschaft.

digiVolution est un observatoire numérique au service des décideurs politiques, universitaires et économiques. digiVolution contribue au débat public en Suisse sur les aspects sécuritaires et numériques de la société.

Fondation Genevoise pour l'Innovation Technologique (FONGIT)

FONGIT is Switzerland's oldest startup incubator first established in 1991. In the past 10 years, FONGIT companies have created 1'800 jobs, raised over 1 billion CHF in funding, and today include 4 unicorns (startups valued at over 1 billion CHF).

FONGIT ist der älteste Startup-Inkubator der Schweiz, der 1991 gegründet wurde. In den letzten 10 Jahren haben die FONGIT-Unternehmen 1'800 Arbeitsplätze geschaffen, über 1 Milliarde CHF an Finanzmitteln eingeworben und umfassen heute 4 Einhörner (Startups im Wert von über 1 Milliarde CHF).

FONGIT est le plus ancien incubateur de startup de Suisse, créé en 1991. Au cours des dix dernières années, les entreprises de FONGIT ont créé 1'800 emplois, levé plus d'un milliard de francs suisses de fonds et comptent aujourd'hui quatre licornes (startup valorisées à plus d'un milliard de francs suisses).

Fondation pour Genève

The Fondation pour Genève is a non-profit that works closely with Federal and cantonal authorities to promote Geneva's influence, attractiveness, and openness to the world. It is currently chaired by Marc Pictet, Senior Partner at Pictet Group.

Die Fondation pour Genève ist eine Non-Profit-Organisation, die eng mit den Bundes- und Kantonsbehörden zusammenarbeitet, um den Einfluss, die Attraktivität und die Weltoffenheit von Genf zu fördern. Sie wird derzeit von Marc Pictet, Senior Partner der Pictet-Gruppe, präsidiert.

La Fondation pour Genève est une organisation à but non lucratif qui travaille en étroite collaboration avec les autorités fédérales et cantonales afin de promouvoir l'influence, l'attractivité et l'ouverture de Genève sur le monde. Elle est actuellement présidée par Marc Pictet, associé senior du groupe Pictet.

Fondation pour l'innovation et la technologie (FIT)

Founded in 1994, the FIT supports the creation and development of new companies in the canton of Vaud and French-speaking Switzerland. It currently supports over 300 startups which employ more than 6'000 people.

Der FIT wurde 1994 gegründet und unterstützt die Gründung und Entwicklung neuer Unternehmen im Kanton Waadt und in der französischsprachigen Schweiz. Derzeit fördert er über 300 Startups, die mehr als 6'000 Mitarbeiter beschäftigen.

Fondé en 1994, la FIT soutient la création et le développement de nouvelles entreprises dans le canton de Vaud et en Suisse romande. Il accompagne actuellement plus de 300 startups qui emploient au total plus de 6'000 personnes.

Founderful AG

Founderful is one of Switzerland's most active early-stage venture capital firms, and the only focusing exclusively on Switzerland. Founderful backed companies have created more than 1'200 jobs.

Founderful ist eine der aktivsten Frühphasen-Risikokapitalgesellschaften in der Schweiz und die einzige, die sich ausschliesslich auf die Schweiz konzentriert. Die von Founderful unterstützten Unternehmen haben mehr als 1'200 Arbeitsplätze geschaffen.

Founderful est l'une des sociétés de capital-risque les plus actives en Suisse dans le domaine des entreprises en phase de démarrage, et la seule à se concentrer exclusivement sur la Suisse. Les entreprises soutenues par Founderful ont créé plus de 1'200 emplois.

Geneva Center for Neutrality

The Geneva Center for Neutrality is a think-tank committed to the importance of dialogue and democratic debate. It aims to create spaces for reflection and discussion on issues related to neutrality, with a particular focus on Swiss neutrality.

Das Genfer Zentrum für Neutralität ist ein Think-Tank, der sich der Bedeutung des Dialogs und der demokratischen Debatte verschrieben hat. Es will Räume für Reflexion und Diskussion über Fragen der Neutralität schaffen, mit besonderem Augenmerk auf die Schweizer Neutralität.

Le Centre de Genève pour la Neutralité est un groupe de réflexion qui s'engage en faveur du dialogue et du débat démocratique. Il vise à créer des espaces de réflexion et de discussion sur les questions liées à la neutralité, en mettant particulièrement l'accent sur la neutralité suisse.

Hostpoint AG

With more than 20 years of experience, Hostpoint is the largest web hosting provider and leading domain registrar in Switzerland. Hostpoint offers simple solutions from a single source – for domains, websites, online stores, and e-mail. Hostpoint has its headquarters in Rapperswil-Jona.

Mit über 20 Jahren Erfahrung ist Hostpoint der grösste Webhosting-Provider und führender Domainregistrar der Schweiz. Hostpoint bietet einfache und unkomplizierte Lösungen aus einer Hand – für Domains, Websites, Webshops und E-Mail. Hostpoint hat seinen Hauptsitz in Rapperswil-Jona.

Avec plus de 20 ans d'expérience, Hostpoint est le plus grand hébergeur web et le premier registraire de noms de domaine en Suisse. Hostpoint propose des solutions simples d'un seul tenant pour les domaines, les sites web, les boutiques en ligne et les e-mails. Hostpoint a son siège à Rapperswil-Jona.

iWay AG

Founded in 1995, iWay is one of the leading Swiss Internet providers for private individuals and SMEs, offering solutions for Internet, telephony, mobile, TV, hosting & cloud, and datacenters.

iWay wurde 1995 gegründet und ist einer der führenden Schweizer Internet-Provider für Privatpersonen und KMU und bietet Lösungen für Internet, Telefonie, Mobile, TV, Hosting & Cloud und Rechenzentren.

Fondée en 1995, iWay est l'un des principaux fournisseurs d'accès Internet suisses pour les particuliers et les PME. Elle propose des solutions pour l'Internet, la téléphonie, la téléphonie mobile, la télévision, l'hébergement et le cloud, ainsi que des centres de données.

NexThink SA

NexThink is a digital employee experience platform founded by EPFL PhD students in 2004. Since then, NexThink has raised over 300 million CHF in venture capital and is one of three Swiss SaaS (software-as-a-service) unicorns.

NexThink ist eine Plattform für digitale Mitarbeitererfahrung, die 2004 von EPFL-Doktoranden gegründet wurde. Seither hat NexThink über 300 Millionen CHF an Risikokapital eingeworben und ist eines von drei Schweizer SaaS (Software-as-a-Service)-Unicorns.

NexThink est une plateforme d'expérience numérique pour les employés fondée en 2004 par des doctorants de l'EPFL. Depuis lors, NexThink a levé plus de 300 millions de francs suisses en capital-risque et fait partie des trois licornes suisses du secteur SaaS (software-as-a-service).

NTS Workspace AG

NTS is a Swiss fiber network operator with over 20 years of experience. The NTS fiber-optic backbone covers the whole of Switzerland and the company also operates carrier-neutral data centers in Bern and Zurich.

NTS ist ein Schweizer Glasfasernetzbetreiber mit über 20 Jahren Erfahrung. Das Glasfaser-Backbone von NTS deckt die gesamte Schweiz ab und das Unternehmen betreibt zudem Carrier-neutrale Rechenzentren in Bern und Zürich.

NTS est un opérateur de réseau fibre optique suisse qui compte plus de 20 ans d'expérience. Le réseau fibre optique de NTS couvre l'ensemble du territoire suisse et l'entreprise exploite également des centres de données neutres à Berne et Zurich.

Nym Technologies SA

Nym is a privacy company based in Neuchâtel whose mission is to create technology that empowers individuals to take control of their digital lives, to overcome barriers to information.

Nym ist ein Unternehmen für den Schutz der Privatsphäre mit Sitz in Neuchâtel, dessen Mission es ist, Technologien zu entwickeln, die Menschen in die Lage versetzen, die Kontrolle über sein digitales Leben zu übernehmen und Informationsbarrieren zu überwinden.

Nym est une entreprise spécialisée dans la protection de la vie privée basée à Neuchâtel, dont la mission est de créer des technologies qui permettent aux individus de prendre le contrôle de leur vie numérique et de surmonter les obstacles à l'accès à l'information.

OneDoc SA

OneDoc was founded by two EPFL graduates in 2017 and is the leading online booking platform for medical appointments in Switzerland, with more than 2.6 million Swiss having an OneDoc account.

OneDoc wurde 2017 von zwei EPFL-Absolventen gegründet und ist die führende Online-Buchungsplattform für Arzttermine in der Schweiz, mit mehr als 2,6 Millionen Schweizerinnen und Schweizern mit einem OneDoc-Konto.

Fondée en 2017 par deux diplômés de l'EPFL, OneDoc est la première plateforme de prise de rendez-vous médicaux en ligne en Suisse, avec plus de 2,6 millions de comptes OneDoc.

Prof. Dr. Simon Schlauri, Ronzani Schlauri Attorneys

Prof. Dr. Schlauri is one of the leading lawyers in IT and telecommunications in Switzerland and is also an adjunct professor at the University of Zurich.

Prof. Dr. Schlauri gehört zu den führenden Anwälten im Bereich IT und Telekommunikation in der Schweiz und ist ausserordentlicher Professor an der Universität Zürich.

Le Prof. Dr. Schlauri est l'un des avocats les plus éminents dans le domaine des technologies de l'information et des télécommunications en Suisse. Il est également professeur associé à l'université de Zurich.

Proton AG

Proton is one of the world's leading privacy and security companies, providing encrypted email, cloud storage, password management, and VPN services to over 100 million end users. Proton is headquartered in Geneva and employs 500 people.

Proton ist eines der weltweit führenden Unternehmen im Bereich Datenschutz und Sicherheit und bietet verschlüsselte E-Mails, Cloud-Speicher, Passwortmanagement und VPN-Dienste für über 100 Millionen Endbenutzer. Proton hat seinen Hauptsitz in Genf und beschäftigt 500 Mitarbeitende.

Proton est l'une des principales entreprises mondiales dans le domaine de la confidentialité et de la sécurité. Elle fournit des services de messagerie électronique cryptée, de stockage dans le cloud, de gestion des mots de passe et de VPN à plus de 100 millions d'utilisateurs. Proton a son siège à Genève et emploie 500 personnes.

Redalpine Venture Partners AG

Redalpine is one of the first multi-stage venture capital firm in Switzerland specializing in investing at the intersection of software and science. Redalpine portfolio companies have created 10'000 jobs and raised over 3 billion CHF.

Redalpine ist eine der ersten mehrstufigen Risikokapitalgesellschaften in der Schweiz, die sich auf Investitionen an der Schnittstelle zwischen Software und Wissenschaft spezialisiert hat. Die Portfoliounternehmen von Redalpine haben 10'000 Arbeitsplätze geschaffen und über 3 Milliarden CHF eingenommen.

Redalpine est l'une des premières sociétés de capital-risque multi-stades en Suisse spécialisée dans les investissements à la croisée du logiciel et de la science. Les entreprises du portefeuille de Redalpine ont créé 10'000 emplois et levé plus de 3 milliards de francs suisses.

Seedstars SA

Seedstars is an international impact investing and education company headquartered in Switzerland but present in 90+ countries. Seedstars invests in promising entrepreneurs of high growth companies, particularly in the developing world.

Seedstars ist ein internationales Unternehmen für Impact Investing und Bildung mit Hauptsitz in der Schweiz und in über 90 Ländern tätig. Seedstars investiert in vielversprechende Unternehmer von wachstumsstarken Unternehmen, insbesondere in Entwicklungsländern.

Seedstars est une société internationale d'investissement à impact social et d'éducation dont le siège social est situé en Suisse, mais qui est présente dans plus de 90 pays. Seedstars investit dans des entrepreneurs prometteurs issus d'entreprises à forte croissance, en particulier dans les pays en développement.

Session Technology Foundation (STF)

STF is the non-profit foundation behind the Session Protocol, a new standard for decentralized private messaging. Session relocated to Switzerland in 2024 specifically due to the privacy laws which are now at threat.

STF ist die gemeinnützige Stiftung, die hinter dem Session-Protokoll steht, einem neuen Standard für dezentralen privaten Nachrichtenaustausch. Session ist 2024 in die Schweiz umgezogen, insbesondere wegen der Datenschutzgesetze, die jetzt bedroht sind.

STF est la fondation à but non lucratif à l'origine du protocole Session, une nouvelle norme pour la messagerie privée décentralisée. Session s'est installée en Suisse en 2024, précisément en raison des lois sur la protection de la vie privée qui sont aujourd'hui menacées.

SIX Group

SIX manages Switzerland's primary stock exchange.

SIX verwaltet die führende Börse der Schweiz.

SIX gère la principale bourse suisse.

SonarSource SA

Headquartered in Geneva, SonarSource is the global leader in developing software for continuous code quality and security. It is one of three SaaS unicorns in Switzerland and has raised over 400 million CHF at a valuation of more than 4 billion CHF.

Mit Hauptsitz in Genf, ist SonarSource weltweit führend in der Entwicklung von Software für kontinuierliche Codequalität und Sicherheit. Das Unternehmen ist eines von drei SaaS-Einhörnern in der Schweiz und hat über 400 Millionen CHF bei einer Bewertung von mehr als 4 Milliarden CHF aufgenommen.

Ayant son siège à Genève, SonarSource est le leader mondial dans le développement de logiciels pour la qualité et la sécurité continues du code. Elle est l'une des trois licornes SaaS en Suisse et a levé plus de 400 millions de francs suisses pour une valorisation supérieure à 4 milliards de francs suisses.

SwissIX Internet Exchange

SwissIX is the largest Internet Exchange Point (IXP) in Switzerland and is present in 7 datacenters across Switzerland.

SwissIX ist der grösste Internet Exchange Point (IXP) der Schweiz und ist in 7 Rechenzentren in der ganzen Schweiz vertreten.

SwissIX est le plus grand point d'échange Internet (IXP) de Suisse et est présent dans 7 centres de données à travers le pays.

Swiss Startup Association (SSA)

With more than 1'600 startup members, the SSA works to enhance the framework conditions for startups in Switzerland and provide them with a unified voice. The SSA collaborates closely with various other startup organizations and associations, regularly exchanging ideas to position Switzerland as the leading startup nation in Europe.

Mit mehr als 1'600 Start-up-Mitgliedern setzt sich die SSA dafür ein, die Rahmenbedingungen für Start-ups in der Schweiz zu verbessern und ihnen eine einheitliche Stimme zu geben. Die SSA arbeitet eng mit verschiedenen anderen Start-up-Organisationen und Verbänden zusammen und tauscht regelmässig Ideen aus, um die Schweiz als führende Start-up-Nation in Europa zu positionieren.

Avec plus de 1'600 membres, la SSA s'engage à améliorer les conditions-cadres pour les startup en Suisse et à leur donner une voix unifiée. Elle collabore étroitement avec diverses autres organisations et associations de startup, échangeant régulièrement des idées afin de positionner la Suisse comme la première nation européenne pour les startups.

Threema GmbH

Threema is a leading encrypted messengers for business and individuals. Threema is based in Pfäffikon (Schwyz) and has millions of customers around the world, including the Swiss army.

Threema ist ein führender verschlüsselter Messenger für Unternehmen und Privatpersonen. Threema hat seinen Sitz in Pfäffikon (Schwyz) und hat Millionen von Kunden auf der ganzen Welt, darunter auch die Schweizer Armee.

Threema est l'un des principaux services de messagerie cryptée pour les entreprises et les particuliers. Basée à Pfäffikon (Schwyz), Threema compte des millions de clients dans le monde entier, dont l'armée suisse.

Trust Valley

Trust Valley is a public-private partnership founded by the Canton of Vaud, the Canton of Geneva, EPFL, UNIGE, and others to promote the excellence of the Lake Geneva region in the fields of digital trust and cybersecurity.

Trust Valley ist eine öffentlich-private Partnerschaft, die vom Kanton Waadt, dem Kanton Genf, der EPFL, der UNIGE und anderen gegründet wurde, um die Exzellenz der Genferseeregion in den Bereichen digitales Vertrauen und Cybersicherheit zu fördern.

Trust Valley est un partenariat public-privé fondé par le canton de Vaud, le canton de Genève, l'EPFL, l'UNIGE et d'autres acteurs afin de promouvoir l'excellence de la région lémanique dans les domaines de la confiance numérique et de la cybersécurité.

VTX Services SA (Groupe Celeste)

Celeste is a fiber and cloud operator, serving over 20'000 enterprise customers in France and Switzerland. Celeste owns dedicated fiber networks and datacenters in both countries.

Celeste ist ein Glasfaser- und Cloud-Betreiber, der über 20'000 Unternehmenskunden in Frankreich und der Schweiz bedient. Celeste besitzt dedizierte Glasfasernetze und Rechenzentren in beiden Ländern.

Celeste est un opérateur fibre et cloud qui dessert plus de 20'000 entreprises en France et en Suisse. Celeste possède des réseaux fibre dédiés et des centres de données dans les deux pays.

Wire Swiss GmbH

Based in Zug, Wire is a leading encrypted messenger for businesses. Since 2024, Wire has been a strategic partner of Schwarz Group, which has a total turnover of over 140 billion CHF.

Mit Hauptsitz in Zug, ist Wire ein führender verschlüsselter Messenger für Unternehmen. Seit 2024 ist Wire ein strategischer Partner der Schwarz Gruppe, die einen Gesamtumsatz von über 140 Milliarden CHF erzielt.

Basée à Zoug, Wire est l'un des principaux services de messagerie cryptée pour les entreprises. Depuis 2024, Wire est un partenaire stratégique du groupe Schwarz, qui réalise un chiffre d'affaires total de plus de 140 milliards de francs suisses.



DIDAS Stellungnahme

zu den

Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)
und Verordnung des EJPD über die Durchführung der Überwachung des Post- und
Fernmeldeverkehrs (VD-ÜPF)

Eingereicht an:

Bundesrat Beat Jans
Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements EJPD
Bundeshaus West
CH-3003 Bern
per Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Eingereicht durch:

Digital Identity and Data Sovereignty Association (www.didas.swiss)
Campus Zug Rotkreuz
Surstoffi 1
CH-6343 Rotkreuz
info@didas.swiss

Rotkreuz, im Mai 2025

Sehr geehrter Herr Bundesrat Jans
Sehr geehrte Empfänger:innen

Im Namen der Digital Identity and Data Sovereignty Association (DIDAS) möchten wir unsere Besorgnis über die geplante Teilrevision der Verordnungen VÜPF und VD-ÜPF zum Ausdruck bringen. Wir schätzen die laufenden Bemühungen des Bundesrats zur Stärkung der digitalen Sicherheit, sehen jedoch in den vorgeschlagenen Anpassungen erhebliche Risiken für den Schutz der Privatsphäre, die Innovationskraft der Schweiz sowie die Glaubwürdigkeit des Landes als vertrauenswürdiger Standort für digitale Dienste. Vor diesem Hintergrund unterstützen wir die Stellungnahme der Digitalen Gesellschaft ausdrücklich und legen Ihnen unsere Position in diesem Schreiben dar.

Wir appellieren an den Bundesrat, die Kohärenz der digitalen Strategie der Schweiz sicherzustellen. Während in öffentlichen Erklärungen – etwa in den Grussbotschaften zur DICE-Konferenz und zum OpenWallet Forum - das Vertrauen, die digitale Souveränität und die Förderung von Privacy-by-Design-Technologien als zentrale Leitprinzipien hervorgehoben werden, widersprechen die geplanten Anpassungen der Überwachungsverordnungen diesen Zielen fundamental. Eine glaubwürdige Digitalpolitik erfordert klare, konsistente Signale: Regulatorische Eingriffe dürfen nicht innovationshemmend wirken und sollen stets im Einklang mit rechtsstaatlichen und völkerrechtlichen Grundsätzen sowie dem Schutz der Privatsphäre stehen.

Hochachtungsvoll,



Daniel Säuberli
Präsident



Tim Weingärtner
Vizepräsident

Die Digital Identity and Data Sovereignty Association (DIDAS) unterstützt die Stellungnahme der Digitalen Gesellschaft gegen die geplante Teilrevision der Verordnungen VÜPF und VD-ÜPF

Die Stellungnahme des Vereins Digitale Gesellschaft kann hier eingesehen werden:

<https://www.digitale-gesellschaft.ch/uploads/2025/05/Stellungnahme-Digitale-Gesellschaft-VUEPF-VD-UePF.pdf>

Die geplanten Änderungen der Teilrevision würden nicht nur - wie in der Stellungnahme der Digitalen Gesellschaft dargelegt - die Privatsphäre beeinträchtigen, sondern auch die Attraktivität der Schweiz als Standort für vertrauenswürdige digitale Dienste wie Proton, Threema oder künftig interessierte internationale Anbieter untergraben, die besonderen Wert auf Datenschutz, digitale Selbstbestimmung und rechtsstaatliche Stabilität legen. Zudem ist die Schweiz mit ihren Aktivitäten rund um die Vertrauensinfrastruktur und die E-ID aktuell hervorragend positioniert, sich international als führender Showcase für menschenzentrierte, datenschutzfreundliche digitale Identitäts- und Vertrauenssysteme zu etablieren. Dieses Potenzial gilt es zu schützen, nicht zu gefährden.

Die Schweiz soll ein glaubwürdiger, innovationsstarker Vertrauensstandort für digitale Innovation durch verifizierbare Daten sowie sicherer und vertrauenswürdiger Kommunikation bleiben, respektive diesen weiter ausbauen und fördern.

Wir sehen dabei eine strategische Inkonsistenz zwischen der aktuellen Regulierungsentwicklung und den in den letzten Monaten auf höchster Ebene formulierten Zielsetzungen:

- In der Grussbotschaft zur Digital Identity unConference Europe (DICE) betont Bundesrat Beat Jans die zentrale Bedeutung des Vertrauens in der digitalen Welt und der Notwendigkeit eines menschenzentrierten digitalen Ökosystems.
<https://www.eid.admin.ch/de/grussbotschaft-von-bundesrat-beat-jans-zur-der-digital-identity-unconference-europe-dice>
- In seiner Ansprache zum OpenWallet Forum High-Level Panel anlässlich des WEF in Davos, sprechst sich Bundesrat Beat Jans für eine sichere und transparente digitale Infrastruktur aus, die Rechtsstaatlichkeit, das Völkerrecht und die Privatsphäre gleichzeitig gewährleistet. <https://www.eid.admin.ch/de/openwallet-forum-high-level-panel-meeting-d>

Die geplante Revision der VÜPF / VD-ÜPF steht diesen Grundsätzen somit fast diametral entgegen. Sie schwächt nicht nur das Vertrauen, sondern gefährdet auch eine der wichtigsten zukünftigen Erfolgschancen der Schweiz: Ihre Positionierung als global führender

Innovationshub und Anwender von kryptologischen Errungenschaften und Privacy Enhancing Technologies (PETs), digitalen Vertrauensdiensten sowie der sicheren Kommunikation.

Die Schweiz muss eine kohärente Strategie verfolgen, die Strafverfolgung im digitalen Raum ermöglicht, jedoch nicht auf Kosten des Rechtsstaatsprinzips und des Schutzes der Privatsphäre. Eine zukunftsfähige Digitalpolitik erfordert eine sorgfältige Balance zwischen dem berechtigten Interesse an Sicherheit und Strafverfolgung einerseits und dem Schutz der Privatsphäre sowie der digitalen Selbstbestimmung andererseits. Transparenz gegenüber staatlichen Stellen darf keinesfalls in pauschaler Überwachung münden. Nur wenn diese Balance transparent gewahrt bleibt, kann das Vertrauen der Bevölkerung in digitale Infrastrukturen gestärkt werden – und nur so kann die Schweiz ihre Rolle als führender Standort für vertrauenswürdige digitale Dienste ausbauen. Zudem kann eine vertrauenswürdige digitale Infrastruktur, die der EID zugrunde liegt, nur entstehen, wenn der Staat selbst vertrauenswürdig und kohärent handelt.

Wir fordern daher:

- Den Verzicht auf die unverhältnismässige Ausweitung der Überwachungspflichten, respektive gemäss den Anträgen der Digitalen Gesellschaft
- Die Entwicklung einer kohärenten Digital-Trust-Strategie der Schweiz, welche die Stärkung von PETs und kryptografischer Innovation begrüßt und fördert
- Kohärente Prinzipien zur digitalen Regulierung, die auf digitale Anforderungen an Handlungsfähigkeit, Autonomie, Rechtstaatlichkeit und der nachhaltigen Resilienz abgestimmt sind.
- Dass Zivilgesellschaftliche Akteure und Organisationen wie die Digitale Gesellschaft, CH++ und weiteren, Expertenorganisationen wie DIDAS aber auch Forschungseinrichtungen frühzeitig in die Ausgestaltung grundlegender Änderungen dieser resp. Solcher mit ähnlicher Tragweite partizipativ einbezogen werden.
- Ein unabhängiges Gremium könnte zudem sicherstellen, dass neue Gesetzes- oder Verordnungsentwürfe systematisch auf ihre Auswirkungen auf Grundrechte, digitale Souveränität und Innovationsklima sowie der Kohärenz mit der einer erarbeiteten Strategie hin geprüft werden.

Diese Position steht im Einklang mit unseren Grundprinzipien: dem Schutz der Privatsphäre durch Technikgestaltung (Privacy by Design), der Förderung digitaler Souveränität und digitaler Selbstbestimmung, einer innovationsfreudlichen und transparenten Regulierung sowie der Sicherstellung von Vertrauenswürdigkeit durch Rechtsstaatlichkeit und klarer Governance-Strukturen.

*Vernehmlassungsantwort zu den Teilrevisionen der VÜPF und der VD-ÜPF
gemäss Schreiben des EJPD vom 29. Januar 2025*

Datum	06.05.2025
Verfasser (Unternehmen)	MME Legal AG; basierend auf der Vernehmlassungsantwort von Prof. Dr. Simon Schlauri, dessen Ausführungen sich MME Legal AG zu 100% anschliesst.
Kontaktperson bei Fragen (Name/Tel./E-Mail)	Dr. Andeas Glarner, Ronald Kogens andreas.glarner@mme.ch Ronald.Kogens@mme.ch T +41 44 254 99 66

Dieses Dokument geht an:

Eidgenössisches Justiz- und Polizeidepartement EJPD, ptss-aemterkonsultationen@isc-ejpd.admin.ch

Sehr geehrter Herr Bundesrat Jans, sehr geehrte Damen und Herren

Wir beziehen uns auf das am 29. Januar 2025 eröffnete Vernehmlassungsverfahren zu Teilrevisionen von VÜPF und VD-ÜPF und bedanken uns für die Möglichkeit einer Stellungnahme.

Wir lehnen die geplante Teilrevisionen der VÜPF und der VD-ÜPF in aller Deutlichkeit und vollumfänglich ab.

Im Bericht des Bundesrates zur aktuellen Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF und der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) ist zu lesen, dass die Revision im Wesentlichen auf die Anpassung der Verordnungen an die KMU-Freundlichkeit abziele. Ein grosser Teil der vorgeschlagenen Änderungen *verfolgt aber gerade das Gegenteil*.

Die Geschäftsgrundlagen von Schweizer Unternehmen wie Threema, Proton und anderer KMU, die weltweit einen hervorragenden Ruf als Anbieterinnen sicherer Kommunikationsdienste im Internet geniessen, drohen durch die Vorlage zerstört zu werden. Die Sicherheit des Internets in der Schweiz soll mit der Revision der Überwachung jeglichen Internetverkehrs regelrecht untergeordnet werden: **«Sicherheit vor Freiheit» ist das neue Paradigma**. Dieses zieht sich wie ein roter Faden quer durch diese völlig verunglückte Reform. KMU, die aus der Schweiz heraus Internet-Dienste anbieten («abgeleitete Kommunikationsdienste» in der Terminologie des Gesetzes), soll die Schweiz als Standort geradezu vergällt werden. Dies scheint denn auch zu gelingen: **Erste der betroffenen Unternehmen haben bereits angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen** (siehe Tages-Anzeiger vom 1. April 2025).

Ein derartiger Paradigmenwechsel, weg von KMU-Schutz und Überwachung mit Augenmass, hin zu knallharter Überwachung, die alle anderen Interessen unterordnet, wird durch das geltende Gesetz (BÜPF) keineswegs gestützt. Der Paradigmenwechsel widerspricht vielmehr geradezu dem Geist des ursprünglichen BÜPF, das Internetdienste, die in der Schweiz meist von KMU betrieben werden, gerade von der Implementierung teurer Überwachungsmassnahmen schützen wollte, und das eine austarierte Interessenabwägung vorsah zwischen Privatsphäre und Freiheit auf der einen Seite und staatlicher Überwachung auf der anderen Seite.

Entgegen dem im Begleitbericht zum vorgelegten Entwurf erklärten Ziel, die «finanzielle Belastung der KMU gering zu halten», stuft die Vorlage eine grosse Mehrheit der Schweizer Anbieterinnen von Internetdiensten in eine höhere Stufe auf, und zwingt sie neu auch in jenen Bereichen zu einer kostspieligen aktiven Überwachungstätigkeit, wo bisher nur eine KMU-freundliche Duldungspflicht bestand. Dies verschiebt das bisherige Gleichgewicht der Interessen zwischen Strafverfolgung und betroffenen Anbieterinnen in drastischer Weise zugunsten der betroffenen Anbieterinnen.

Die vorgeschlagenen Anpassungen bringen ganz erhebliche Risiken für den Innovations- und Wirtschaftsstandort Schweiz mit sich und erfüllen die Kernziele der Revision, die Entlastung von KMU, gerade nicht. Der Ruf der Schweiz als sicherer Hafen für vertrauenswürdige IT-Anbieter droht durch die Revision nachhaltig beschädigt zu werden. Wir haben bereits Anfragen von internationalen Medien erhalten, warum die Schweiz von ihren Grundprinzipien, dem Schutz der Privatsphäre, abweicht. Deshalb lehnen wir die Revision vollumfänglich ab.

Auch **die Schweizer Armee** nutzt solche Dienste, wie beispielsweise Threema, und zwar gerade aufgrund des hohen gebotenen Sicherheitsstandards. Die Annahme dieser Revision, welche dieses Sicherheitsniveau gezielt untergraben will, verletzt damit indirekt auch das direkte Interesse der Schweiz an lokal betriebenen Hochsicherheitsanwendungen. Gerade in der heutigen Zeit, in der die Zuverlässigkeit der grossen US-Anbieter in ihrer Abhängigkeit von einer zunehmend erratisch agierenden US-Regierung mehr und mehr in Frage steht, erscheint dies als **inakzeptable Hochrisikostrategie**.

Nicht zuletzt ist mit Nachdruck darauf hinzuweisen, dass die Revision die Überwachung ganz allgemein stark ausweitet. Dies ist mit der durch den Gesetzgeber im BÜPF festgelegten, fein austarierten Interessenabwägung zwischen Freiheit und Privatsphäre der Einwohner der Schweiz einerseits und Sicherheit durch Überwachungsmassnahmen andererseits absolut nicht vereinbar. Die Revision entpuppt sich geradezu als eine Art Wunschkonzert für Überwachungsbehörden. Insbesondere ist künftig auch **eine komplette inhaltliche Überwachung des gesamten Internetverkehrs** der Schweiz vorgesehen. Dies ohne dass eine solche inhaltliche Überwachung durch die gesetzlichen Grundlagen des BÜPF in irgend einer Weise gedeckt wäre: Zulässig ist gemäss BÜPF einzig und allein die Überwachung von Randdaten des Fernmeldeverkehrs, und selbst die Zulässigkeit der in diesem Kontext angewendeten anlasslosen Vorratsdatenspeicherung von Randdaten ist bis heute umstritten und Gegenstand von Gerichtsverfahren, ja in der EU bereits höchstrichterlich als menschenrechtswidrig erkannt. Die durch die Verordnungsrevision eingeführte *Inhaltsüberwachung* ist in der Schweiz damit erst recht **offensichtlich illegal und verfassungswidrig**.

Abschliessend sei noch der Hinweis angebracht, dass wir die Gesetzgebungstechnik des Entwurfs für überaus schlecht halten. **Sowohl der Verordnungstext als auch der zugehörige erläuternde Bericht sind über weite Strecken höchst verwirrend und unverständlich formuliert**, unter anderem mit einer Vielzahl von Querverweisen, technischen Fehlern und unklarer Begrifflichkeit (für ein Beispiel hierfür siehe unten, Bemerkungen zu Art. 43a). Die Texte sind in dieser Form selbst für Fachleute über weite Strecken nicht zu verstehen, geschweige denn als Ganzes zu überblicken. Für KMU, die durch die Revision neu mit erheblich strenger Pflichten konfrontiert werden, ist eine rechtskonforme Umsetzung dieser Vorlage daher ein schlicht aussichtsloses Unterfangen.

Das Legalitätsprinzip gemäss Art. 5 Bundesverfassung fordert vom Gesetzgeber, dass Gesetzestexte für die Adressaten verständlich formuliert sind. Die Texte der Verordnungsrevision genügen dieser Anforderung offensichtlich in keiner Weise. Nur schon aufgrund der völlig fehlenden Verständlichkeit ist die Verfassungsmässigkeit der Revision insgesamt *höchst zweifelhaft*. Wir fordern nur schon deshalb einen Rückzug der vorgelegten Texte, eine komplette Überarbeitung zur Verbesserung der Verständlichkeit und eine erneute Auflage zur Vernehmlassung.

Freundliche Grüsse

Dr. Andreas Glarner, LL.M.

Ronald Kogens LL.M.

Bemerkungen zu einzelnen Artikeln der VÜPF

Nr.	Artikel	Antrag	Begründung / Bemerkung
VÜPF / OSCPT / OSCPT			
0.	Alle Artikel	Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.	<p>Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kunden auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.</p> <p>Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.dgl. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.</p>
1.	16b, Abs. 1	Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.»	Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile, wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Anforderungen in Kauf nehmen.
2.	16c, Abs. 3	Streichung von lit. a «automatisierte Erteilung der Auskünfte (Art. 18 Abs. 2);»	Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Dies untergräbt rechtsstaatliche Prinzipien doppelt: Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>dienen als «natürliche» Schutzmechanismen gegen eine überschiessende, missbräuchliche oder zumindest unverhältnismässige Nutzung solcher Massnahmen durch die Untersuchungsbehörden.</p> <p>Der vorgesehene Umsetzungszeitraum von 12 Monaten für die rechtssichere Implementierung eines derart komplexen Systems völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.</p>
3.	Art. 16d	<p>Streichung von Onlinespeicherdielen und VPN-Anbietern in der Auslegung</p>	<p>Eine klarere Definition des Begriffs AAKD ist begrüssenswert, doch die neue Auslegung gemäss erläuterndem Bericht geht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdielen wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter, etc.) genutzt werden.</p> <p>Art. 2 lit. c BüPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug den gesetzlichen Rahmen sprengt. Onlinespeicherdielen sind deshalb aus Art. 16d zu streichen.</p> <p>Zudem anerkennt der erläuternde Bericht, dass VPNs zur Anonymisierung der Nutzer*innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Anbieter von VPNs sind daher ebenfalls aus dem Geltungsbereich von Art. 16d auszunehmen.</p>
4.	Art. 16e, Art. 16f und Art. 16g	<p>Streichung der Artikel und Beibehaltung der bestehenden Kriterien</p> <p>Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).</p>	<p>Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch diametral entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung. Dies daher, weil neu KMU bereits mit mehr als 5'000 Nutzern erfasst werden.</p> <p>Die Einführung von 5000 Nutzern als gesondert zu beurteilende Untergrenze verletzt aus unserer Sicht bereits Art. 27 Abs. 3 BüPF, denn 5000 Personen keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strenger Überwachungsmassnahmen, gerechtfertigt wären. 5000 Nutzer werden in der digitalen Welt vielmehr sehr rasch erreicht.</p> <p>Zusätzlich führt das Einführen eines «Konzernatbestandes» in Art. 16f Abs. 3 zu massiven Problemen, da</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>die Produkte nun nicht mehr für sich alleine eine bestimmte Grösse erreichen müssen, sondern die relevanten Zahlen anhand des Umsatzes des Unternehmens, bzw. in Konzernverhältnissen sogar des Konzerns bestimmt werden. Vor allem bei Unternehmen mit Beteiligungsfirmen im Hintergrund fallen nun neu alle Dienstleistungen und Produkte automatisch unter die härteste Stufe, egal ob sie sich erst in einem frühen Entwicklungsstadium befinden. Dies behindert Innovation, da jedes Projekt bereits mit volumfanglichen Überwachungspflichten geplant und eingeführt werden müsste. Durch diese extreme Einstiegshürde wird der Innovationsstandort Schweiz nachhaltig geschädigt.</p> <p>Gleichzeitig wird auch der Wirkungsbereich der VÜPF stark erweitert. Während heute ein Unternehmen einen grossen Teil seiner Geschäftstätigkeit durch abgeleitete Kommunikationsdienste erbringen muss (Art. 22 Abs. 1 lit. b und Art. 52 Abs. 1 lit. b VÜPF), fällt dieses Kriterium neu weg. Dadurch können künftig auch Unternehmen, deren Geschäftstätigkeit nur am Rande auf abgeleiteten Kommunikationsdiensten basiert, wie Onlineshops, Marktplätze, Auktionsplattformen, Zeitungen, Computerspielhersteller und zahlreiche weitere Unternehmen, unter die VÜPF fallen – allein deshalb, weil ihre Produkte irgendeine Form privater Kommunikation zwischen Nutzer*innen und/oder Drittanbietern ermöglichen.</p> <p>Die vorgeschlagene Regelung stünde sodann im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali, das die zu weite Betroffenheit und die seltene Anwendung von Downgrades kritisierte: «Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»</p> <p>Statt KMU zu entlasten, führt die Revision neu sogar zu einer «automatischen Hochstufung per Verordnung ohne konkretisierende Verfügung (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.</p> <p>Die neue Regelung steht zudem in offensichtlichem Widerspruch zur bisherigen Praxis, denn bis heute wurde gemäss Angaben des Dienst-ÜPF keine einzige AAKD hochgestuft. Auch der Bundesrat stützte sich ausdrücklich auf die geltende Kombination von drei Schranken – einem Unternehmensfokus auf Kommunikationsdienste, einer Umsatzgrenze von 100 Millionen Franken sowie einer grossen Nutzerzahl – als er noch 2023 begründete, die Umsetzung des BÜPF sei gerade wegen der genannten Schranken als KMU-freundlich zu verstehen. Die vorliegende Revision hebt jedoch genau diese Kombination kumulativer Kriterien auf und will die einzelnen Kriterien künftig alternativ anwenden bzw. streicht sie sogar vollständig. Dadurch verlieren die bisherigen Schutzmechanismen ihre Wirkung, und das BÜPF soll neu auf viele KMU Anwendung finden, die früher nicht unter Gesetz und Verordnung fielen.</p> <p>Die Analyse der offiziellen Statistik des Dienstes ÜPF macht die offensichtliche Unverhältnismässigkeit</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>dieses Ansinnens deutlich. Im Jahr 2023 betrafen 98,95 % der total 9'430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,05 % für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,73 % wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100 % des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.</p> <p>Wesentlich ist insbesondere eine neue Pflicht zur Identifikation der Nutzer: Hiervon betroffen sind nicht nur alle AAKD mit reduzierten oder vollen Pflichten (und damit de facto fast alle AAKD der Schweiz), sondern auch all deren Wiederverkäufer. Im Ergebnis führt die neue Verordnung aus unserer Sicht dazu, dass man sich bei keinem marktrelevanten Dienst mehr anmelden kann, ohne den Pass, Führerschein oder ID zu hinterlegen oder zumindest Daten wie eine Telefonnummer anzugeben, die man ohne Pass oder ID nicht erhalten kann.</p> <p>Die automatische Hochstufung an sich führt bereits zu erheblicher Rechtsunsicherheit bei den betroffenen Unternehmen. Unter dem bestehenden System werden die generell-abstrakten Normen der VÜPF mittels Verfügung auf einen konkreten Einzelfall angewendet. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes ist aber im Zweifelsfall möglicherweise nur schwer zu beantworten. Zweifelsohne besteht hier ein schutzwürdiges Interesse seitens der AAKD daran, zu wissen, ob sie die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Nur das bisherige System entspricht den allgemeinen Grundsätzen des Verwaltungsverfahrens, welches für die Anwendung einer generell-abstrakten Norm eine Konkretisierung durch die Verwaltung voraussetzt. Von einer automatischen Hochstufung von AAKD ist daher aus Gründen der Rechtssicherheit abzusehen. Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.</p> <p>Gegenüber der alten VÜPF erweitert die Revision die Pflichten zur Automatisierung sodann noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragen wie z.B. IR_59 und IR_60, welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen. Genau diese Möglichkeit einer manuellen Intervention ist aber für die Provider kritisch, um Missbräuche zu verhindern, die wiederum die Verträge mit ihren Kunden und das Fernmeldegeheimnis verletzen könnten. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente damit erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>ersatzlos gestrichen werden.</p> <p>Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 Bst. b der alten VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grossen[n] Teil ihrer Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. Damit fallen insbesondere bereits Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz. Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Dies setzt der Innovation in der Schweiz neue riesige Hürden entgegen.</p> <p>Auch Non-Profit-Organisationen wie die Signal Foundation, die kaum Umsätze erwirtschaften, geraten unter diese verschärften Vorgaben. Während sie bisher unter Duldungspflichten verbleiben konnten, solange sie Art. 22 Abs. 1 VÜPF nicht erfüllten, wird neu allein auf die Anzahl der Nutzer*innen abgestellt, womit z.B. Signal neu als AAKD mit vollen Pflichten erfasst würde. Dies würde dazu führen, dass Signal in der Schweiz entweder zu einem Rückzug aus dem Markt gezwungen wird oder erhebliche rechtliche Konsequenzen riskiert, da Signal keine IP-Adressen speichert und somit gegen Art. 19 RevVÜPF verstößt.</p> <p>Die Regelung ignoriert zudem wirtschaftliche Realitäten: Ein hoher Nutzerkreis bedeutet bei Non-Profits keine finanzielle Tragfähigkeit für umfangreiche Überwachungsmassnahmen. Damit werden Open-Source- und Non-Profit-Lösungen gezielt aus dem Markt gedrängt, während bestehende Monopole wie WhatsApp (96 % Marktanteil in der Schweiz) gestärkt werden. Die neue Regelung ist daher aus ökonomischer Sicht zu verwerfen. Das Kriterium der reinen Nutzerzahl ist ungeeignet und muss gestrichen werden.</p> <p>Nicht zuletzt schwächt die Regelung auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger*innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, Ende-zu-Ende-verschlüsselter Kommunikation ist heute wichtiger denn je.</p> <p>Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade als rechtswidrig gilt (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer*innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, sondern allein diese</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Anhäufung an Daten malt eine Zielscheibe auf den Rücken von Schweizer Unternehmen und Dienstleistungen für Hackerangriffe aus der ganzen Welt.</p> <p>Weiters ist zu erwähnen, dass es gar nicht erwiesen ist, dass die Speicherung der fraglichen Daten eine merklich höhere Quote erfolgreicher Ermittlungen durch die Strafverfolgungsbehörden mit sich bringen würde. Im Gegenteil müssen die bereits existierenden Sekundärdaten, die allein durch die Bereitstellung eines Dienstes für den Nutzer entstehen, besser genutzt werden. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisshandlung via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfügt, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden. Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren.</p> <p>Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Souveränität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.</p> <p>Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das Datenschutzgesetz. Der Entwurf bringt nicht, wie der Begleitbericht dem Leser in geradezu in Orwell'scher Manier weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit und steht in direktem Gegensatz zum besagten Postulat 19.4031.</p> <p>Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen, und das bestehende System muss beibehalten werden.</p>
5.	Art. 16h Abs. 2	Streichung der Ausführung im erläuternden Bericht und	Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Nutzer*innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die

Nr.	Artikel	Antrag	Begründung / Bemerkung
		ein Abstellen der Formulierung auf die gleichzeitige Anzahl Nutzer.	<p>praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 Rev. VÜPF, gemäss dem die das WLAN erschliessenden FDA die Verantwortung für die Identifikation der Nutzer der WLANs tragen.</p> <p>Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer*innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24) oder die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22). Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDAs unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden. Unter der bestehenden Regelung konnte eine FDA anhand der Lokation (z.B. Bibliothek, Flughafen) eine Einschätzung treffen. Die neue Definition hingegen würde von ihr verlangen, Zugriff auf jedes private Netzwerk zu erhalten, um Hardware und Einstellungen zu prüfen – ein offensichtlich verfassungswidriges und auch praktisch unmögliches Unterfangen. Diese vage Formulierung führt zu anhaltender Rechtsunsicherheit für FDA.</p> <p>Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten.</p> <p>Zudem könnte Art. 16h dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist*innen, Whistleblower*innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer*innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen. Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt.</p>
	Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2	Streichung des «Konzerntatbestand» und Beibehaltung der bestehenden Regelung	Die Verordnung nimmt neu nicht mehr die Umsatz- und Nutzerzahlen der betroffenen Unternehmen, sondern die Zahlen des jeweiligen Konzerns als Basis für Up- und Downgrades. Die Begründung zur Einführung dieses «Konzerntatbestands», wonach die neue Regelung für die betroffenen Unternehmen zu einer Vereinfachung führe, ist kontraintuitiv, ja offensichtlich falsch und irreführend. In der Praxis sind die betroffenen Unternehmen nämlich schon heute verpflichtet, ihre Buchhaltung nach Produkten aufzugliedern. Somit können die Kennzahlen bereits heute sehr einfach festgestellt werden. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.
6.	Art. 19 Abs. 1	Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller	Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht.

Nr.	Artikel	Antrag	Begründung / Bemerkung
		erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation von Teilnehmenden.	<p>Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des Schweizer Datenschutzgesetzes, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch der Schutz der Schweizer Kundschaft massiv beeinträchtigt wird. Datenschutzfreundliche Unternehmen werden bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.</p> <p>Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Dies wahrt nicht nur den Datenschutz, sondern schützt auch die Wettbewerbsfähigkeit von KMU, stärkt den Innovationsstandort Schweiz und die digitale Souveränität unseres Landes.</p>
7.	Art. 18	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.
8.	Art. 19 Abs. 2	Ersatzlose Streichung zugunsten bestehender Regelung	Eine Überwachung von Kunden durch FDA, ob diese die neuen Vorgaben der VÜPF zu WLANs einhalten (Art. 19 Abs. 2 Rev.VÜPF), und erst recht die dazu gelieferte Erklärung im erläuternden Bericht, wonach die FDA die Identifikation der WLAN-Nutzer vorzunehmen hätten, ist weder gesetzeskonform noch zumutbar (siehe vorstehend). Art. 19 Abs. 2 ist ersatzlos zu streichen.
9.	Art. 21 Abs. 1 lit. a	Streichung	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.
10.	Art. 22	beibehalten	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.
11.	Art. 11 Abs. 4	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.
12.	Art. 16b	Streichung	Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.
13.	Art. 31 Abs. 1	Streichung Teil «Anbieter mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.
14.	Art. 51 und 52	beibehalten	Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.
15.	Art. 60a	Streichung des Artikels	<p>Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen.</p> <p>Art. 60a VÜPF (Erläuterung Bundesrat: «...lediglich redaktionelle Änderungen....») sieht vor, dass Fernmeldedienstanbieterinnen über einen rückwirkenden Zeitraum von 6 Monaten alle Ziel-IP-Adressen liefern müssen, welche ihre Kunden besucht haben. Damit wird einerseits das Surfverhalten der gesamten schweizerischen Bevölkerung anlasslos und völlig unverhältnismässig ausspioniert. Andererseits wird die klare Vorgabe des BÜPF umgangen, das nur die Speicherung von Randdaten, aber nicht die Speicherung</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>von Inhaltsdaten vorsieht.</p> <p>Die geplante Überwachung des Internetverkehrs führt zu einer Überwachung, wer im Internet welche Adressen besucht hat. Dies geht zweifellos über die Schranken der gesetzlichen Regelung hinaus, dies insbesondere nachdem bereits die Aufzeichnung reiner Randdaten höchst umstritten und Gegenstand laufender Gerichtsverfahren ist. Hinzu kommt folgendes: Während bislang die Überwachung einer IP-Adresse nur im Rahmen einer sog. Echtzeit-Überwachung zulässig war, welche entsprechende Bewilligungen durch ein Gericht erforderte, muss neu nur noch ein einfaches Auskunftsbegehren durch die zuständige Behörde genehmigt werden. Die Abfragen erfolgen automatisiert.</p> <p>Art. 60a sieht weiter vor, dass bei nicht exakt zuordenbaren IP-Adressen die kompletten Listen aller Nutzerinnen und Nutzer zu liefern ist. IP-Adressen sind ein rares Gut. Alle FDA teilen diese den Nutzenden im Millisekunden-Takt zu. Da die Zeitstempel der Systemanbieter nicht immer übereinstimmen, sind diese IP-Adressen nicht immer eindeutig einem Nutzenden zuzuordnen. Neu müssen Provider nun komplettene Listen aller Nutzenden liefern. Dies bringt Zehntausende in den Fokus von Überwachungsbehörden, was auf eine Art Rasterfahndung nach Delikten über grosse Teile der Bevölkerung hinausläuft. Entdecken Strafverfolger dabei zufälligerweise etwas, können sie umgehend Strafverfahren einleiten.</p> <p>Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde sodann gemäss Bericht gezielt auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten.</p> <p>Art. 60a ist zu streichen.</p>
16.	Art. 42a und Art. 43a	Streichung des Artikels	<p>Sowohl Art. 42a als auch Art. 43a fordern die Abrufbarkeit des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Nicht nur gilt auch hier wieder die Limite von 5'000 Nutzern, was somit fast die gesamte AAKD-Landschaft der Schweiz flächendeckend umfasst, sondern solche Abfragen sollen nun auch durch eine einfach «IR_» Abfrage gemacht werden können, welche im Gegensatz zu den «HD_»-Abfragen und den «RT_»-Überwachungen ohne weitere juristische Aufsicht automatisiert abgerufen werden können, obwohl es sich auch hier um das Abrufen einer IP-Adresse in der Vergangenheit handelt, genau wie bei den «HD_» abfragen, welche deutlich strenger reglementiert sind. Es ist nicht nachvollziehbar und verletzt aus unserer Sicht die gesetzliche Grundlage des BÜPF, dass Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber.</p> <p>Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser Automatisierten Auskünfte ergibt. Durch das Fehlen solcher Limiten könnte daher z.B. alle 5 Minuten eine</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>solche Anfrage automatisiert gestellt werden. Zunächst können sich dadurch lähmende Kosten für die betroffenen AAKD ergeben. Sodann können die Anfragen an ein automatisiertes Auskunftssystem gestellt werden, und es können auf diese Weise viele der Informationen welche ursprünglich über die juristisch sichereren HD_ und RT_Auskunfts-/Überwachungstypen liegen, neu über den rechtlich unsicheren IR-Typ eingeholt werden. IR_59 und IR_60 ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne dass sie den benötigten Kontrollen dieser invasiven Überwachungsarten unterliegen würden.</p> <p>Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind, wie dies das BÜPF vorsieht.</p> <p>Die beiden Artikel sind daher vollumfänglich zu streichen.</p> <p>Diese neue Regelung und der zugehörige erläuternde Bericht sind im Übrigen eklatante Beispiele für die eingangs bemängelte überaus verwirrende und unverständliche Darstellung von Verordnungstext und erläuterndem Bericht.</p> <p>Im erläuternden Bericht steht auf S. 39 wörtlich:</p> <p><i>«In Absatz 1 sind die zu liefernden Angaben geregelt. Gemäss Buchstabe a ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin der oder dem Teilnehmenden einen solchen zugeteilt hat. Der «eindeutige Dienstidentifikator» gemäss Buchstabe b bezeichnet den Fernmelde- oder abgeleiteten Kommunikationsdienst, auf den sich die Antwort bezieht, eindeutig im Bereich der Anbieterin. In Buchstabe c werden die zu liefernden Angaben über den Ursprung der Verbindung bei der letzten zugriffsrelevanten Aktivität aufgezählt. Diese Angaben können für die Identifikation der Benutzerinnen und Benutzer nützlich sein.»</i></p> <p>Der Leser bzw. die Leserin urteile selber über die Verständlichkeit.</p> <p>Folgende Begriffe sind auch für den fachkundigen Leser nicht nachvollziehbar, bzw. es stellen sich folgende Verständnisfragen:</p> <ul style="list-style-type: none"> - Eindeutiger Identifikator: Was ist gemeint? Ist die Kundennummer des Internetproviders gemeint? Oder jene des genutzten dritten Fernmeldedienstes oder abgeleiteten Kommunikationsdienstes? Wie soll der Internetprovider überhaupt an diese Daten herankommen? - Eindeutiger Dienstidentifikator: Muss der Internetprovider eine Liste aller möglichen durch seine Kunden im Internet genutzten Kommunikationsdienste führen und aufzeichnen, muss er zudem aufzeichnen welcher Kunde welchen Dienst wann genau genutzt hat? Woher hat er diese Liste?

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Wie kann er herausfinden, ob ein Kunde gerade einen bestimmten Dienst nutzt? Gilt dies auch für ausländische Dienste? Nur für AAKD, für ausländische Fernmeldedienste, oder für alle Internetangebote weltweit? Der erläuternde Bericht bleibt hier völlig unklar.</p> <ul style="list-style-type: none"> - Was ist mit «Antwort» gemeint? Die Antwort des Servers des abgeleiteten Kommunikationsdienstes, den der Kunde besucht hat, oder die Antwort des Kundengeräts auf eine Nachricht von diesem Kommunikationsdienst? - Was ist mit «eindeutig im Bereich der Anbieterin» gemeint? Die Formulierung ist auch hier unverständlich. - Wie soll man sich eine «Antwort von einem anderen Fernmeldedienst» vorstellen? Muss ein Internetprovider die Herkunft sämtlicher auf seinem Netz eintreffenden Datenpakete aufzeichnen und dem Dienst ÜPF auf Anfrage diese Aufzeichnungen herausgeben? Wie soll die gigantische Masse an Daten, die durch ein solches Logging anfällt, durch die Internetprovider gemanaged werden? - Was ist mit «letzter zugriffsrelevanter Aktivitäten» gemeint? Geht es hier um die durch Kunden des Internetproviders aufgerufenen AAKD und andere Internetangebote? Wie soll der Internetprovider wissen, ob eine durch den Kunden aufgerufene IP-Adresse zu einem überwachungspflichtigen AAKD gehört, oder allenfalls zu einem nicht überwachungspflichtigen Dienst? Muss er einfach den ganzen Verkehr aufzeichnen? Wie weit zurück gehen die «zugriffsrelevanten» Aktivitäten? Müssen alle Daten für sechs Monate aufbewahrt werden? - Abgesehen davon: Wo wäre die gesetzliche Grundlage im BüPF für die vorgesehene inhaltliche Überwachung des Internetverkehrs? Das BüPF selber regelt bisher ausschliesslich die Überwachung der Randdaten, nicht aber von Inhaltsdaten, und spätestens dann, wenn Randdaten en passant auch Auskunft über die vom Kunden abgerufenen Inhalte geben, handelt es sich dabei um Inhaltsdaten, deren Sammlung erst recht gesetzes- und verfassungswidrig wäre, nachdem schon das Sammeln reiner Randdaten als menschenrechtswidrig taxiert wurde.
17.	50a	Artikel streichen	<p>Art. 50a sieht neu vor, dass Anbieter verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Diese Pflicht gilt nicht mehr nur für FDA (Art. 26 BüPF) oder ausnahmsweise für ausgewählte AAKD von hoher wirtschaftlicher Bedeutung (Art. 27 BüPF), sondern soll nun vorgabemässig und ohne Differenzierung auf sämtliche Anbieter mit mehr als 5'000 Teilnehmern angewendet werden, womit wohl fast die gesamte Schweizer AAKD-Branche betroffen ist (kaum ein Produkt ist lebensfähig mit weniger als 5000 Teilnehmern).</p> <p>Dies stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar.</p> <p>Diese Ausweitung ist nicht nur unverhältnismässig, sondern gefährdet aktiv nahezu die gesamte Schweizer IT-Branche: Indem de facto alle Anbieter vorgabemässig gezwungen werden, ihre</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			<p>Verschlüsselungssysteme für Behörden jederzeit entschlüsselbar zu gestalten, entstehen enorme Sicherheitsrisiken, denn Verschlüsselung ist wie eine Eierschale: Unversehrt ist sie stark, aber der kleinste Riss führt zu einer erheblichen Schwächung. Die betroffenen Systeme werden durch den vom Verordnungsgeber nun verpflichtend vorgesehenen Einbau von Hintertüren anfällig für Hackerangriffe, Datenmissbrauch und Spionage. Dies widerspricht Art. 13 BV und dem diesen konkretisierenden Datenschutzgesetz, das den Schutz personenbezogener Daten ausdrücklich durch wirksame technische Massnahmen – insbesondere Verschlüsselung – vorschreibt. Eine durch den Anbieter aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung in jedem Fall.</p> <p>Genau eine solche Schwächung der Verschlüsselung wurde kürzlich vom Europäischen Gerichtshof für Menschenrechte im Fall PODCHASOV gegen Russland (33696/19) als Verstoss gegen Grundrechte gewertet. Art. 50a verstösst somit auch gegen geltendes Völkerrecht.</p> <p>Nebst diesem Verstoss gegen das Völkerrecht wird aber auch das Gebot der Verhältnismässigkeit aus Art. 36 BV nicht eingehalten, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördararbeit steht. Wie bereits bei Art. 16e, Art. 16f und Art. 16g erwähnt, müssen zuerst die einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.</p> <p>Zusätzlich, und wie bereits bei Art. 16d erwähnt, verhindert Art. 50a die effektive Erbringung von VPN-Diensten. Bei solch einem VPN kontrolliert der Betreiber sowohl den Eingangs- als auch den Endpunkt. Da die Kommunikation vom Endpunkt zu einer Webseite aufgrund der vorherrschenden Struktur im allgemeinen Internet nicht End-zu-End-Verschlüsselt erfolgen kann, werden schon kleine VPNs (mit 5000 Nutzern) dazu gezwungen ihre eigene Verschlüsselung zu entfernen und ihre Kunden zu überwachen. Da der Schutz der Privatsphäre der Nutzer*innen von VPNs just den Kernpunkt oder USP der Dienstleistung darstellt, werden Schweizer VPN-Anbieterinnen hierdurch am internationalen Markt übermässig benachteiligt, ja ihres eigentlichen Daseinszwecks beraubt.</p> <p>Wesentlich ist zudem, dass Anbieter von Mail- oder Messaging-Apps zwangsläufig die Nachricht in der App in einer menschenlesbaren Version anzeigen muss, und dass an dieser Stelle die End-zu-End-Verschlüsselung notwendigerweise bereits entfernt ist. Der Wortlaut von Art. 50a lässt entgegen sämtlichen Beteuerungen des Dienstes ÜPF bereits anlässlich der letzten Revision der VÜPF weiterhin</p>

Nr.	Artikel	Antrag	Begründung / Bemerkung
			offen, ob eine Entfernung der Verschlüsselung auch an dieser Stelle gefordert werden können soll. Angesichts der seit Jahren erkennbaren Tendenz der Schweizer Überwachungsbehörden, die Anwendbarkeit des Überwachungsrechts laufend weiter auszudehnen und sich dabei nur durch Gerichte bremsen zu lassen, ist bei dieser Gelegenheit erneut die Klarstellung zu fordern, wonach die Entfernung von Verschlüsselungen, die erst in der Sphäre des Benutzers angebracht werden (wenngleich auch durch Software der Anbieterin) nicht verlangt werden darf. Dies ist zumindest im erläuternden Bericht zu erwähnen. Der erneute Verzicht wäre nichts anderes als eine Einladung an die Überwachungsbehörden, die Einführung einer offensichtlich illegalen und vom BÜPF keineswegs vorgesehenen «Chatkontrolle» auf dem «Auslegungsweg» vorzunehmen.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Artikel	Antrag	Begründung / Bemerkung
VD-ÜPF / OME-SCPT / OE-SCPT		
Art. 14 Abs. 3 VD-ÜPF	Streichung	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit 5000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Absatz ist daher ersatzlos zu streichen.
Art. 14 Abs. 4 VD-ÜPF	Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten.	Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der Unterworfenen AAKD massiv. Dies ist wie beschrieben weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.
Art. 20 Abs. 1 VD-ÜPF	Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»	Wie bereits bei Art. 16e bis 16f Rev.VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer*innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.



Lausanne, le 6 mai 2025

Jean-Louis Biberstein
(responsable suppléant Service SCPT,
responsable Droit et contrôle de gestion)
Service Surveillance de la correspondance par
poste et télécommunication
+41 58 462 26 27
jean-louis.biberstein@isc-ejpd.admin.ch

Madame, Monsieur,

Cette lettre a pour objectif d'exprimer notre inquiétude par rapport aux propositions de révision des ordonnances de surveillance OSCPT et OME-SCPT.

AKENES SA qui opère sous la marque Exoscale est un fournisseur d'infrastructure cloud dont le siège est situé à Lausanne. Elle fournit des ressources de calcul, de réseau et de stockage via huit zones réparties en Suisse, en Autriche, en Allemagne, en Croatie et en Bulgarie. Ses valeurs fondamentales sont centrées sur la simplicité, la souveraineté et la durabilité.

Les propositions énoncées auraient pour impact

- un coût non supportable actuellement dans la structure de marge actuelle, spécifiquement des produits d'hébergement de fichiers en nuage, pour mettre en place le stockage des métadonnées ainsi que leur accès et leur rétention sur une période étendue.
- réduction de l'attractivité des fournisseurs suisses en matière de protection de données, qui concentrerait notre marché potentiel actuellement Européen à la seule place de marché Suisse, trop restreint pour des services d'infrastructure ciblant les économies d'échelle.

Ainsi nous nous joignons à un mouvement de l'industrie numérique et de nombreuses start-up et scale-up suisses qui réclament des modifications substantielles dans la mise en place des ces ordonnances.

Cordialement,

Antoine Coetsier - co-fondateur et COO

Réf: AB

T direct: +41 26 305 51 00

Courriel: andreas.behr@fr.ch

À l'attention de
Messieurs les Conseillers fédéraux
Guy Parmelin, Vice-président du Conseil fédéral,
Beat Jans, Chef du DFJP

PAR COURRIER ELECTRONIQUE

info@gs-ejpd.admin.ch

info@gs-wbf.admin.ch

Fribourg, le 2 juin 2025

Révision partielle de deux ordonnances d'exécution de la surveillance de la correspondance par poste et télécommunication (OSCPT et OME-SCPT) - Enjeux pour la place économique suisse

Monsieur le Vice-président du Conseil fédéral,
Monsieur le Conseiller fédéral,

En notre qualité de Conseillers-ères d'État chargés-es de l'économie de Suisse occidentale, nous souhaitons attirer votre attention sur les effets préoccupants que pourrait produire la révision envisagée des ordonnances d'application de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT et OME-SCPT). Cette révision, si elle devait être conduite dans sa forme actuelle, risquerait d'affaiblir un pilier stratégique de l'économie suisse : celui de la confiance numérique.

Depuis plus d'une décennie, notre pays s'est imposé comme une référence internationale en matière de technologies de confidentialité, attirant des entreprises innovantes, suisses et étrangères, qui ont fait de la Suisse un espace de sécurité juridique, de stabilité politique et de respect de la vie privée. Il en résulte un écosystème en pleine croissance, compétitif et diversifié, composé d'acteurs actifs dans la cybersécurité, le chiffrement, la protection des données et les services de communication sécurisés.

Certaines de ces entreprises ont adopté une architecture technique reposant sur le chiffrement de bout en bout. Ce modèle garantit que seuls les utilisateurs légitimes peuvent accéder au contenu des communications — sans que les prestataires eux-mêmes n'y aient accès. Ce choix technologique, qui constitue à la fois un engagement éthique et un avantage concurrentiel, est essentiel à la protection des personnes ou organisations particulièrement exposées : journalistes, avocats, professionnels de santé, ONG ou lanceurs d'alerte.

Plusieurs entreprises emblématiques illustrent cette approche. À Genève, la société Proton AG, issue du CERN, s'est imposée comme un leader mondial de ce type de services. À Schwytz, Threema GmbH développe une messagerie sécurisée employée au quotidien

dans l'administration publique. À Zurich, Tresorit propose des solutions de stockage chiffré, largement utilisées par les milieux médicaux et juridiques. À Neuchâtel, Nym Technologies SA œuvre dans les réseaux anonymisés. Et tout récemment, la messagerie Session, développée en Australie, a choisi de relocaliser ses activités en Suisse, précisément pour bénéficier de son cadre juridique exigeant, mais protecteur.

Les obligations prévues par le projet de révision — automatisation des réponses, fourniture de contenus, extension des métadonnées — rendraient incompatible avec le cadre légal envisagé le modèle fondé sur le chiffrement de bout en bout. Ce dernier serait, sans être formellement interdit, rendu structurellement inapplicable. Ce qui est en jeu, ce n'est donc pas seulement la conformité à de nouveaux standards techniques, mais l'existence même de ces services — et avec eux, la crédibilité de la Suisse comme place technologique de confiance. Les conséquences seraient majeures : départ d'entreprises, fragilisation d'un secteur clé, perte de confiance des usagers, et affaiblissement de la position suisse dans une compétition mondiale de plus en plus rude autour des standards de la confiance numérique et en particulier de la cybersécurité.

Il convient enfin de veiller à ce que les obligations imposées par la révision soient proportionnées à la réalité économique des entreprises concernées, notamment les plus petites structures. Si les grands opérateurs sont majoritairement sollicités dans les procédures de surveillance, nombre de PME pourraient être affectées par des exigences techniques ou financières disproportionnées. Or, les investissements nécessaires risquent d'entamer leur capacité d'innovation, voire leur viabilité, sans bénéfice tangible en matière de sécurité publique.

À cet égard, nous invitons le Conseil fédéral à évaluer en profondeur l'impact économique concret de la révision, en amont de toute décision, et à engager un dialogue structuré avec les acteurs concernés. Il ne saurait s'agir d'une simple consultation formelle, mais d'un échange ouvert, techniquement informé et susceptible d'adapter le dispositif projeté aux réalités du terrain. Il en va de l'attractivité durable de la Suisse en tant que place technologique de confiance.

Persuadés de votre attachement à un équilibre mesuré entre sécurité et liberté économique, nous vous prions de croire, Monsieur le Vice-président du Conseil fédéral, Monsieur le Conseiller fédéral, à l'assurance de notre haute considération.



Olivier Curty
Président CDEP-SO



Andreas Behr
Secrétaire général

Copie

-
- > Jean-Louis Biberstein, Service Surveillance de la correspondance par poste et télécommunication
(par courrier électronique : jean-louis.biberstein@isc-ejpd.admin.ch)
 - > Adresse pour les réponses à la consultation (ptss-aemterkonsultationen@isc-ejpd.admin.ch)



Consultation response: Partial Revision of LSCPT

Date: 6 May, 2025



Twilio's Response to the Consultation on the Partial Revision of LSCPT

Twilio appreciates the opportunity to provide comments on the Swiss government's proposal for a partial revision of the Act on the Surveillance of Postal and Telecommunications Correspondence ("[LSCPT](#)") and its implementing orders, collectively referred to in this note as the "**Ordinances**":

- [Ordinance on the Surveillance of Postal and Telecommunications Traffic \("OSCPT"\)](#); and
- [Ordinance on the Implementation of Surveillance of Postal and Telecommunications Traffic \("OME-SCPT"\)](#),

As a Business-to-Business (B2B) cloud communications company, Twilio empowers customer engagement communications for businesses, governments, and nonprofits of all sizes across Europe. Twilio transforms legacy communication systems into cloud-based software, making telecom services more modern, efficient, and scalable.

Twilio provides the following comments on certain aspects of the proposed revisions:

Scope: risks around the classification of services

Concerns for Disproportionate Obligations on B2B Derived Communication Services

The proposed revisions to the Act contain two criteria for subjecting a service to more stringent obligations, one of which is based on the number of *users* of the service. Twilio has some concern about how the average number of users of a service might be counted under this rule.

Twilio, like other B2B service providers, has a relatively small number of business customers, each of which uses Twilio's communications platform to send messages to a large number of individual recipients, who are not Twilio customers and have no other relationship to it. Twilio provides no services to those recipients directly, and may be subject to disproportionate obligations if individual message recipients are counted as its users.

Without a clear definition of end user, B2B services like Twilio may inadvertently be captured by disproportionate obligations which are not appropriate given their position in the value chain and the intent of the revision. The lack of a clear definition for B2B services may put Twilio's average number of users at risk of being overcounted. This is because both the services provided to Twilio's customers and the services used by the end users—who have no direct relationship with Twilio—could be counted. To mitigate this risk and ensure that proportionality is maintained while still enabling the policy objectives to be achieved, only direct business customers should be considered as end users for B2B companies. Additionally, in Business-to-Consumer (B2C) relations, only consumers should be considered as end users.



A Clear Procedure for Service Classification

Twilio urges the Swiss government to clarify the classification procedure of a service. This would enable service providers to have better legal certainty, and preparedness in compliance processes.

Additionally, it remains unclear who is responsible for such a classification. This lack of clarity also raises a risk of misclassification, creating legal uncertainty for cloud-based communication service providers, like Twilio, and other providers whose services may fall into multiple categories. An updated and clear process for classifying services, including a timely and transparent appeals process for providers, is needed if this proposal were to be implemented.

The variety of services and complexity of the value chain for communication products is constantly changing. Twilio's services often rely on telecommunications service providers (TSPs) for the transmission and underlying network capabilities, and these service components are provided to our customers who are also contracting with an internet service provider for access. Twilio services largely include:

- Applications or programs for the transmission of data, between users and which are not provided with network access;
- Electronic messaging capabilities for third parties; and
- Online storage services.

Twilio's services do not include traditional telecommunication network facilities historically considered to be TSPs, and as such, we rely on our upstream partners for technical compliance with the regulatory requirements that concern their infrastructure. In the case of this proposal, all hosting services are best and more consistently classified under the FSCD category. We understand it is not the intent or goal of the revision of the Ordinances to bring undue obligations to B2B providers without network facilities and infrastructure such as Twilio. Applying the obligations as drafted would be difficult (depending on third parties) or sometimes even technically impossible to comply with, making them disproportionate and inappropriate in our view.

Consistency between Swiss and EU jurisdictions

Like Twilio, many Swiss companies also offer services in the EU market, subject to EU rules around personal data, lawful access to data for law enforcement authorities, and content moderation. Consistency between Swiss and EU laws is therefore of prime importance to ensure legal certainty and foster scalability for cross-border service providers, while respecting the local specificities of each jurisdiction. In this context, Twilio would call for consistency on the following aspects:

Encryption



Twilio welcomes the clarification made in the explanatory note, where the new Article 50a on removing encryption only applies to providers with restricted or full obligations who have the encryption key, and excludes end-to-end encryption on the client side. However, the procedure leading to the issuance of an order to decrypt the data is not explicitly mentioned in the revision, which raises legal and procedural questions.

Twilio strongly urges the Swiss government to uphold the right to encryption, especially in direct messaging applications where law enforcement authorities' access to encrypted data can only be considered as a last resort in a targeted and limited manner, subject to rigorous judicial review, without contravening human rights.

Monitoring

In force since 2022, the EU's Digital Services Act (DSA) bans general monitoring practices for information, facts or circumstances indicating illegal activity (Article 8). It is therefore important that the extended monitoring obligations applicable to relevant providers, in particular Article 50 on surveillance duties under the proposed revision, do not give rise to potential inconsistencies with the prohibition under the DSA.

Policy recommendations

- Address definitions of users and what requirements and obligations should be placed on B2B services. This should be undertaken with due consideration of service providers' positions in the value chain, and importantly, whether the service providers have network facilities/infrastructure of their own. This may require a reconsideration of the current classification of TSP services to ensure they better align with traditional network facilities and infrastructure.
- Clarify the classification procedure of each communication service, and a clear appeals process for any decision to ensure legal certainty for the provider.
- Continue to strive for consistency between Swiss and EU law on encryption and monitoring in communication services.
- Extension of the time for implementation, with at least a year from the date of enactment.



Schweizerischer Anwaltsverband
Fédération Suisse des Avocats
Federazione Svizzera degli Avvocati
Swiss Bar Association

Eidgenössisches Justiz- und
Polizeidepartement EJPD (EFD)

Per Email versandt:

ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, der 16. Mai 2025

Stellungnahme des Schweizerischen Anwaltsverbands SAV-FSA zur Teilrevision der Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat

Sehr geehrte Damen und Herren

Der Bundesrat hat am 29. Januar 2025 die Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) eröffnet. Der Schweizerische Anwaltsverband bedankt sich für die Einladung zur Vernehmlassung, die gewährte Fristerstreckung und nimmt dazu wie folgt Stellung:

Die vorliegende Stellungnahme beschränkt sich auf eine Abschätzung, inwieweit die vorgeschlagenen Änderungen mit übergeordnetem Recht vereinbar sind (1.-3.), und weitergehende Bedenken aus Sicht der schweizerischen Anwaltschaft ab (4.).

1. Verstösse gegen das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs

1.1 Unzulässige Ausweitung des Begriffs “grosse Benutzerschaft”

Die Revision definiert in den neuen Artikeln 16a und 16d VÜPF die Kategorien der mitwirkungspflichtigen Unternehmen neu. Besonders problematisch dürfte die deutliche Absenkung der Schwellenwerte für erweiterte Überwachungspflichten sein. Nach Art. 27 Abs. 3 BÜPF dürfen erweiterte Überwachungspflichten für AAKD nur bei einer “grossen Benutzerschaft” verlangt werden. Die Revision setzt diese Schwelle nun bereits bei 5'000 Nutzenden an, unabhängig vom Umsatz. Diese Auslegung des unbestimmten Rechtsbegriffs “grosse Benutzerschaft” dürfte mit dem Willen des Gesetzgebers nicht vereinbar sein. Die Revision dürfte die gesetzliche Ermächtigung unzulässig überschreiten.

1.2 Neues Kategorisierungsmodell ohne ausreichende gesetzliche Grundlage

Die Einführung der dreistufigen Differenzierung für AAKD mit minimalen, mittleren und vollen Pflichten findet im BÜPF keine hinreichende gesetzliche Grundlage. Das Gesetz unterscheidet lediglich zwischen minimalen Pflichten (für alle AAKD) und darüber hinausgehenden Pflichten (für AAKD mit “grosser Benutzerschaft”). Die Entscheidung des Bundesverwaltungsgerichts in Sachen Threema (A-550/2019) hat bereits die Notwendigkeit einer klaren Abgrenzung zwischen Fernmeldedienstanbieterinnen (FDA) und AAKD betont. Das Bundesgericht hat diese Entscheidung bestätigt (2C_544/2020). Das neue Kategorisierungsmodell verwischt durch die Einführung der mittleren Kategorie diese rechtlich Unterscheidung und schafft ein gesetzlich nicht vorgesehenes Hybrid-Modell, was die gesetzliche Ermächtigung unzulässig überschreiten dürfte.

2. Verstösse gegen die Bundesverfassung der Schweizerischen Eidgenossenschaft

2.1 Verletzung des Verhältnismässigkeitsprinzips

Die Revision dürfte gegen den verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit (Art 5 BV) verstossen, indem sie bereits kleine Unternehmen mit 5'000 Nutzern umfangreichen Überwachungspflichten unterwirft. Diese (somit bereits für kleine Unternehmen geltenden, umfangreichen) Massnahmen dürften in ihrer Eingriffsintensität nicht durch den verfolgten Zweck gerechtfertigt sein. Darüber hinaus dürften sie besonders Schweizer KMUs unverhältnismäßig stark belasten.

2.2 Verletzung des Gesetzesvorbehalts

Gemäss Art. 36 BV bedürfen Einschränkungen von Grundrechten einer gesetzlichen Grundlage. Der Schutz des Post- und Fernmeldeverkehrs ist ein verfassungsmässig garantierter Grundrecht (Art. 13 BV). Die vorgeschlagenen Verordnungsänderungen erweitern die Überwachungsmöglichkeiten erheblich, ohne dass dafür eine - aus unserer Sicht - ausreichend bestimmte gesetzliche Grundlage bestehen dürfte.

2.3 Verletzung des Rechtsgleichheitsgebots

Die unterschiedliche Behandlung von Anbietern ähnlicher Grösse, z.B. an der Schwelle von 5'000 Nutzern, dürfte gegen das Rechtsgleichheitsgebot (Art. 8 BV) verstossen. Während

internationale Großkonzerne technische und finanzielle Ressourcen haben, um die (umfangreichen) Anforderungen zu erfüllen, dürften KMUs bezogen auf Ihre Grösse und finanzielle Möglichkeiten überproportional (Kosten pro Nutzer) belastet werden.

3. Verstösse gegen die Konvention zum Schutze der Menschenrechte und Grundfreiheiten

3.1 Unverhältnismässiger Eingriff in das Recht auf Privatleben

Die vorgesehenen, zusätzlichen Überwachungsmassnahmen dürften einen Eingriff in die durch Art. 8 EMRK geschützten Rechte darstellen, insbesondere in das im Recht auf Privatleben enthaltene Recht auf Achtung der Vertraulichkeit der Korrespondenz. Gemäss Art. 8 Abs. 2 EMRK muss ein solcher Eingriff "in einer demokratischen Gesellschaft notwendig" sein.

Die niedrigen Schwellenwerte für erweiterte Überwachungspflichten dürften aus unserer Sicht zu einer flächendeckenden Überwachungsinfrastruktur führen, die weit über das hinausgeht, was für eine effektive Strafverfolgung objektiv notwendig ist. Dies dürfte den Grundsatz der Verhältnismässigkeit verletzen, wie er vom Europäischen Gerichtshof für Menschenrechte in ständiger Rechtsprechung ausgelegt wird.

3.2 Verletzung des Gesetzesvorbehalts

Der Eingriff in das durch Art. 8 EMRK geschützte Recht muss gemäss Wortlaut und ständiger Rechtsprechung des EGMR "gesetzlich vorgesehen" sein. Dies bedeutet, dass eine gesetzliche Grundlage vorhanden und hinreichend bestimmt formuliert sein muss. Die extensive Auslegung des unbestimmten Rechtsbegriffs "grosse Benutzerschaft" in Art. 27 Abs. 3 BÜPF durch die Verordnung dürfte diese Anforderung nicht erfüllen. Ein AAKD mit 5'000 Nutzern dürfte nach unserer Ansicht nicht über eine grosse Benutzerschaft iSd Art. 27 Abs. 3 BÜPF verfügen.

Besonders problematisch dürfte zudem die in Art. 16d VÜPF neu eingeführte mittlere Kategorie von AAKD sein, die zur (Vorrats-)Speicherung von Randdaten und zur Entschlüsselung von Kommunikation verpflichtet werden sollen. Diese weitreichenden Maßnahmen dürften eine explizite gesetzliche Grundlage erfordern, die im BÜPF betreffend AAKD nicht existiert.

4. Schlussüberlegungen und Empfehlung

Die vorgeschlagenen Teilrevision der VÜPF und VD-ÜPF weisen nach unserer Ansicht rechtliche Mängel auf. Die Revision dürfte grundlegend mit Rücksicht auf das BÜPF, die schweizerische Verfassung und unter Beachtung der internationalen Verpflichtungen der Schweiz neu zu gestalten sein. Nur so dürfte eine zweckdienliche Fernmeldeüberwachung ohne massive Kollateralschäden geschaffen werden können.

Wir bedauern daher auch, dass der erläuternde Bericht sich lediglich auf Auswirkungen auf den Bund, Kantone/Gemeinde und MWPs beschränkt. Wir regen an, dass im Rahmen der weiteren Befassung die Interessen der Strafverfolgungsbehörden im Rahmen einer

umfangreicheren Folgenabschätzung ggf. ein wenig mehr mit dem Wesensgehalt unserer Grundrechte zu tarieren.

Ein besonderes Augenmerk möchten wir auf den (bösen) Schein einer gemäss Vernehmlassung nun gar vertieften, anlasslosen Massenüberwachung der anwaltlichen Kommunikation mit unserer Mandantschaft lenken. Wir bewerten die anlasslose, massenhafte Speicherung der Kommunikationsmetadata von Berufsträgern grundsätzlich als nicht gerechtfertigten Eingriff in die Privatsphäre und die Berufsausübung. Mangels expliziter Ausnahme oder Abschirmungspflicht für geschützte Berufskommunikation besteht eine Schutzlücke. Aus Sicht der Anwaltschaft ist nicht erst ein Zugriff, sondern bereits die Speicherung privilegierter Kommunikationsdaten problematisch.

Gemäss der gegenständlichen Vernehmlassung würden zahlreiche neue Datensammlungen bei einer Vielzahl von kleineren Anbietern entstehen, die u.a. für die detaillierte Rekonstruktion sensibler beruflicher Kommunikation von Anwälten mit Mandanten missbraucht werden können. Kleinere AAKD verfügen oft nicht über vergleichbare Datenschutzstandards, Compliance-Prozesse oder Verschlüsselungsmassnahmen wie grosse Anbieter. Dadurch allein besteht ein höheres Risiko unberechtigter Zugriffe oder Datenpannen, die aber ebenso auch bei grösseren Anbietern auftreten. Die neuen Hackingziele für staatliche und private Akteure können unserer Mandantschaft erheblichen Schaden verursachen, und das Vertrauen in die geschützte Kommunikation mit der Anwaltschaft verringern (Abschreckungseffekt für Rechtssuchende). Mit dem Vertrauen in die Anwaltschaft würde zwangsläufig das Vertrauen in den schweizerischen Rechtsstaat insgesamt sinken.

Mit Blick auf die o.g. Grundkonstellation wäre die schweizerische Anwaltschaft dankbar, wenn das EJDP jedenfalls bis zur Grundsatzentscheidung in Az. 47351/18 (EGMR) von weiteren Ausweitungen/Verschärfungen der anlasslosen Massenüberwachung auf Verordnungsebene Abstand nehmen könnte.

Wir danken Ihnen für Ihre geschätzte Kenntnisnahme.

Mit vorzüglicher Hochachtung

Präsident SAV

Matthias Miescher



Generalsekretär SAV

René Rall



Von: Pedro Faustino <hi@pedrofaustino.com>

Gesendet: Donnerstag, 10. April 2025 17:56

An: Biberstein Jean-Louis ISC-EJPD <jean-louis.biberstein@isc-ejpd.admin.ch>

Betreff: Prise de position dans le cadre de la consultation sur l'ordonnance relative à la surveillance des communications

À l'attention de l'autorité compétente,

Je me permets, en tant que citoyen suisse profondément attaché aux libertés fondamentales, à la démocratie et à la neutralité numérique de notre pays, de vous adresser la présente prise de position dans le cadre de la consultation relative à l'ordonnance mentionnée dans le communiqué du Conseil fédéral du 29 janvier 2025 (msg-id-103968).

1. Opposition à l'atteinte à la vie privée

L'ordonnance proposée, en imposant aux fournisseurs de services de communication (comme Proton, Threema, Nym, etc.) de collecter des données d'identification et, potentiellement, de compromettre le chiffrement de bout en bout, constitue une atteinte directe au droit fondamental à la vie privée inscrit dans la Constitution fédérale (art. 13).

Une telle mesure va à l'encontre des principes démocratiques suisses et ouvre la voie à une surveillance généralisée qui ne devrait exister que dans des cadres strictement proportionnés, ciblés et encadrés par la justice. Elle risque d'introduire une culture de méfiance et de contrôle au lieu de promouvoir la confiance entre les citoyens et l'État.

2. Menace pour les entreprises suisses innovantes

Cette ordonnance fragilise des entreprises suisses reconnues mondialement pour leur engagement en faveur de la confidentialité numérique. Des sociétés comme Proton, Threema et Nym sont des fleurons de notre souveraineté technologique. En rendant leur modèle économique non viable, cette législation nuira non seulement à leur réputation, mais aussi à l'attractivité de la Suisse en tant que place technologique et refuge de la confidentialité.

3. Procédé antidémocratique préoccupant

Il est profondément regrettable qu'un projet de cette portée, qui touche à des droits fondamentaux, soit introduit par voie d'ordonnance sans débat parlementaire approfondi, ni possibilité de référendum populaire. Une telle approche réduit la transparence du processus démocratique et affaiblit la légitimité d'une réglementation aussi sensible.

4. Recommandations

Je recommande instamment :

- Le retrait ou la révision en profondeur de cette ordonnance.
- L'ouverture d'un dialogue avec les entreprises technologiques suisses, les associations de défense des droits numériques, les experts juridiques et les citoyens.
- La garantie explicite de la protection du chiffrement de bout en bout et de l'anonymat en ligne dans les textes légaux.
- Un encadrement judiciaire rigoureux de toute mesure de surveillance, limité à des cas individuels et proportionnés.

Conclusion

La Suisse ne doit pas devenir un terrain d'expérimentation pour la surveillance numérique. Elle doit rester un exemple mondial en matière de respect des droits individuels, de neutralité technologique et de démocratie participative. En tant que citoyen, je vous exhorte à reconsidérer ce projet dans cet esprit.

Je vous remercie de prendre en compte cette prise de position.

Avec mes salutations respectueuses,

Pedro Faustino

Wollerau, SZ

10-Avril-2025

Prise de Position Formelle:

Concernant la révision partielle des ordonnances OSCPT et OME-SCPT

Soumise dans le cadre de la consultation ouverte par le Département fédéral de justice et police (DFJP)

Date : 14 Avril 2025

Auteur : George Bowring

Contact : georgebowring@gmail.com,

1. Introduction

Nous exprimons par la présente notre **opposition résolue** au projet de révision partielle des ordonnances OSCPT et OME-SCPT.

Sous couvert de clarification et de mise à jour technique, ce projet représente un **glissement grave et disproportionné vers une surveillance généralisée** des communications électroniques en Suisse.

Nous appelons à son retrait immédiat, au nom :

- des **droits fondamentaux**, notamment la protection de la sphère privée et des données ;
 - de la **stabilité juridique et économique** pour les entreprises suisses du numérique ;
 - de la **crédibilité internationale** de la Suisse comme havre de confiance numérique.
-

2. Atteinte aux libertés fondamentales et au principe de proportionnalité

Cette révision introduit :

- une multiplication des **types de surveillance en temps réel et rétroactive** ;
- une obligation élargie de **collecte des métadonnées** — sans exigence judiciaire préalable ;
- des critères vagues pour classer toute entreprise numérique comme « **personne obligée de collaborer** » (POC), même à partir de 5000 utilisateurs.

En permettant la **collecte préventive de métadonnées** sur une large portion de la population, cette réforme entre en **contradiction manifeste avec les articles 5 et 13 de la Constitution fédérale**, le principe de proportionnalité, et les garanties de la Convention européenne des droits de l'homme.

3. Menace directe à l'écosystème numérique suisse : le cas Proton

La Suisse a su attirer des **leaders mondiaux de la technologie respectueuse de la vie privée**, tels que **Proton**, précisément grâce à son équilibre subtil entre sécurité, neutralité, et protection des données.

La société Proton, basée à Genève, emploie 150 personnes en Suisse et propose des services sécurisés à plus de **100 millions d'utilisateurs** dans le monde. Le fondateur Andy Yen a été clair

« Si cette révision entre en vigueur, Proton quittera la Suisse. »

Il ne s'agit pas d'une menace en l'air : **les plans de délocalisation sont prêts**, et les serveurs ont déjà commencé à être déplacés à l'étranger depuis 2021. La **Trust Valley romande** et la **Crypto Valley alémanique** risquent de perdre leurs figures de proue à cause de cette fuite en avant réglementaire.

4. Rétention de métadonnées : un précédent dangereux

L'enjeu fondamental est celui des **métadonnées** :

- Qui écrit à qui ?
- Quand ?
- D'où ?
- Via quel service ?

Les contenus peuvent rester chiffrés mais les métadonnées, comme l'admettait déjà un ancien directeur de la NSA, permettent d'**identifier, localiser, profiler et traquer** n'importe quel utilisateur. Ces données, autrefois accessibles **sur décision judiciaire**, pourraient désormais être transmises **en continu et sans contrôle**, y compris à l'étranger.

5. Une réforme à rebours du droit européen

La directive européenne sur la conservation des données a été invalidée par la CJUE, précisément pour cause de **collecte de masse injustifiée**.

Vouloir instaurer en Suisse un régime **plus intrusif que celui de l'UE**, en violation de notre propre jurisprudence et de nos engagements internationaux, est **juridiquement risqué et économiquement suicidaire**.

6. Impacts disproportionnés sur l'économie numérique suisse

Cette réforme menace non seulement les grandes entreprises comme Proton, mais aussi **toutes les PME innovantes**, qui seraient contraintes de :

- se doter de systèmes d'interception et de stockage de données comparables à ceux de Swisscom ;
- assumer des coûts techniques et juridiques faramineux ;
- naviguer dans un **climat d'insécurité réglementaire** permanent.

Nous risquons de voir fuir **startups, talents, investisseurs et centres de données**. À l'heure où la souveraineté numérique devient stratégique, cette réforme revient à **saborder nos propres atouts**.

7. Ce que nous demandons

Nous appelons le Conseil fédéral à :

1. **Retirer le projet actuel de révision** de l'OSCPT et de l'OME-SCPT.
 2. **Ouvrir un véritable dialogue** avec les acteurs du numérique, les spécialistes de la protection des données, les juristes et la société civile.
 3. **Garantir qu'aucune obligation de surveillance ou de rétention de données** ne soit imposée sans décision judiciaire individuelle.
 4. **Renforcer la sécurité juridique** en cohérence avec le droit européen et les principes de l'État de droit.
 5. **Préserver l'attractivité de la Suisse comme hub technologique fondé sur la confiance.**
-

8. Conclusion

Dans un monde où le **multilatéralisme est en crise**, la Suisse a une carte unique à jouer : celle de la **neutralité**, de la **stabilité** et de la **confiance numérique**. En garantissant une **protection exemplaire des données personnelles**, elle peut devenir un havre pour les particuliers et entreprises du monde entier qui cherchent une alternative crédible aux modèles intrusifs dominants.

Cette révision va directement à l'encontre de cet avantage comparatif. En affaiblissant les garanties de protection des données privées, la Suisse risque de compromettre sa position stratégique dans l'économie numérique mondiale.

Cette réforme précipitée met en péril une filière économique stratégique et nos valeurs fondamentales.

Avec nos salutations respectueuses,

George Bowring

Geneva Gov Tech Foundation

An: Biberstein Jean-Louis ISC-EJPD <jean-louis.biberstein@isc-ejpd.admin.ch>

Betreff: Re: Concerns Regarding the New Surveillance Regulations

Dear Jean-Louis

Did you receive my previous email and took it into consultation? Could you please write me back that you have confirmed to have received the letter? Thank you.

Best regards

On April 4, 2025 12:52:10 PM GMT+02:00, N <natzki@mailbox.org> wrote:

Dear Jean-Louis

I am writing to express my strong concerns regarding the proposed revision of the regulations related to the surveillance of postal and telecommunications traffic (VÜPF and VD-ÜPF) that was opened for consultation on January 29, 2025.

As a Swiss citizen and someone who deeply values privacy and the integrity of our data protection laws, I believe this proposal undermines the strong privacy protections that Switzerland has long been known for. The introduction of increased data retention and surveillance, along with the requirement to remove encryption, is a worrying step back for privacy rights in our country.

Encryption is an essential tool for safeguarding the privacy and security of individuals and businesses alike. The proposed changes will weaken encryption measures that are indispensable for protecting sensitive information in today's digital world. This is particularly concerning in a time when countless individuals and organizations are working tirelessly to ensure that encryption remains a cornerstone of a free and open society. The fact that this proposal seeks to weaken those protections is not only harmful but also unnecessary.

Furthermore, it is troubling that such a significant decision, which will affect the privacy of all citizens, is being made without a public referendum. The Swiss people should have the right to vote on such matters, especially when they involve such a fundamental right as privacy. The absence of a referendum means that many citizens, who are rightfully concerned about the implications of these changes, will not have a direct say in the outcome.

I urge you to reconsider these proposed changes and the negative impact they would have on the privacy and freedom of Swiss citizens. It is crucial that we continue to uphold and protect the strong privacy laws that make Switzerland a global leader in data protection.

Thank you for your attention to this critical issue.

Sincerely,

N

Von: eric@metadesprit.com <eric@metadesprit.com>

Gesendet: Mittwoch, 30. April 2025 15:07

An: Biberstein Jean-Louis ISC-EJPD <jean-louis.biberstein@isc-ejpd.admin.ch>

Betreff: Surveillance des télécommunications - consultation

Monsieur Biberstein,

Par la présente, et en qualité de citoyen de nationalité suisse, je me permets d'apporter mes remarques concernant la révision partielle des ordonnances liées à la Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication.

J'ai pris connaissance avec intérêt des propositions du Conseil Fédéral, particulièrement l'introduction, pour les fournisseurs de services de communication dérivés, d'obligations d'identification et de mise à disposition de données historiques dans le contexte d'enquêtes judiciaires ou d'activités de renseignement.

Mon interprétation est que les organes d'enquête cherchent à harmoniser la pratique actuellement pratiquée sur les réseaux téléphoniques et GSM, permettant de connaître qui a communiqué avec qui, et à quel moment, ceci de manière rétroactive. L'extension desdites pratiques aux applications de télécommunication chiffrée est l'objectif de l'adaptation de la législation.

Je comprends parfaitement les raisons qui poussent les autorités de poursuite pénale dans cette direction, ayant moi-même par le passé fait partie des organes de surveillance. Je comprends également que les modifications proposées n'atteindront pas leur objectif, puisqu'elles engendreraient un départ systématique des entreprises actuellement établies en Suisse fournissant des services de communication chiffrés et axés sur la vie privée.

En effet, ces prestataires de services ont un modèle d'affaires basé sur la confidentialité des données. Ils attirent donc une base de clientèle qui cherche la discréetion et la limitation des données collectées au strict minimum. Une obligation systématique d'identification, comme elle est précisée dans le futur article 19 alinéa 1 de l'ordonnance, ferait probablement perdre une majorité de clients à ces prestataires, les mettant dans une situation économique impossible à gérer.

Par ailleurs, l'obligation de stockage de données historiques évoquée à l'article 21 alinéa 1 (obligation de renseignement) représente assurément une friction considérable, vu la masse d'informations que cela représente. Stocker systématiquement les en-têtes de messages durant toute la relation commerciale et durant six mois après celle-ci constitue des coûts extrêmement élevés que les entreprises de petite et moyenne taille ne pourront pas assumer.

Si l'ordonnance est modifiée en l'état du projet, nous aurons donc plusieurs entreprises actuellement suisses qui se verront contraintes de déplacer leurs sièges sociaux et leurs activités hors de notre pays, ceci pour des questions de compétitivité. Nous aurons également l'arrêt net de tout nouveau projet lié aux télécommunications privées sur notre territoire, puisque la barrière à l'entrée serait trop élevée pour pouvoir lancer une entreprise dans ce domaine. Le coût d'opportunité d'une telle législation est énorme.

Sans compter la perte de confiance du monde concernant la Suisse comme "coffre-fort des données numériques".

L'objectif de la loi ne serait par ailleurs pas atteint, puisqu'il compliquerait encore plus le travail des autorités d'enquête. Ces dernières seraient alors obligées d'aller récupérer les données convoitées dans des juridictions étrangères, ces dernières n'étant pas toujours très collaboratives. Les ex-entreprises suisses continueraient de délivrer le même service qu'auparavant, les utilisateurs cherchant la confidentialité continuant à les utiliser comme auparavant.

L'unique résultante serait alors une perte économique et de confiance pour la Suisse, mais également une non-croissance future dans le domaine spécifique de la vie privée et des technologies de communication chiffrées.

Au-delà des aspects purement pécuniaires, les services de sécurité de la Confédération ainsi que l'Armée, qui utilisent actuellement Threema pour leurs échanges confidentiels, se verraient obligés d'utiliser un service étranger. Ils seraient par conséquent à la merci d'une puissance étrangère, cette dernière pouvant décider à tout moment de couper le service et ainsi rendre nos autorités impotentes.

En conclusion : l'introduction de telles dispositions, particulièrement celle concernant la fourniture de données rétroactives, rendrait le territoire suisse totalement stérile pour toute entreprise ou projet axé sur la préservation de la vie privée et les télécommunications encryptées. La conséquence en serait le départ vers d'autres juridictions de services présentement établis, tels que Threema ou Proton, mais également l'impossibilité pour de nouvelles entreprises de s'établir, la limite des 5'000 utilisateurs étant rapidement atteinte.

Si l'objectif de l'ordonnance est de diminuer la compétitivité de la Suisse, il serait alors atteint. Pour ce qui est de l'efficacité de la lutte contre la criminalité, je me permets de douter d'une quelconque amélioration.

En vous remerciant pour votre lecture et pour la prise en considération de mon point de vue, je vous prie de croire, Monsieur Biberstein, à mes considérations distinguées.

Eric Mermod
1228 Plan-les-Ouates

---English

Jean-Louis Biberstein

[REDACTED]

Dear Mr. Biberstein,

I have been a resident of Switzerland for 16 years, though not yet a citizen, and I sincerely thank you for considering the input of permanent residents like myself.

I am deeply concerned about the proposed law on "Surveillance des télécommunications et entreprises obligées de collaborer." I believe it poses a serious threat to democracy, which depends fundamentally on the free flow of information. Around the world, authoritarian regimes such as those in Turkey, Russia, and China increasingly punish citizens for exercising their democratic rights or seeking information to stay informed. Switzerland, as a beacon of effective democracy, should not normalize surveillance of its citizens. Such measures risk creating a society where people fear visiting independent news sites, worried their names might be recorded. While this may seem distant now, the global trajectory suggests otherwise.

Thank you for your attention to these concerns.

Respectfully,

John Nanninga

[REDACTED]

Eidgenössisches Justiz- und Polizeidepartement
(EJPD)
Bundeshaus West
CH-3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 05.05.2025

Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat Beat Jans
Sehr geehrte Empfänger:innen

Die geplante Revision der VÜPF ist ein Frontalangriff auf unsere Grundrechte, die Rechtsstaatlichkeit sowie den IT- und Innovationsstandort Schweiz. Deshalb lehne ich die Revision vollumfänglich und in aller Deutlichkeit ab. Zudem steht diese Revision im Widerspruch zum Bestreben nach einer stärkeren europäischen digitalen Souveränität und ist verheerend schädlich für den Wirtschaftsstandort Schweiz sowie für auf Privatsphäre fokussierte Unternehmen. Firmen wie Proton oder Threema müssten die Schweiz verlassen – was sicherlich nicht im Interesse der Schweiz ist. Zudem nutzt auch die Schweizer Regierung Threema, was ebenfalls zu bedenken ist, falls Threema gezwungen wäre, ins Ausland zu verlagern.

Für vertiefte Informationen, möchte ich auf die Vernehmlassungsantwort der Digitalen Gesellschaft verweisen:
<https://www.digitale-gesellschaft.ch/uploads/2025/05/Stellungnahme-Digitale-Gesellschaft-VUePF-VD-UePF.pdf>

Freundliche Grüsse,
Christophe Nicolet

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
CH-3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Bern, 5. Mai 2025

Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat Beat Jans
Sehr geehrte Empfänger:innen

Am 29. Januar 2025 eröffnete der Bundesrat die Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF).

Eine Ausweitung der Überwachung von solch erheblicher Tragweite darf nicht einfach auf Verordnungsstufe geregelt werden. Die Regelungen gehören zwingend in ein Gesetz, müssen vom Parlament erlassen und einer demokratischen Legitimation mittels Referendum unterstellt werden. Der Versuch, dermassen weitreichende Überwachungspflichten auf dem Verordnungsweg einzuführen, stellt einen klaren Verstoss gegen das Legalitätsprinzip dar und untergräbt die Kompetenzordnung.

Mit freundlichen Grüßen

Adrian Hildbrand

[REDACTED]

[REDACTED]

Von: Manuel Brunner
Gesendet: Montag, 5. Mai 2025 13:08:48 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Persönliche Stellungnahme zu den Änderungen VÜPF/VD-ÜPF

Sehr geehrte Damen und Herren

Ich bin besorgt über die geplanten Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und möchte Ihnen meine persönliche Stellungnahme dazu mitteilen. Die geplante Revision ist ein Frontalangriff auf unsere Grundrechte, die Rechtsstaatlichkeit und den IT- und Innovationsstandort Schweiz. Die Änderungen würden geltendes Recht in einem Ausmass verletzen, das alarmieren muss.

Zu den Hauptpunkten gehören aus meiner Sicht die folgenden Punkte:

- Die geplante Revision würde die Überwachung massiv ausweiten und den Zugang zu geschützten Kommunikationsmitteln für private Nutzer, Unternehmen und schutzbedürftige Personengruppen verwehren.
- Die Änderungen würden den Innovations- und Wirtschaftsstandort Schweiz schwächen, indem sie die Ausweitung der Überwachung und die damit verbundenen, übermässigen Mitwirkungspflichten fördern.
- Die geplante Revision ignoriert die Schutzbedürfnisse von Whistleblowern, Menschen mit ungeklärtem Aufenthaltsstatus oder ohne Papiere und Aktivistinnen, indem sie den Zugang zu vertraulichen Kommunikationsmitteln verwehren.

Ich bitte Sie, diese Bedenken zu berücksichtigen und die geplante Revision in ihrer jetzigen Form abzulehnen.

Freundliche Grüsse
Manuel Brunner

Chancey Gilbert

[REDACTED]
CH-8400 Winterthur

Eidgenössisches Justiz- und Polizeidepartement (EJPD)

Bundeshaus West

CH-3003 Bern

Per email an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Winterthur, 5. Mai 2025

Stellungnahme zur Teilrevision VÜPF und VD-ÜPF

Sehr geehrte Damen und Herren,

Im Rahmen der Vernehmlassung zu den Änderungen der Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) möchte ich meine ernsthaften Bedenken äussern.

Die geplante Ausweitung der Identifikations- und Überwachungspflichten für Anbieter von Kommunikationsdiensten würde nahezu alle Anbieter in der Schweiz betreffen. Dies stellt einen schwerwiegenden Angriff auf die Grundrechte dar. Besonders besorgt bin ich über die Auswirkungen auf KMU sowie Non-Profit- und Open-Source-Projekte, die durch die neuen Pflichten benachteiligt werden könnten.

Bereits jetzt sind die Überwachungsmassnahmen unverhältnismässig. Die geplante Verschärfung würde den Zugang zu datenschutzfreundlichen Diensten einschränken, was die informationelle Selbstbestimmung und den Schutz der Privatsphäre gefährdet. Diese Rechte sind durch die Bundesverfassung und internationale Abkommen garantiert und dürfen nicht leichtfertig aufgegeben werden.

Eine Ausweitung der Überwachung von solch erheblicher Tragweite muss gesetzlich geregelt werden, nicht per Verordnung. Die demokratische Legitimation durch das Parlament und ein mögliches Referendum sind zwingend erforderlich. Der aktuelle Ansatz des Bundesrats verstösst gegen das Legalitätsprinzip und untergräbt die Kompetenzordnung.

Ich fordere das EJPD auf, die vorgeschlagenen Änderungen zu überdenken und sich für den Schutz von Grundrechten und datenschutzfreundlichen Lösungen in der Schweiz einzusetzen.

Vielen Dank für die Berücksichtigung meiner Stellungnahme.

Mit freundlichen Grüßen,

Chancey Gilbert

Basel, 5. Mai 2025

Vernehmlassungsantwort zu den Teilrevisionen der VÜPF und der VD-ÜPF

Sehr geehrte Damen und Herren

Ich danke Ihnen für die Möglichkeit zur Stellungnahme und nehme wie folgt zu den vorgeschlagenen Teilrevisionen der VÜPF und der VD-ÜPF Stellung:

Zunächst möchte ich betonen, dass ich die Stellungnahme der Digitalen Gesellschaft vollumfänglich unterstütze. Die dort vorgebrachten Argumente spiegeln meine Bedenken und Einschätzungen treffend wider.¹

Aus meiner Sicht stehen die vorgeschlagenen Änderungen in keinem angemessenen Verhältnis zwischen Kosten und Nutzen. Besonders für kleine und mittlere Unternehmen (KMU) bedeuten die geplanten Anpassungen eine unverhältnismässige Belastung. Die vorgesehene harte Limite von 5'000 Nutzerinnen und Nutzern sind für Anbieter von digitalen Dienstleistungen problematisch, da diese Schwelle aufgrund der globalen Verfügbarkeit ihrer Angebote rasch erreicht wird. Damit werden insbesondere innovative und kleinere Anbieter massiv benachteiligt.

Die Lage wird aus meiner Sicht zusätzlich verschärft, da die ausländischen «Big Player» wie Google, Meta und Microsoft Stand heute bereits den grössten Teil des Marktes abdecken.

Weitergehend kritisiere ich Artikel 16h. Personen, die ihren Internetzugang teilen, wie die Freifunk-Bewegung², würden nicht mehr betrieben werden können. Gerade in Zeiten, in denen digitale Infrastruktur vermehrt angegriffen wird und der Wunsch nach digitaler Unabhängigkeit in der Bevölkerung grösser wird, wäre es eine fatale Entscheidung, Projekte, die digitale Kommunikation resilenter gestalten, zu unterdrücken.

Ebenfalls ist die Definition «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen.» zu allumfassend.

Bereits etablierte Systeme wie das Tor Netzwerk, welches direkt von der Teilnahme Freiwilliger abhängig ist, würden unterbunden werden.

Die Einschränkungen würden sich aber nicht nur negativ auf etablierte Systeme auswirken, sondern auch auf Personen, die «Matrix Bridge Server»³ zur Verfügung stellen, um Interoperabilität zwischen Messengern zu ermöglichen. Bestrebungen im Bereich Barrierefreiheit würden aufgrund dessen massiv leiden.

Besten Dank für die Kenntnisnahme
Freundliche Grüsse

Gabriel Amstutz

1 <https://www.digitale-gesellschaft.ch/uploads/2025/05/Stellungnahme-Digitale-Gesellschaft-VUePF-VD-UePF.pdf>

2 <https://freifunk.net/>

3 <https://matrix.org/ecosystem/bridges/>

Von: Chris Ensor

Gesendet: Montag, 5. Mai 2025 17:09:00 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Einspruch gegen die Ausweitung von Überwachungsmaßnahmen

Sehr geehrte Mitglieder des Bundesrates,

ich schreibe Ihnen, um meinen starken Einspruch gegen die jüngsten Vorschläge auszudrücken, die darauf abzielen, die Überwachungsmassnahmen durch Änderungen der Telekommunikationsüberwachungsordnungen (VÜPF und VD-ÜPF) erheblich auszubauen.

Als Privatperson bin ich zutiefst besorgt darüber, dass diese Änderungen mein grundlegendes Recht auf Privatsphäre untergraben, welches ein Eckpfeiler jeder demokratischen Gesellschaft ist. Die geplante Ausweitung der staatlichen Überwachungsbefugnisse stellt eine ernsthafte Bedrohung nicht nur für individuelle Rechte dar, sondern untergräbt auch das Vertrauen in unsere Institutionen. Der Umfang dieser vorgeschlagenen Massnahmen erscheint übertrieben und nicht gerechtfertigt, insbesondere in einem Land, das stolz darauf ist, Bürgerfreiheiten zu wahren.

Überwachungsmassnahmen, die ohne strenge Aufsicht und Rechenschaftspflicht durchgeführt werden, schaffen ein Umfeld, in dem Bürger sich ständig überwacht fühlen könnten. Dies kann zu einem abkühlenden Effekt auf die Meinungsfreiheit und den Dissens führen, die essentielle Bestandteile einer gesunden Demokratie sind. Es ist von entscheidender Bedeutung, dass alle sicherheitsrelevanten Massnahmen nicht auf Kosten der Privatsphäre und Freiheiten gehen, die uns von unserer Verfassung garantiert werden.

Darüber hinaus bitte ich Sie, die potenziellen Auswirkungen dieser Politik auf verschiedene Sektoren zu berücksichtigen, einschließlich Technologie- und Kommunikationsunternehmen, die gezwungen sein könnten, sich an invasive Vorschriften zu halten. Solche Änderungen könnten auch Innovation und Investitionen in unserem Land entmutigen.

Ich fordere Sie respektvoll auf, die vorgeschlagenen Änderungen der Telekommunikationsüberwachungsordnungen zu überdenken und den Schutz der Privatsphäre der Bürger zu priorisieren. Ich ermutige Sie, alternative Ansätze zu suchen, die die Sicherheit erhöhen, ohne die individuellen Freiheiten einzuschränken.

Vielen Dank für Ihre Aufmerksamkeit in dieser Angelegenheit. Ich hoffe, dass Sie sich bei Ihren weiteren Entscheidungen für den Schutz unserer Privatsphäre einsetzen.

Mit freundlichen Grüßen,

CHRIS ENSOR

email: chris@chrisensor.com

Von: Mike

Gesendet: Montag, 5. Mai 2025 20:04:23 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Ablehnung der vorgeschlagenen Änderungen der Schweizer Überwachungsgesetze

Sehr geehrter Herr Bundesrat Beat Jans

Sehr geehrte Empfänger:innen

Hiermit möchte ich meine entschiedene Ablehnung der vorgeschlagenen Änderungen der Schweizer Überwachungsgesetze, wie sie in der laufenden Vernehmlassung dargelegt werden, zum Ausdruck bringen. Ich bin überzeugt, dass diese Änderungen eine ernsthafte Bedrohung für die Privatsphäre und die Bürgerrechte der Menschen in der Schweiz darstellen und die Prinzipien der Demokratie und der Menschenrechte untergraben.

Der Versuch, bestehende Regelungen zu ändern, um strengere Überwachungsmaßnahmen durchzusetzen, insbesondere nachdem das Schweizer Bundesgericht den vorherigen Versuch für rechtswidrig erklärt hat, wirft ernsthafte rechtliche und ethische Bedenken auf. Es ist alarmierend, dass derart weitreichende Änderungen ohne Volksabstimmung vorgenommen werden können, wodurch der demokratische Prozess umgangen und den Bürgerinnen und Bürgern die Möglichkeit genommen wird, ihre Meinung zu Fragen zu äußern, die ihre Rechte direkt betreffen.

Die von der Digitalen Gesellschaft Schweiz vorgebrachten Argumente (vgl. Anhang) unterstreichen die potenzielle Rechtswidrigkeit dieser vorgeschlagenen Änderungen, da sie gegen höherrangiges Recht, einschließlich der Schweizer Bundesverfassung und der Europäischen Menschenrechtskonvention, verstößen könnten. Es ist von entscheidender Bedeutung, dass jede Gesetzgebung diese grundlegenden rechtlichen Rahmenbedingungen respektiert, und ich fordere Sie auf, die Auswirkungen dieses Vorschlags zu überdenken.

Zudem können die Auswirkungen dieser Änderungen auf datenschutzorientierte Unternehmen und Dienste in der Schweiz nicht hoch genug eingeschätzt werden. Die vorgeschlagenen Massnahmen könnten Unternehmen wie Threema, Proton und NymVPN dazu zwingen, ihre Geschäftsmodelle zu ändern oder ihre Aktivitäten ganz einzustellen, was nicht nur der digitalen Landschaft in der Schweiz schaden, sondern auch der wachsenden Bewegung für digitale Souveränität und Unabhängigkeit von grossen Technologieunternehmen zuwiderlaufen würde.

Ich fordere Sie auf, die Bedenken der Digitalen Gesellschaft Schweiz und anderer Interessengruppen zu berücksichtigen. Die möglichen Folgen dieser Änderungen sind weitreichend und könnten zu einem Überwachungsstaat führen, der die Rechte und Freiheiten der Menschen verletzt.

Abschliessend bitte ich Sie, die vorgeschlagenen Änderungen der Schweizer Überwachungsgesetze abzulehnen und die Werte der Privatsphäre, der Demokratie und der Menschenrechte, die für unsere Gesellschaft grundlegend sind, zu verteidigen.

Ich danke Ihnen für die Berücksichtigung meiner Ansichten zu diesem wichtigen Thema.

Mit freundlichen Grüissen

Michael Jung

Digitale Gesellschaft, CH-4000 Basel

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
CH-3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Basel, 2. Mai 2025

Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat Beat Jans
Sehr geehrte Empfänger:innen

Am 29. Januar 2025 eröffnete der Bundesrat die Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF). Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Vorentwurf wie folgt Stellung:

Vorbemerkung

Die geplante Revision der VÜPF ist ein Frontalangriff auf unsere Grundrechte, die Rechtsstaatlichkeit sowie den IT- und Innovationsstandort Schweiz.

Mit ihrer Umsetzung würde geltendes Recht in einem Ausmass verletzt, das alarmieren muss: Die Revision ist in vielerlei Hinsicht unvereinbar mit dem Bundesgesetz betreffend die Überwachung des

Post- und Fernmeldeverkehrs (BÜPF), verstösst gegen das Datenschutzgesetz (DSG), steht in klarem Widerspruch zu den verfassungsmässigen Grundrechten und verstösst gegen Völkerrecht. Die vorgesehenen Änderungen führen zu einer massiv ausgeweiteten Überwachung – ganz grundsätzlich und flächendeckend. Dies ist mit der Ausrichtung des BÜPF, das eine fein austarierte Interessenabwägung zwischen Freiheit und Privatsphäre einerseits und Sicherheit durch Überwachungsmassnahmen andererseits verfolgt, absolut nicht vereinbar.

Die Auswirkungen auf den Wirtschafts- und Innovationsstandort Schweiz wären verheerend: Die Ausweitung der Überwachung und die damit verbundenen, übermässigen Mitwirkungspflichten machen die Schweiz für IT-Anbieter äusserst unattraktiv. Renommierte Unternehmen wie Proton oder Threema, deren Geschäftsmodelle durch die Vorlage direkt ins Visier geraten, würden in ihrer Existenz bedroht. Die ersten Konsequenzen sind bereits sichtbar: Proton hat angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen (siehe [Tages-Anzeiger vom 1. April 2025](#)). Der Chef des Unternehmens erklärte in einem Interview: «Diese Entscheidung ist wirtschaftlicher Selbstmord für die Schweiz» ([watson.ch vom 9. April 2025](#)). Ähnlich äussert sich Threema-Chef Robin Simon: «Der Wirtschaftsstandort würde durch die Revision geschwächt und für Tech-Start-ups unattraktiv.» Aktuell lasse sich Threema alle Optionen offen ([Tages-Anzeiger vom 8. April 2025](#)). Diese Warnzeichen sind ernst zu nehmen und zeigen das verheerende Ausmass der geplanten Revision.

Neben den verheerenden wirtschaftlichen Auswirkungen wird gleichzeitig der grundrechtlich garantierte Anspruch auf sichere und vertrauliche Kommunikation ausgehöhlt. Wenn Anbieterinnen abwandern, bleibt jedoch – als wäre dies nicht genug – nicht nur privaten Nutzer:innen der Zugang zu geschützten Kommunikationsmitteln verwehrt.

Ebenso betroffen sind auch Personen, die einem Berufsgeheimnis unterstehen, wie Journalistinnen oder Anwälte. Die Änderungen treffen zudem schutzbedürftige Personengruppen besonders hart: Whistleblower:innen, Menschen mit ungeklärtem Aufenthaltsstatus oder ohne Papiere aber auch Aktivist:innen verlieren ebenso den Zugang zu vertraulichen Kommunikationsmitteln. Die Revision ignoriert diese Schutzbedürfnisse und erweitert stattdessen die Eingriffsbefugnisse des Staates in einer Weise, die hochgefährlich ist.

Besonders widersprüchlich erscheint das Vorgehen des Bundes angesichts der Tatsache, dass ausgerechnet der Bundesrat selbst Threema als Messenger nutzt – ein Dienst, den er nun faktisch aus dem Markt drängt. Damit sägt die Regierung ausgerechnet an jenem Ast, auf dem sie in Sachen sicherer Kommunikation bislang selbst sitzt.

Hinzu kommt: Die geplanten Regelungen sind technisch unausgereift, unnötig komplex und in Teilen schlüssig nicht umsetzbar. Vielmehr wird ein kaum noch durchschaubares Normengeflecht geschaffen, das weder den Mitwirkungspflichtigen noch den Betroffenen ein Mindestmass an Rechtsklarheit bietet. Die Revision wird ausserdem präsentiert, als handle es sich dabei um Änderungen zur besseren Überblickbarkeit der Rechtslage und zur Schaffung von mehr Rechtssicherheit - tatsächlich aber wird der persönliche Anwendungsbereich der Mitwirkungspflichtigen enorm erweitert und eine Vielzahl neuer Anbieterinnen in den Kreis der Mitwirkungspflichtigen einbezogen. Von Transparenz kann nicht die Rede sein.

Es ist im Übrigen nicht haltbar, dass eine dermassen breit angelegte Ausweitung von Pflichten auf Verordnungsstufe angelegt wird. Solch einschneidende Veränderungen mit weitreichenden Konsequenzen sind in Gesetzesform zu erlassen. Der Bundesrat überschreitet seine Kompetenzen hier um ein Weites.

Diese Vorlage schwächt nicht nur den Innovations- und Wirtschaftsstandort Schweiz – sie untergräbt gleichzeitig im grossen Stil verfassungsmässig geschützte Rechte. Aus grundrechtlicher, datenschutzrechtlicher und gesellschaftspolitischer Sicht ist sie schlicht inakzeptabel. Die geplanten Änderungen stehen dem erklärten Ziel von mehr Freundlichkeit sowie allgemeinen rechtsstaatlichen Grundsätzen sowie Schutzbedürfnissen Einzelner diametral entgegen.

Deshalb lehnen wir die Revision vollumfänglich und in aller Deutlichkeit ab.

Bemerkungen zu einzelnen Artikeln der VÜPF

Alle Artikel

Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung (Art. 6 Abs. 3 DSG) gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kund:innen auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.

Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.ä. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.

Antrag: Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.

Art. 16b Abs. 1

Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile (Art. 16b Abs. 1 lit. b Ziff. 2 VE-VÜPF) wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Mitwirkungspflichten in Kauf nehmen.

Dazu kommt, dass das Kriterium bezüglich der Überwachungsaufträge nicht vom BÜPF gestützt wird, denn: Die Anzahl von Überwachungsaufträgen ist von der wirtschaftlichen Bedeutung einer FDA völlig losgelöst. Die wirtschaftliche Bedeutung ist aber gemäss Art. 26 Abs. 6 BÜPF ausschlaggebend dafür, ob eine FDA von den vollen Pflichten (teilweise) befreit werden kann. Im Umkehrschluss ist die wirtschaftliche Bedeutsamkeit somit Erfordernis für die Auferlegung von vollen Pflichten. Wenn eine FDA nun aber rein aufgrund einer bestimmten Anzahl von Überwachungsaufträgen nach Art. 16b Abs. 1 lit. b Ziff. 1 VE-VÜPF als vollpflichtige FDA qualifiziert wird, steht dies im Widerspruch zum BÜPF und entbehrt damit einer Rechtsgrundlage.

Dieses bereits in der aktuellen Version der VÜPF vorhandene Problem sollte im Zuge einer Revision nicht bestehen bleiben, sondern muss behoben werden.

Antrag: Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter

Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.» Es ist auf die Regelung in Art. 26 Abs. 6 BÜPF abzustellen und eine Einzelfallbetrachtung zur Einstufung vorzunehmen.

Art. 16c Abs. 3

Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als «natürliche» Schutzmechanismen gegen eine übermässige oder missbräuchliche Nutzung solcher Massnahmen durch die Untersuchungsbehörden. Die automatisierte Erteilung von Auskünften ist unverhältnismässig und widerspricht dem Prinzip der Datenminimierung. Die pauschale und undifferenzierte Regel beeinträchtigt zwangsläufig den Grundrechtsschutz.

Der vorgesehene Umsetzungszeitraum von 12 Monaten zur Umsetzung eines dermassen komplexen Systems ist ausserdem völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.

Antrag: Streichung von lit. a «automatisierte Erteilung der Auskünfte» (ebenso in Art. 18 Abs. 2).

Art. 16d

Gemäss erläuterndem Bericht stellen Kommunikationsdienste, die nicht zu den in Art. 16a Abs. 1 aufgezählten Fernmeldediensten gehören und auf die die Ausnahmen nach Art. 16a Abs. 2 nicht zutreffen, abgeleitete Kommunikationsdienste dar. Diese klarere Definition des Begriffs AAKD ist begrüssenswert, doch ist die Konkretisierung der abgeleiteten Kommunikationsdienste im erläuternden Bericht einerseits rechtsstaatlich problematisch und andererseits geht die neue Auslegung nach den Ausführungen im erläuterndem Bericht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdielen wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter etc.) genutzt werden.

Art. 2 lit. c BÜPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft jedoch auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug in die Auslegung unrechtmässig ist – auch hier setzt sich die Revision inakzeptabel über die gesetzlichen Vorgaben des BÜPF hinweg. Onlinespeicherdielen sind deshalb aus Art. 16d zu streichen.

Zudem anerkennt der erläuternde Bericht zwar, dass VPNs zur Anonymisierung der Nutzer:innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil angebrachte Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Das Bedürfnis, auch künftig VPN-Dienste in Anspruch nehmen zu können, ist zu schützen und darf nicht vereitelt werden. Anbieter von VPNs sind daher ebenfalls aus Art. 16d auszunehmen.

Es ist irritierend, dass die bewusst separat ausgestalteten Kategorien AAKD und FDA einander zunehmend angeglichen werden, und zwar zuungunsten der AAKD, die als Kategorie mit grundsätzlich weniger weitreichenden Pflichten als die FDA konzipiert wurde. Dies missachtet den Willen des Gesetzgebers, den es zu wahren gilt.

Antrag: Streichung von Onlinespeicherdiensten und VPN-Anbieterinnen aus der Aufzählung der möglichen abgeleiteten Kommunikationsdienste in den Ausführungen zu Art. 16d im erläuternden Bericht und in der Auslegung.

Art. 16e, Art. 16f und Art. 16g

Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch komplett entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung mit deutlich erweiterten Pflichten. Entscheidend ist, dass neuerdings das Kriterium von 5'000 Nutzer:innen allein zum Auferlegen massiver Überwachungspflichten ausreicht: Erreicht eine AAKD diese Grösse, fällt sie neu in die Kategorie der AAKD mit reduzierten Pflichten und untersteht somit bereits sehr weitgehenden Mitwirkungspflichten, insbesondere der Identifikationspflicht.

Die Einführung von 5'000 Nutzer:innen als gesondert zu beurteilende Untergrenze verletzt Art. 27 Abs. 3 BÜPF, denn 5'000 Personen sind keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strengereren Überwachungsmassnahmen, gerechtfertigt wären. 5'000 Nutzer:innen werden in der digitalen Welt vielmehr sehr rasch erreicht – die Revision verkennt technische Realitäten.

Zusätzlich führt das Einführen eines Konzernatbestandes in Art. 16f Abs. 3 zu massiven Problemen: Produkte und Dienste müssen nicht mehr für sich allein bestimmte Schwellenwerte erreichen – es genügt, wenn das Mutterunternehmen oder verbundene Gesellschaften diese überschreiten. Insbesondere bei Unternehmen mit Beteiligungsstrukturen führt dies dazu, dass sämtliche Angebote pauschal der höchsten Überwachungsstufe unterstellt werden – unabhängig davon, ob sich einzelne Dienste noch im frühen Entwicklungsstadium befinden oder faktisch kaum genutzt werden. Somit müsste jedes neue Projekt von Beginn an mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden, was Innovation behindert. Zudem missachtet der Konzernatbestand das Verhältnismässigkeitsgebot: Unterschiedliche organisatorische Einheiten mit eigenständigen Angeboten werden unrechtmässig zusammengefasst, obwohl sie individuell zu prüfen wären. Die Anwendung starrer Schwellen auf ganze Konzerne statt auf einzelne Dienste umgeht eine notwendige Einzelfallprüfung.

Eine solche Regelung stünde sodann *im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali*, das die zu seltene Anwendung von Downgrades kritisierte:

«Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»

Statt KMU zu entlasten, führt die Revision neu zu einem «automatischen» *Upgrade per Verordnung ohne Verfügung* (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.

Eine Analyse der offiziellen VÜPF-Statistik unterstreicht diese offensichtliche Unverhältnismässigkeit. Im Jahr 2023 betrafen 98,97% der total 9'430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,03% für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,74% wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100% des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.

Die neue Vorlage schliesst nun ebenfalls sowohl die Registrierung via normaler E-Mail als auch die komplett anonyme Registrierung (z. B. Signal oder Telegram) aus, da AAKD bereits mit reduzierten Pflichten neu automatisch zwingend die Endnutzer:innen identifizieren müssen. Hiervon betroffen sind nicht nur alle AAKD mit reduzierten Pflichten, sondern auch all deren Wiederverkäufer. Faktisch resultiert das Gesetz somit darin, dass man sich bei keinem Dienst mehr anmelden können soll, ohne den Pass, Führerschein oder die ID entweder direkt oder indirekt zu hinterlegen. Dass Nutzer:innen künftig hierzu gezwungen wären, stellt einen massiven Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 BV) dar und ist unzumutbar.

Ein weiteres Kernproblem, das die automatische Hochstufung mit sich bringt, ist die Rechtsunsicherheit. Die Vorlage will mit klarer definierten Kategorien und Pflichten ein übersichtlichere Situation schaffen, verfehlt dieses Ziel jedoch gänzlich. Bislang fand die Hochstufung per Verfügung statt, wodurch es für die Mitwirkungspflichtigen klar erkennbar war, wann sie unter welche Pflichten fallen. Ausserdem bewirkt diese Praxis eine sinnvolle Einzelfallbetrachtung anstelle pauschaler und unzweckmässiger automatischer Hochstufungen. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den massgebenden Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes kann aber im Zweifelsfall nur schwer zu beantworten sein. Gerade deshalb besteht ein schutzwürdiges Interesse der Anbieter an Klarheit über ihre Pflichten, da sie fortan eventuell die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Diese Umstrukturierung lässt ich nicht mit der Funktionsweise von Verwaltungsverfahren vereinbaren. Die Pflicht zur Abklärung, wann eine Hochstufung vorliegt und was diese für das Unternehmen bedeutet, darf nicht in die Verantwortung der Unternehmen fallen. Der Staat zieht sich hier aus der Verantwortung und schiebt diese den Unternehmen zu, wodurch diesen zwangsläufig zeitlicher und finanzieller Mehraufwand entsteht. Von einer automatischen Hochstufung von AAKD ist daher abzusehen.

Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.

Gegenüber der geltenden VÜPF *erweitert die Revision die Pflichten zur Automatisierung noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragetypen wie z. B. "IR_59" und "IR_60", welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen.* Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.

Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 lit. b der geltenden VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grosse[n] Teil ihrer

Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. *Damit fallen auch Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz.*

Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Auch hiermit werden neue Hürden für Innovation geschaffen. Die Regelung ist unverhältnismässig und nicht sachdienlich.

Auch Non-Profit-Organisationen geraten unter die verschärften Vorgaben. Unter den neuen Kriterien wird aber allein auf die Anzahl der Nutzer:innen abgestellt für die Einstufung als AAKD. Dieses Kriterium greift jedoch zu kurz: Es berücksichtigt insbesondere nicht die wirtschaftliche Tragfähigkeit der Anbieter:innen. Gerade bei Open-Source- und Non-Profit-Lösungen mit grosser Reichweite, aber geringem Budget, führt dies zu einer verheerenden finanziellen Belastung: Anbieter:innen mit solchen Projekten würden gezwungen, umfangreiche Überwachungsmassnahmen einzuführen. Solche Anbieter:innen würden gezielt aus dem Schweizer Markt gedrängt, während gleichzeitig bestehende Monopole wie WhatsApp (96% Marktanteil in der Schweiz) gestärkt würden.

Es muss ausserdem klar festgehalten werden, dass sich das BÜPF und die VÜPF nur auf Anbieter:innen beziehen können, die in der Schweiz tatsächlich tätig sind. Die Erlasse dürfen nicht so ausgelegt werden, dass sie eine extraterritoriale Wirkung entfalten und internationale Dienste wie Signal, WhatsApp oder Microsoft Teams erfasst sind.

Das Kriterium der reinen Nutzer:innenzahl ist ungeeignet und muss gestrichen werden.

Die Regelung schwächt auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade us-amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger:innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, End-zu-End-verschlüsselter Kommunikation ist heute wichtiger denn je und fällt in den Bereich grundrechtlich geschützter Ansprüche, die es zu wahren gilt. Diese Ansprüche dürfen nicht aufs Spiel gesetzt werden, um ein knallhartes Überwachungsregime der Kommunikation in der Schweiz durchzusetzen – die Prioritäten werden höchst fragwürdig gesetzt.

Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade illegal ist (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer:innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, diese zu erhebenden Datenmengen sind von enormem Ausmass und bergen folglich massive Risiken für Hackerangriffe.

Des Weiteren ist nicht belegt, dass die Speicherung der betreffenden Daten zu spürbar mehr erfolgreichen Ermittlungen führt. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisshandlung via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfüge, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.

Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren. Diese Handhabe bedeutet einen Verstoss gegen das Legalitätsprinzip und untergräbt legislative Kompetenzen. Ausserdem verfügt die Schweiz bereits über reichlich Mittel zur Aufklärung und Verfolgung von Straftaten, die Behörden können bereits heute auf sicherheitsrelevante Daten zurückgreifen. Unternehmen wie Proton (s. «Positionspapier zur Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)» von Proton) kooperieren seit Jahren mit den Schweizer Strafverfolgungsbehörden und dem Nachrichtendienst des Bundes (NDB). Wenn nun solche Unternehmen aus bereits genannten Gründen zur Abwanderung gezwungen werden, bewirkt die Revision auch hier das genaue Gegenteil ihrer erklärten Ziele: Anstatt der Schaffung besserer Möglichkeiten zur Strafverfolgung würden die Schweizer Behörden wie etwa Fedpol den Zugriff auf wichtige Partner bei der Beschaffung sicherheitsrelevanter Daten verlieren.

Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Integrität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.

Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das DSG. Der Entwurf bringt nicht, wie der Begleitbericht den Leser:innen weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit, steht in direktem Gegensatz zum besagten Postulat 19.4031 und bedeutet massive Eingriffe in grundrechtlich geschützte Sphären, sowohl von Unternehmen als auch von Nutzer:innen.

Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen und das bestehende System muss beibehalten werden.

Antrag: Streichung der Artikel und Beibehaltung der bestehenden Kriterien und der zwei Kategorien von AAKD. + Ausnahmen für Pilotprojekte (auch von grossen Firmen) und Non-Profits per se. Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).

Art. 16h

Art. 16h konkretisiert die Kategorie der «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» aus Art. 2 lit. e BÜPF. Die Vorschrift verfehlt ihr Ziel – anstatt Unsicherheiten darüber zu beheben, wer unter diese Kategorie fällt, schafft sie weitere Unklarheiten. Der schwammig formulierte Verordnungstext könnte dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist:innen, Whistleblower:innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber:innen solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer:innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen.

Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt. Die Unklarheit bezüglich der Einordnung von TOR-Servers wirft weitere Fragen auf, denn wenn TOR nicht als PZD zu qualifizieren

ist, müsste TOR – gleich wie die VPNs – der Kategorie der AAKD zugeordnet werden. Somit stünden Betreiber:innen von TOR-Servern – wie etwa die Digitale Gesellschaft – unter der Identifikationspflicht. Diese ist jedoch, wie dargelegt, nicht umsetzbar.

Es braucht somit entweder die Zusicherung, dass Betreiberinnen von TOR-Nodes nicht dem BÜPF und der VÜPF unterstellt sind oder aber Kategorien von Mitwirkungspflichten, die so gestaltet sind, dass ein:e Betreiber:in eines TOR-Nodes nicht einer Identifikationspflicht unterstellt wird – z. B. indem die Schwelle für das Auferlegen der Identifikationspflicht auf 1 Mio. Nutzer:innen angehoben wird.

Wären Betreiber:innen von TOR-Nodes von der Identifikationspflicht erfasst, würde dies fundamentale Grundrechte wie das Recht auf Privatsphäre und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK), die Meinungs- und Informationsfreiheit (Art. 16 BV, Art. 10 EMRK) gefährden. Ebenso würde das datenschutzrechtliche Prinzip der Datensicherheit (Art. 8 DSG) komplett unterlaufen. Diese Eingriffe in national und international geschützte Rechtsansprüche sind nicht hinzunehmend.

Dieser potentielle Angriff auf die genannten Grundrechte ist hochproblematisch und setzt ein politisches Statement: Die Schweiz bewegt sich weg von Grundrechtsschutz hin zum hochgerüsteten Überwachungsstaat.

Antrag: Es muss sichergestellt werden, dass Technologien wie TOR oder I2P nicht vom Anwendungsbereich der VÜPF erfasst sind.

Art. 16h Abs. 2

Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Endbenutzer:innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 VE-VÜPF: Gemäss diesem Artikel trägt die das WLAN erschliessenden FDA die Verantwortung zur Identifikation der Nutzer:innen. Die Regelung führt also dazu, dass FDA, die einen Vertrag haben mit «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» (PZD), sehr schnell für die Identifikation der Endnutzer:innen ihrer Vertragspartner zuständig sind. Diese Regelung ist unsinnig und schlicht nicht umsetzbar.

Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer:innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24), die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22) oder der Verwendung von IPv6. Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDA unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden.

Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten: FDA resp. Anbieterinnen von öffentlichen WLAN-Zugängen dürfen nur unter einer Identifikationspflicht stehen, wenn die PZD, die den Zugang der FDA nutzt, «professionell betrieben» ist – und zwar nach der aktuellen Auslegungsform (s. Erläuternder Bericht zur (letzten)Totalrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs):

«Mit «professionell betrieben» ist gemeint, dass eine FDA oder eine auf öffentliche WLAN-Zugangspunkte spezialisierte IT-Dienstleisterin den technischen Betrieb des öffentlichen WLAN-

Zugangspunktes durchführt, die dies auch noch für andere öffentliche WLAN-Zugangspunkte an anderen Standorten macht. Wenn eine natürliche oder juristische Person an ihrem Internetzugang selbst einen öffentlichen WLAN-Zugangspunkt technisch betreibt und diesen Zugang Dritten zur Verfügung stellt, muss die FDA, die den Internetzugang anbietet, keine Identifikation der Endbenutzenden sicherstellen.»

So wird sichergestellt, dass FDA nicht unmöglich umzusetzenden Pflichten unterstellt werden.

Antrag: Streichung der Ausführung im erläuternden Bericht. Das Kriterium «professionell betrieben» ist nach der bislang geltenden Regelung zu verstehen. Art. 16h Abs. 2 ist ersatzlos zu streichen und im Zusammenhang mit Art. 19 Abs. 2 ist auf die aktuelle Definition von «professionell betrieben» abzustellen.

Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2

Bei Konzernen knüpft die VE-VÜPF nicht mehr an die Umsatz- und Nutzer:innenzahlen des betroffenen Unternehmens an, neu sind die Zahlen des Konzerns ausschlaggebend für eine Hoch- oder Herunterstufung. Die Begründung, dies diene der Vereinfachung, ist unlogisch und irreführend: Unternehmen müssen ihre Zahlen ohnehin produktbezogen ausweisen, die nötigen Daten liegen also längst vor. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.

Antrag: Streichung des «Konzernatbestand» und Beibehaltung der bestehenden Regelung.

Art. 19 Abs. 1

Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD – erfasst sind die AAKD mit reduzierten und mit vollen Pflichten – widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht. Durch die neuen Schwellenwerte zur Einstufung findet eine beachtliche Ausweitung der Identifikationspflicht statt.

Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des DSG, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch insbesondere der Grundrechtsschutz von Nutzer:innen in der Schweiz massiv beeinträchtigt wird. Die Identifikationspflicht greift immens in das Recht auf informationelle Selbstbestimmung ein und hält einer Grundrechtsprüfung nach Art. 36 BV schon allein aufgrund ihrer Unverhältnismässigkeit nicht stand.

Bezüglich einschneidender Pflichten, die potentiell schwere Grundrechtseingriffe bedeuten – wie es bei Identifikationspflichten zweifellos der Fall ist – muss Rechtsetzung in jedem Fall mit äusserster Sorgfalt und unter strenger Beachtung des Verhältnismässigkeitsgebots erfolgen. Außerdem darf sich eine solche Pflicht nicht über gesetzliche Vorgaben, wie in diesem Fall vom BÜPF vorgegeben, hinwegsetzen.

Durch die breite Auferlegung einer solchen Pflicht werden datenschutzfreundliche Unternehmen bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird. Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Nur so können datenschutzrechtliche Vorgaben und die Rechte Betroffener gewahrt werden.

Antrag: Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation von Teilnehmenden.

Art. 18

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 19 Abs. 2

Das Kriterium «professionell betrieben» ist nach der bestehenden Regelung auszulegen (s. vorstehen). Es sei ausserdem darauf hingewiesen, dass sich aus dieser Regelung eine vertragsrechtliche Problematik zwischen den FDA und den PZD ergeben würde, die nicht tragbar ist.

Antrag: Auslegung des Kriteriums «professionell betrieben» nach der bestehenden Regelung und nicht i. S. v. Art. 16h Abs. 2.

Art. 21 Abs. 1 lit. a

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.

Antrag: Streichung

Art. 22

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.

Antrag: beibehalten

Art. 11 Abs. 4

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.

Antrag: Streichung

Art. 16b

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.

Antrag: Streichung

Art. 31 Abs. 1

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 51 und 52

Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.

Antrag: beibehalten

Art. 60a

Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde laut den Erläuterungen bewusst auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten. Art. 60a ist zu streichen.

Antrag: Streichung des Artikels

Art. 42a und 43a

Die Art. 42a und 43a führen neu die Abfragetypen «IR_59» und «IR_60» ein, über die sensible Daten automatisiert abgefragt werden können. Sie verlangen von Anbietern, dass sie jederzeit Auskunft geben können bezüglich des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Auch für das Auferlegen dieser Pflicht gilt die fragliche Schwelle von 5'000 Nutzer:innen. Erfasst ist somit nahezu die gesamte AAKD-Landschaft der Schweiz.

Das Problem liegt darin, dass die «IR_»-Abfragen zu Informationen nach Art. 42a und 43a neu automatisiert abgerufen werden können – im Gegensatz zu den «HD_»- (historische Daten) und «RT»- (Echtzeitüberwachung) Abfragen, die strengeren Regeln und einer juristischen Kontrolle unterliegen.

Bei den «IR_59»- und «IR_60»-Abfragen handelt es sich allerdings um sensible Informationen wie etwa das Abrufen einer IP-Adresse. Solche Informationen mussten bislang zurecht über strengere Abfragetypen eingeholt werden. Es ist nicht nachvollziehbar, warum Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber. Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser automatisierten Auskünfte ergibt. Unternehmen sind daher nur unzulänglich geschützt vor missbräuchlichen Anfragen und vor Kosten, die ihnen durch die Pflicht, diese Auskünfte automatisch weiterzugeben, entstehen wird.

Künftig könnten so umfangreiche Informationen über die neuen Abfragetypen beschafft werden, die bislang zurecht den strengerem Regeln der rechtlich sichereren Informations-/Überwachungstypen «HD_» und «RT_» unterworfen waren. «IR_59» und «IR_60» ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne den erforderlichen Kontrollen dieser invasiven Überwachungstypen unterworfen zu sein.

Die Entwicklung, dass mittels «IR_»-Abfragen neu auch personenbezogene sensible Nutzungsdaten eingeholt werden können, widerspricht der Logik der unterschiedlichen Abfragetypen und öffnet Tür und Tor für missbräuchliche Abfragen und eine Echtzeitüberwachung von Millionen von Nutzer:innen. Auch hier stehen grundrechtlich geschützte Ansprüche auf dem Spiel, die mit einer solchen Regelung auf nicht nachvollziehbare Weise untergraben und missachtet werden.

Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind. Die AAKD müssten künftig gewisse Datenkategorien systematisch erheben, um dieser Pflicht nachzukommen. Art. 27 Abs. 2 BÜPF erklärt allerdings, dass AAKD «auf Verlangen die *ihnen zur Verfügung stehenden* Randdaten des Fernmeldeverkehrs der überwachten Person liefern» müssen. Bei einer dahingehenden Auslegung des Bestimmungen bedeutete dies einen weiteren Verstoss gegen das BÜPF.

Unter rechtsstaatlichen Gesichtspunkten gilt es ausserdem die geplante Schwächung der Institution des Zwangsmassnahmengerichts auf das Schärfste zu kritisieren. Mit der Schaffung der zwei neuen Auskunftstypen, die mittels einfacher Auskunftsanfrage automatisch abgerufen werden können, werden rechtliche Kontrollmechanismen wie das Zwangsmassnahmengericht umgangen und der Einflussbereich der Staatsanwaltschaft noch weiter ausgebaut. Art. 42a und 43a sind daher vollumfänglich zu streichen.

Antrag: Streichung der Artikel

Art. 50a

Art. 50a sieht vor, dass Anbieter:innen verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Auch diese Pflicht soll eine Vielzahl neuer Unternehmen erfassen: Betroffen sind nicht mehr nur FDA (Art. 26 BÜPF) und ausnahmsweise AAKD (Art. 27 BÜPF), sondern sämtliche Anbieter:innen mit mehr als 5'000 Nutzer:innen. Im Ergebnis wäre fast die gesamte Schweizer AAKD-Branche betroffen (kaum ein Produkt ist lebensfähig mit weniger als 5'000 Teilnehmer:innen).

Die Ausdehnung dieser Pflicht auf AAKD stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar: Es findet keine Einzelfallprüfung statt und die AAKD werden dieser Pflicht unterworfen, auch wenn sie keineswegs «Dienstleistungen von grosser

wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten», was jedoch gesetzliche Vorgabe ist (Art. 27 Abs. 3 BÜPF).

Problematisch ist zudem, dass aufgrund dieser Vorgabe Anbieter:innen ihrer Verschlüsselungen so konfigurieren müssen, dass sie von ihnen aufgehoben werden können – eine durch Anbieter:innen aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung allerdings in jedem Fall. Dies führt zu schwächeren Verschlüsselungen und der Abnahme der Sicherheit von Kommunikationsdiensten.

Daraus ergibt sich eine Grundrechtsproblematik von erheblicher Tragweite: Das Verhältnismässigkeitsgebot aus Art. 36 BV kann nicht eingehalten werden, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Die Interessenabwägung darf hier nicht zuungunsten der Grundrechtsträger:innen erfolgen, da es sich bei deren Interessen um solche von fundamentalem Gewicht – dem Zugang zu sicherer Kommunikation und damit direkt verbunden dem Recht auf freie Meinungsäusserung – handelt.

Wichtig ist, dass Verschlüsselungen, die auf dem Endgerät der Nutzer:innen erfolgen – also End-zu-End-Verschlüsselungen – nicht unter die Pflicht zur Aufhebung gemäss Art. 50a VE-VÜPF fallen dürfen. Diese Form der Verschlüsselung liegt ausschliesslich in der Sphäre der Nutzer:innen und es wäre untragbar, die Pflicht zur Aufhebung von Verschlüsselungen in dieser Sphäre zu verlangen. Die Anbieter:innen dürfen daher nicht dazu verpflichtet werden, diese Inhalte zu entschlüsseln und zugänglich zu machen. Im Gegensatz dazu betrifft die Transportverschlüsselung «lediglich» die Verbindung zwischen Client und Server und kann von Anbieter:innen kontrolliert werden. Es ist wichtig, dass diese technischen Unterscheidungen und unterschiedlichen Schutzwirkungen und -richtungen bei rechtlichen Umsetzungen beachtet werden. Wir begrüssen die Klarstellung im erläuternden Bericht, dass die End-zu-End-Verschlüsselung vom Anwendungsbereich ausgenommen ist. Es muss jedoch ebenso klar sein, dass das ganze Endgerät von Nutzer:innen aus dem Anwendungsbereich von Art. 50a VE-VÜPF ausgenommen ist.

Es braucht im Übrigen auch eine Klarstellung darüber, dass eine rückwirkende Möglichkeit zur Aufhebung klar ausgeschlossen ist. Eine solche würde de facto eine Vorratsdatenspeicherung verschlüsselter Inhalte und Keys darstellen, die mit dem Prinzip der Datenminimierung (Art. 6 Abs. 3 DSG) und dem Schutz der Privatsphäre (Art. 13 BV) unvereinbar ist.

Antrag: Streichung der «Anbieterin mit reduzierten Pflichten» aus dem Anwendungsbereich sowie eine Klarstellung darüber, dass die Aufhebung von Verschlüsselungen auf dem Endgerät der Nutzer:innen sowie eine rückwirkende Verpflichtung zur Aufhebung ausgeschlossen sind.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Art. 14 Abs. 3 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und wirtschaftlich nicht tragbar, was das Einführen von Fristen obsolet werden lässt. Der Absatz ist daher ersatzlos zu streichen.

Antrag: Streichung

Art. 14 Abs. 4 VD-ÜPF

Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der Unterworfenen AAKD – da auch AAKD mit reduzierten Pflichten erfasst sind – massiv. Dies ist wie bereits ausgeführt weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.

Antrag: Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten»

Art. 20 Abs. 1 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen, ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.

Antrag: Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»

Schlussbemerkung

Trotz des Umfangs dieser Stellungnahme gilt: Das Ausbleiben einer expliziten Bemerkung zu einzelnen Bestimmungen bedeutet keine Zustimmung der Digitalen Gesellschaft. Die Ablehnung der Revision bleibt volumnäiglich bestehen.

Freundliche Grüsse

Erik Schönenberger
Geschäftsleiter

Von: Julija Zivkovic

Gesendet: Montag, 5. Mai 2025 20:10:14 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Vernehmlassungsantwort zur Teilrevision der VÜPF und VD-ÜPF

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
CH-3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

5. Mai 2025, Zürich

Vernehmlassungsantwort zur Teilrevision der VÜPF und VD-ÜPF

Sehr geehrte Damen und Herren,

mit dieser Vernehmlassungsantwort möchte ich meine klaren Bedenken gegenüber der geplanten Teilrevision der VÜPF und VD-ÜPF zum Ausdruck bringen.

Die vorgeschlagenen Änderungen würden eine erhebliche Ausweitung der Überwachungsbefugnisse in der Schweiz bedeuten – und das, obwohl ein ähnlicher Versuch durch ein Merkblatt bereits vom Bundesgericht als rechtswidrig eingestuft wurde. Nun soll dasselbe Ziel über eine Verordnungänderung erreicht werden – ohne parlamentarische Debatte oder Möglichkeit eines Referendums. Dieses Vorgehen halte ich in einem demokratischen Rechtsstaat für höchst problematisch.

Die Stellungnahme der Digitalen Gesellschaft Schweiz vom 2. Mai 2025 (<https://www.digitale-gesellschaft.ch/2025/05/02/bundesrat-will-ueberwachungsstaat-per-verordnung-massiv-ausbauen-stellungnahme-zur-teilrevision-vuepf-und-vd-uepf/>) zeigt auf, dass der Entwurf grundlegende rechtliche Prinzipien verletzt – insbesondere die Bundesverfassung sowie die Europäische Menschenrechtskonvention (EMRK). Ich teile diese Einschätzung vollumfänglich.

Roger Gantner

[REDACTED]

[REDACTED]

ecip@gmx.com

Flums, 5. Mai 2025

Fernmeldeüberwachung und mitwirkungspflichtige Unternehmen

Sehr geehrte Damen und Herren

Mit grossem Unbehagen habe ich von der Fernmeldeüberwachung und der damit verbundenen Mitwirkungspflicht für Unternehmen Kenntnis genommen. Solche Massnahmen greifen in die Privatsphäre unbescholtener Bürger ein und untergraben grundlegende Prinzipien eines freiheitlichen Rechtsstaates.

Der Staat hat weder das Recht noch die moralische Legitimation, sich in die vertrauliche Kommunikation von Individuen einzumischen, solange kein konkreter und rechtsstaatlich begründeter Verdacht besteht.

Die flächendeckende oder präventive Überwachung ist ein gefährlicher Schritt in Richtung Überwachungsstaat und widerspricht demokratischen Grundwerten.

Ich lehne diese Entwicklung entschieden ab und fordere eine Rückbesinnung auf den Schutz der persönlichen Kommunikationsfreiheit.

Mit freundlichen Grüßen

Roger Gantner

Von: Andrey Moine
Gesendet: Montag, 5. Mai 2025 20:29:06 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Vernehmlassungsantwort zur Änderung der VÜPF und VD-ÜPF

Guten Tag

Gerne informiere ich Sie über das PDF im Anhang, welches Ihnen vermutlich bereits mehrmals zugestellt wurde und erläutern soll, warum die "Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)" und "Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)" kompletter Unfug im Namen der "Sicherheit" und nur ein Trick ist, um die Kompetenzen des Bundes auszuweiten.

Falls die Änderungen wie geplant umgesetzt werden, sollten die Politiker und der Bundesrat in Bern als erstes von dieser Änderung profitieren. Da sie nichts zu verbergen haben sollen, sollten sie (bzw. ihre Kommunikation) zu aller erst überwacht werden. Ihre Daten sollten der Öffentlichkeit zur Verfügung stehen, damit die Schweizer messen können, wie gut sie ihre Arbeit umsetzen. Ein fairer Deal.

Da sie vermutlich etwas dagegen haben werden, sollte die Verordnung mindestens wie anhand des PDFs umgesetzt werden. Ansonsten ist dies Doppelmoral auf höchster Ebene. Wenn nicht, wäre auch ein Wegzug von Unternehmen wie z.B. Proton denkbar:

<https://www.derbund.ch/andy-yen-gegen-revisionsplan-des-bundesrats-mit-dieser-aggressiven-ueberwachung-muesste-proton-die-schweiz-verlassen-487339556764>

Die ist nur ein Beispiel eines Unternehmens, und doch schwächt dies den Standort Schweiz, welcher international für starken Datenschutz bekannt ist.
Die Schweiz bekäme anderfalls ein zweites Grossbritannien, Australien oder als aktuelles Beispiel die USA, bei denen Recht keine Rolle spielt. Ist das das Ziel?

Weitere Infos können Sie hier abrufen:

<https://www.digitale-gesellschaft.ch/2025/05/02/bundesrat-will-ueberwachungsstaat-per-verordnung-massiv-ausbauen-stellungnahme-zur-teilrevision-vuepf-und-vd-uepf/>

Freundliche Grüsse

Digitale Gesellschaft, CH-4000 Basel

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
CH-3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Basel, 2. Mai 2025

Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat Beat Jans
Sehr geehrte Empfänger:innen

Am 29. Januar 2025 eröffnete der Bundesrat die Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF). Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Vorentwurf wie folgt Stellung:

Vorbemerkung

Die geplante Revision der VÜPF ist ein Frontalangriff auf unsere Grundrechte, die Rechtsstaatlichkeit sowie den IT- und Innovationsstandort Schweiz.

Mit ihrer Umsetzung würde geltendes Recht in einem Ausmass verletzt, das alarmieren muss: Die Revision ist in vielerlei Hinsicht unvereinbar mit dem Bundesgesetz betreffend die Überwachung des

Post- und Fernmeldeverkehrs (BÜPF), verstösst gegen das Datenschutzgesetz (DSG), steht in klarem Widerspruch zu den verfassungsmässigen Grundrechten und verstösst gegen Völkerrecht. Die vorgesehenen Änderungen führen zu einer massiv ausgeweiteten Überwachung – ganz grundsätzlich und flächendeckend. Dies ist mit der Ausrichtung des BÜPF, das eine fein austarierte Interessenabwägung zwischen Freiheit und Privatsphäre einerseits und Sicherheit durch Überwachungsmassnahmen andererseits verfolgt, absolut nicht vereinbar.

Die Auswirkungen auf den Wirtschafts- und Innovationsstandort Schweiz wären verheerend: Die Ausweitung der Überwachung und die damit verbundenen, übermässigen Mitwirkungspflichten machen die Schweiz für IT-Anbieter äusserst unattraktiv. Renommierte Unternehmen wie Proton oder Threema, deren Geschäftsmodelle durch die Vorlage direkt ins Visier geraten, würden in ihrer Existenz bedroht. Die ersten Konsequenzen sind bereits sichtbar: Proton hat angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen (siehe [Tages-Anzeiger vom 1. April 2025](#)). Der Chef des Unternehmens erklärte in einem Interview: «Diese Entscheidung ist wirtschaftlicher Selbstmord für die Schweiz» ([watson.ch vom 9. April 2025](#)). Ähnlich äussert sich Threema-Chef Robin Simon: «Der Wirtschaftsstandort würde durch die Revision geschwächt und für Tech-Start-ups unattraktiv.» Aktuell lasse sich Threema alle Optionen offen ([Tages-Anzeiger vom 8. April 2025](#)). Diese Warnzeichen sind ernst zu nehmen und zeigen das verheerende Ausmass der geplanten Revision.

Neben den verheerenden wirtschaftlichen Auswirkungen wird gleichzeitig der grundrechtlich garantierte Anspruch auf sichere und vertrauliche Kommunikation ausgehöhlt. Wenn Anbieterinnen abwandern, bleibt jedoch – als wäre dies nicht genug – nicht nur privaten Nutzer:innen der Zugang zu geschützten Kommunikationsmitteln verwehrt.

Ebenso betroffen sind auch Personen, die einem Berufsgeheimnis unterstehen, wie Journalistinnen oder Anwälte. Die Änderungen treffen zudem schutzbedürftige Personengruppen besonders hart: Whistleblower:innen, Menschen mit ungeklärtem Aufenthaltsstatus oder ohne Papiere aber auch Aktivist:innen verlieren ebenso den Zugang zu vertraulichen Kommunikationsmitteln. Die Revision ignoriert diese Schutzbedürfnisse und erweitert stattdessen die Eingriffsbefugnisse des Staates in einer Weise, die hochgefährlich ist.

Besonders widersprüchlich erscheint das Vorgehen des Bundes angesichts der Tatsache, dass ausgerechnet der Bundesrat selbst Threema als Messenger nutzt – ein Dienst, den er nun faktisch aus dem Markt drängt. Damit sägt die Regierung ausgerechnet an jenem Ast, auf dem sie in Sachen sicherer Kommunikation bislang selbst sitzt.

Hinzu kommt: Die geplanten Regelungen sind technisch unausgereift, unnötig komplex und in Teilen schlüssig nicht umsetzbar. Vielmehr wird ein kaum noch durchschaubares Normengeflecht geschaffen, das weder den Mitwirkungspflichtigen noch den Betroffenen ein Mindestmass an Rechtsklarheit bietet. Die Revision wird ausserdem präsentiert, als handle es sich dabei um Änderungen zur besseren Überblickbarkeit der Rechtslage und zur Schaffung von mehr Rechtssicherheit - tatsächlich aber wird der persönliche Anwendungsbereich der Mitwirkungspflichtigen enorm erweitert und eine Vielzahl neuer Anbieterinnen in den Kreis der Mitwirkungspflichtigen einbezogen. Von Transparenz kann nicht die Rede sein.

Es ist im Übrigen nicht haltbar, dass eine dermassen breit angelegte Ausweitung von Pflichten auf Verordnungsstufe angelegt wird. Solch einschneidende Veränderungen mit weitreichenden Konsequenzen sind in Gesetzesform zu erlassen. Der Bundesrat überschreitet seine Kompetenzen hier um ein Weites.

Diese Vorlage schwächt nicht nur den Innovations- und Wirtschaftsstandort Schweiz – sie untergräbt gleichzeitig im grossen Stil verfassungsmässig geschützte Rechte. Aus grundrechtlicher, datenschutzrechtlicher und gesellschaftspolitischer Sicht ist sie schlicht inakzeptabel. Die geplanten Änderungen stehen dem erklärten Ziel von mehr Freundlichkeit sowie allgemeinen rechtsstaatlichen Grundsätzen sowie Schutzbedürfnissen Einzelner diametral entgegen.

Deshalb lehnen wir die Revision vollumfänglich und in aller Deutlichkeit ab.

Bemerkungen zu einzelnen Artikeln der VÜPF

Alle Artikel

Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung (Art. 6 Abs. 3 DSG) gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kund:innen auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.

Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.ä. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.

Antrag: Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.

Art. 16b Abs. 1

Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile (Art. 16b Abs. 1 lit. b Ziff. 2 VE-VÜPF) wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Mitwirkungspflichten in Kauf nehmen.

Dazu kommt, dass das Kriterium bezüglich der Überwachungsaufträge nicht vom BÜPF gestützt wird, denn: Die Anzahl von Überwachungsaufträgen ist von der wirtschaftlichen Bedeutung einer FDA völlig losgelöst. Die wirtschaftliche Bedeutung ist aber gemäss Art. 26 Abs. 6 BÜPF ausschlaggebend dafür, ob eine FDA von den vollen Pflichten (teilweise) befreit werden kann. Im Umkehrschluss ist die wirtschaftliche Bedeutsamkeit somit Erfordernis für die Auferlegung von vollen Pflichten. Wenn eine FDA nun aber rein aufgrund einer bestimmten Anzahl von Überwachungsaufträgen nach Art. 16b Abs. 1 lit. b Ziff. 1 VE-VÜPF als vollpflichtige FDA qualifiziert wird, steht dies im Widerspruch zum BÜPF und entbehrt damit einer Rechtsgrundlage.

Dieses bereits in der aktuellen Version der VÜPF vorhandene Problem sollte im Zuge einer Revision nicht bestehen bleiben, sondern muss behoben werden.

Antrag: Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter

Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.» Es ist auf die Regelung in Art. 26 Abs. 6 BÜPF abzustellen und eine Einzelfallbetrachtung zur Einstufung vorzunehmen.

Art. 16c Abs. 3

Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als «natürliche» Schutzmechanismen gegen eine übermässige oder missbräuchliche Nutzung solcher Massnahmen durch die Untersuchungsbehörden. Die automatisierte Erteilung von Auskünften ist unverhältnismässig und widerspricht dem Prinzip der Datenminimierung. Die pauschale und undifferenzierte Regel beeinträchtigt zwangsläufig den Grundrechtsschutz.

Der vorgesehene Umsetzungszeitraum von 12 Monaten zur Umsetzung eines dermassen komplexen Systems ist ausserdem völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.

Antrag: Streichung von lit. a «automatisierte Erteilung der Auskünfte» (ebenso in Art. 18 Abs. 2).

Art. 16d

Gemäss erläuterndem Bericht stellen Kommunikationsdienste, die nicht zu den in Art. 16a Abs. 1 aufgezählten Fernmeldediensten gehören und auf die die Ausnahmen nach Art. 16a Abs. 2 nicht zutreffen, abgeleitete Kommunikationsdienste dar. Diese klarere Definition des Begriffs AAKD ist begrüssenswert, doch ist die Konkretisierung der abgeleiteten Kommunikationsdienste im erläuternden Bericht einerseits rechtsstaatlich problematisch und andererseits geht die neue Auslegung nach den Ausführungen im erläuterndem Bericht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdielen wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter etc.) genutzt werden.

Art. 2 lit. c BÜPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft jedoch auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug in die Auslegung unrechtmässig ist – auch hier setzt sich die Revision inakzeptabel über die gesetzlichen Vorgaben des BÜPF hinweg. Onlinespeicherdielen sind deshalb aus Art. 16d zu streichen.

Zudem anerkennt der erläuternde Bericht zwar, dass VPNs zur Anonymisierung der Nutzer:innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil angebrachte Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Das Bedürfnis, auch künftig VPN-Dienste in Anspruch nehmen zu können, ist zu schützen und darf nicht vereitelt werden. Anbieter von VPNs sind daher ebenfalls aus Art. 16d auszunehmen.

Es ist irritierend, dass die bewusst separat ausgestalteten Kategorien AAKD und FDA einander zunehmend angeglichen werden, und zwar zuungunsten der AAKD, die als Kategorie mit grundsätzlich weniger weitreichenden Pflichten als die FDA konzipiert wurde. Dies missachtet den Willen des Gesetzgebers, den es zu wahren gilt.

Antrag: Streichung von Onlinespeicherdiensten und VPN-Anbieterinnen aus der Aufzählung der möglichen abgeleiteten Kommunikationsdienste in den Ausführungen zu Art. 16d im erläuternden Bericht und in der Auslegung.

Art. 16e, Art. 16f und Art. 16g

Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch komplett entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung mit deutlich erweiterten Pflichten. Entscheidend ist, dass neuerdings das Kriterium von 5'000 Nutzer:innen allein zum Auferlegen massiver Überwachungspflichten ausreicht: Erreicht eine AAKD diese Grösse, fällt sie neu in die Kategorie der AAKD mit reduzierten Pflichten und untersteht somit bereits sehr weitgehenden Mitwirkungspflichten, insbesondere der Identifikationspflicht.

Die Einführung von 5'000 Nutzer:innen als gesondert zu beurteilende Untergrenze verletzt Art. 27 Abs. 3 BÜPF, denn 5'000 Personen sind keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strengereren Überwachungsmassnahmen, gerechtfertigt wären. 5'000 Nutzer:innen werden in der digitalen Welt vielmehr sehr rasch erreicht – die Revision verkennt technische Realitäten.

Zusätzlich führt das Einführen eines Konzernatbestandes in Art. 16f Abs. 3 zu massiven Problemen: Produkte und Dienste müssen nicht mehr für sich allein bestimmte Schwellenwerte erreichen – es genügt, wenn das Mutterunternehmen oder verbundene Gesellschaften diese überschreiten. Insbesondere bei Unternehmen mit Beteiligungsstrukturen führt dies dazu, dass sämtliche Angebote pauschal der höchsten Überwachungsstufe unterstellt werden – unabhängig davon, ob sich einzelne Dienste noch im frühen Entwicklungsstadium befinden oder faktisch kaum genutzt werden. Somit müsste jedes neue Projekt von Beginn an mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden, was Innovation behindert. Zudem missachtet der Konzernatbestand das Verhältnismässigkeitsgebot: Unterschiedliche organisatorische Einheiten mit eigenständigen Angeboten werden unrechtmässig zusammengefasst, obwohl sie individuell zu prüfen wären. Die Anwendung starrer Schwellen auf ganze Konzerne statt auf einzelne Dienste umgeht eine notwendige Einzelfallprüfung.

Eine solche Regelung stünde sodann *im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali*, das die zu seltene Anwendung von Downgrades kritisierte:

«Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»

Statt KMU zu entlasten, führt die Revision neu zu einem «automatischen» *Upgrade per Verordnung ohne Verfügung* (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.

Eine Analyse der offiziellen VÜPF-Statistik unterstreicht diese offensichtliche Unverhältnismässigkeit. Im Jahr 2023 betrafen 98,97% der total 9'430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,03% für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,74% wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100% des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.

Die neue Vorlage schliesst nun ebenfalls sowohl die Registrierung via normaler E-Mail als auch die komplett anonyme Registrierung (z. B. Signal oder Telegram) aus, da AAKD bereits mit reduzierten Pflichten neu automatisch zwingend die Endnutzer:innen identifizieren müssen. Hiervon betroffen sind nicht nur alle AAKD mit reduzierten Pflichten, sondern auch all deren Wiederverkäufer. Faktisch resultiert das Gesetz somit darin, dass man sich bei keinem Dienst mehr anmelden können soll, ohne den Pass, Führerschein oder die ID entweder direkt oder indirekt zu hinterlegen. Dass Nutzer:innen künftig hierzu gezwungen wären, stellt einen massiven Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 BV) dar und ist unzumutbar.

Ein weiteres Kernproblem, das die automatische Hochstufung mit sich bringt, ist die Rechtsunsicherheit. Die Vorlage will mit klarer definierten Kategorien und Pflichten ein übersichtlichere Situation schaffen, verfehlt dieses Ziel jedoch gänzlich. Bislang fand die Hochstufung per Verfügung statt, wodurch es für die Mitwirkungspflichtigen klar erkennbar war, wann sie unter welche Pflichten fallen. Ausserdem bewirkt diese Praxis eine sinnvolle Einzelfallbetrachtung anstelle pauschaler und unzweckmässiger automatischer Hochstufungen. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den massgebenden Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes kann aber im Zweifelsfall nur schwer zu beantworten sein. Gerade deshalb besteht ein schutzwürdiges Interesse der Anbieter an Klarheit über ihre Pflichten, da sie fortan eventuell die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Diese Umstrukturierung lässt ich nicht mit der Funktionsweise von Verwaltungsverfahren vereinbaren. Die Pflicht zur Abklärung, wann eine Hochstufung vorliegt und was diese für das Unternehmen bedeutet, darf nicht in die Verantwortung der Unternehmen fallen. Der Staat zieht sich hier aus der Verantwortung und schiebt diese den Unternehmen zu, wodurch diesen zwangsläufig zeitlicher und finanzieller Mehraufwand entsteht. Von einer automatischen Hochstufung von AAKD ist daher abzusehen.

Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.

Gegenüber der geltenden VÜPF *erweitert die Revision die Pflichten zur Automatisierung noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragetypen wie z. B. "IR_59" und "IR_60", welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen.* Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.

Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 lit. b der geltenden VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grosse[n] Teil ihrer

Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. *Damit fallen auch Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz.*

Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Auch hiermit werden neue Hürden für Innovation geschaffen. Die Regelung ist unverhältnismässig und nicht sachdienlich.

Auch Non-Profit-Organisationen geraten unter die verschärften Vorgaben. Unter den neuen Kriterien wird aber allein auf die Anzahl der Nutzer:innen abgestellt für die Einstufung als AAKD. Dieses Kriterium greift jedoch zu kurz: Es berücksichtigt insbesondere nicht die wirtschaftliche Tragfähigkeit der Anbieter:innen. Gerade bei Open-Source- und Non-Profit-Lösungen mit grosser Reichweite, aber geringem Budget, führt dies zu einer verheerenden finanziellen Belastung: Anbieter:innen mit solchen Projekten würden gezwungen, umfangreiche Überwachungsmassnahmen einzuführen. Solche Anbieter:innen würden gezielt aus dem Schweizer Markt gedrängt, während gleichzeitig bestehende Monopole wie WhatsApp (96% Marktanteil in der Schweiz) gestärkt würden.

Es muss ausserdem klar festgehalten werden, dass sich das BÜPF und die VÜPF nur auf Anbieter:innen beziehen können, die in der Schweiz tatsächlich tätig sind. Die Erlasse dürfen nicht so ausgelegt werden, dass sie eine extraterritoriale Wirkung entfalten und internationale Dienste wie Signal, WhatsApp oder Microsoft Teams erfasst sind.

Das Kriterium der reinen Nutzer:innenzahl ist ungeeignet und muss gestrichen werden.

Die Regelung schwächt auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade us-amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger:innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, End-zu-End-verschlüsselter Kommunikation ist heute wichtiger denn je und fällt in den Bereich grundrechtlich geschützter Ansprüche, die es zu wahren gilt. Diese Ansprüche dürfen nicht aufs Spiel gesetzt werden, um ein knallhartes Überwachungsregime der Kommunikation in der Schweiz durchzusetzen – die Prioritäten werden höchst fragwürdig gesetzt.

Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade illegal ist (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer:innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, diese zu erhebenden Datenmengen sind von enormem Ausmass und bergen folglich massive Risiken für Hackerangriffe.

Des Weiteren ist nicht belegt, dass die Speicherung der betreffenden Daten zu spürbar mehr erfolgreichen Ermittlungen führt. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisshandlung via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfüge, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.

Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren. Diese Handhabe bedeutet einen Verstoss gegen das Legalitätsprinzip und untergräbt legislative Kompetenzen. Ausserdem verfügt die Schweiz bereits über reichlich Mittel zur Aufklärung und Verfolgung von Straftaten, die Behörden können bereits heute auf sicherheitsrelevante Daten zurückgreifen. Unternehmen wie Proton (s. «Positionspapier zur Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)» von Proton) kooperieren seit Jahren mit den Schweizer Strafverfolgungsbehörden und dem Nachrichtendienst des Bundes (NDB). Wenn nun solche Unternehmen aus bereits genannten Gründen zur Abwanderung gezwungen werden, bewirkt die Revision auch hier das genaue Gegenteil ihrer erklärten Ziele: Anstatt der Schaffung besserer Möglichkeiten zur Strafverfolgung würden die Schweizer Behörden wie etwa Fedpol den Zugriff auf wichtige Partner bei der Beschaffung sicherheitsrelevanter Daten verlieren.

Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Integrität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.

Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das DSG. Der Entwurf bringt nicht, wie der Begleitbericht den Leser:innen weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit, steht in direktem Gegensatz zum besagten Postulat 19.4031 und bedeutet massive Eingriffe in grundrechtlich geschützte Sphären, sowohl von Unternehmen als auch von Nutzer:innen.

Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen und das bestehende System muss beibehalten werden.

Antrag: Streichung der Artikel und Beibehaltung der bestehenden Kriterien und der zwei Kategorien von AAKD. + Ausnahmen für Pilotprojekte (auch von grossen Firmen) und Non-Profits per se. Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).

Art. 16h

Art. 16h konkretisiert die Kategorie der «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» aus Art. 2 lit. e BÜPF. Die Vorschrift verfehlt ihr Ziel – anstatt Unsicherheiten darüber zu beheben, wer unter diese Kategorie fällt, schafft sie weitere Unklarheiten. Der schwammig formulierte Verordnungstext könnte dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist:innen, Whistleblower:innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber:innen solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer:innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen.

Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt. Die Unklarheit bezüglich der Einordnung von TOR-Servers wirft weitere Fragen auf, denn wenn TOR nicht als PZD zu qualifizieren

ist, müsste TOR – gleich wie die VPNs – der Kategorie der AAKD zugeordnet werden. Somit stünden Betreiber:innen von TOR-Servern – wie etwa die Digitale Gesellschaft – unter der Identifikationspflicht. Diese ist jedoch, wie dargelegt, nicht umsetzbar.

Es braucht somit entweder die Zusicherung, dass Betreiberinnen von TOR-Nodes nicht dem BÜPF und der VÜPF unterstellt sind oder aber Kategorien von Mitwirkungspflichten, die so gestaltet sind, dass ein:e Betreiber:in eines TOR-Nodes nicht einer Identifikationspflicht unterstellt wird – z. B. indem die Schwelle für das Auferlegen der Identifikationspflicht auf 1 Mio. Nutzer:innen angehoben wird.

Wären Betreiber:innen von TOR-Nodes von der Identifikationspflicht erfasst, würde dies fundamentale Grundrechte wie das Recht auf Privatsphäre und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK), die Meinungs- und Informationsfreiheit (Art. 16 BV, Art. 10 EMRK) gefährden. Ebenso würde das datenschutzrechtliche Prinzip der Datensicherheit (Art. 8 DSG) komplett unterlaufen. Diese Eingriffe in national und international geschützte Rechtsansprüche sind nicht hinzunehmend.

Dieser potentielle Angriff auf die genannten Grundrechte ist hochproblematisch und setzt ein politisches Statement: Die Schweiz bewegt sich weg von Grundrechtsschutz hin zum hochgerüsteten Überwachungsstaat.

Antrag: Es muss sichergestellt werden, dass Technologien wie TOR oder I2P nicht vom Anwendungsbereich der VÜPF erfasst sind.

Art. 16h Abs. 2

Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Endbenutzer:innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 VE-VÜPF: Gemäss diesem Artikel trägt die das WLAN erschliessenden FDA die Verantwortung zur Identifikation der Nutzer:innen. Die Regelung führt also dazu, dass FDA, die einen Vertrag haben mit «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» (PZD), sehr schnell für die Identifikation der Endnutzer:innen ihrer Vertragspartner zuständig sind. Diese Regelung ist unsinnig und schlicht nicht umsetzbar.

Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer:innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24), die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22) oder der Verwendung von IPv6. Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDA unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden.

Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten: FDA resp. Anbieterinnen von öffentlichen WLAN-Zugängen dürfen nur unter einer Identifikationspflicht stehen, wenn die PZD, die den Zugang der FDA nutzt, «professionell betrieben» ist – und zwar nach der aktuellen Auslegungsform (s. Erläuternder Bericht zur (letzten)Totalrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs):

«Mit «professionell betrieben» ist gemeint, dass eine FDA oder eine auf öffentliche WLAN-Zugangspunkte spezialisierte IT-Dienstleisterin den technischen Betrieb des öffentlichen WLAN-

Zugangspunktes durchführt, die dies auch noch für andere öffentliche WLAN-Zugangspunkte an anderen Standorten macht. Wenn eine natürliche oder juristische Person an ihrem Internetzugang selbst einen öffentlichen WLAN-Zugangspunkt technisch betreibt und diesen Zugang Dritten zur Verfügung stellt, muss die FDA, die den Internetzugang anbietet, keine Identifikation der Endbenutzenden sicherstellen.»

So wird sichergestellt, dass FDA nicht unmöglich umzusetzenden Pflichten unterstellt werden.

Antrag: Streichung der Ausführung im erläuternden Bericht. Das Kriterium «professionell betrieben» ist nach der bislang geltenden Regelung zu verstehen. Art. 16h Abs. 2 ist ersatzlos zu streichen und im Zusammenhang mit Art. 19 Abs. 2 ist auf die aktuelle Definition von «professionell betrieben» abzustellen.

Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2

Bei Konzernen knüpft die VE-VÜPF nicht mehr an die Umsatz- und Nutzer:innenzahlen des betroffenen Unternehmens an, neu sind die Zahlen des Konzerns ausschlaggebend für eine Hoch- oder Herunterstufung. Die Begründung, dies diene der Vereinfachung, ist unlogisch und irreführend: Unternehmen müssen ihre Zahlen ohnehin produktbezogen ausweisen, die nötigen Daten liegen also längst vor. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.

Antrag: Streichung des «Konzernatbestand» und Beibehaltung der bestehenden Regelung.

Art. 19 Abs. 1

Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD – erfasst sind die AAKD mit reduzierten und mit vollen Pflichten – widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht. Durch die neuen Schwellenwerte zur Einstufung findet eine beachtliche Ausweitung der Identifikationspflicht statt.

Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des DSG, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch insbesondere der Grundrechtsschutz von Nutzer:innen in der Schweiz massiv beeinträchtigt wird. Die Identifikationspflicht greift immens in das Recht auf informationelle Selbstbestimmung ein und hält einer Grundrechtsprüfung nach Art. 36 BV schon allein aufgrund ihrer Unverhältnismässigkeit nicht stand.

Bezüglich einschneidender Pflichten, die potentiell schwere Grundrechtseingriffe bedeuten – wie es bei Identifikationspflichten zweifellos der Fall ist – muss Rechtsetzung in jedem Fall mit äusserster Sorgfalt und unter strenger Beachtung des Verhältnismässigkeitsgebots erfolgen. Außerdem darf sich eine solche Pflicht nicht über gesetzliche Vorgaben, wie in diesem Fall vom BÜPF vorgegeben, hinwegsetzen.

Durch die breite Auferlegung einer solchen Pflicht werden datenschutzfreundliche Unternehmen bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird. Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Nur so können datenschutzrechtliche Vorgaben und die Rechte Betroffener gewahrt werden.

Antrag: Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation von Teilnehmenden.

Art. 18

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 19 Abs. 2

Das Kriterium «professionell betrieben» ist nach der bestehenden Regelung auszulegen (s. vorstehen). Es sei ausserdem darauf hingewiesen, dass sich aus dieser Regelung eine vertragsrechtliche Problematik zwischen den FDA und den PZD ergeben würde, die nicht tragbar ist.

Antrag: Auslegung des Kriteriums «professionell betrieben» nach der bestehenden Regelung und nicht i. S. v. Art. 16h Abs. 2.

Art. 21 Abs. 1 lit. a

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.

Antrag: Streichung

Art. 22

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.

Antrag: beibehalten

Art. 11 Abs. 4

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.

Antrag: Streichung

Art. 16b

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.

Antrag: Streichung

Art. 31 Abs. 1

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 51 und 52

Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.

Antrag: beibehalten

Art. 60a

Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde laut den Erläuterungen bewusst auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten. Art. 60a ist zu streichen.

Antrag: Streichung des Artikels

Art. 42a und 43a

Die Art. 42a und 43a führen neu die Abfragetypen «IR_59» und «IR_60» ein, über die sensible Daten automatisiert abgefragt werden können. Sie verlangen von Anbietern, dass sie jederzeit Auskunft geben können bezüglich des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Auch für das Auferlegen dieser Pflicht gilt die fragliche Schwelle von 5'000 Nutzer:innen. Erfasst ist somit nahezu die gesamte AAKD-Landschaft der Schweiz.

Das Problem liegt darin, dass die «IR_»-Abfragen zu Informationen nach Art. 42a und 43a neu automatisiert abgerufen werden können – im Gegensatz zu den «HD_»- (historische Daten) und «RT»- (Echtzeitüberwachung) Abfragen, die strengeren Regeln und einer juristischen Kontrolle unterliegen.

Bei den «IR_59»- und «IR_60»-Abfragen handelt es sich allerdings um sensible Informationen wie etwa das Abrufen einer IP-Adresse. Solche Informationen mussten bislang zurecht über strengere Abfragetypen eingeholt werden. Es ist nicht nachvollziehbar, warum Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber. Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser automatisierten Auskünfte ergibt. Unternehmen sind daher nur unzulänglich geschützt vor missbräuchlichen Anfragen und vor Kosten, die ihnen durch die Pflicht, diese Auskünfte automatisch weiterzugeben, entstehen wird.

Künftig könnten so umfangreiche Informationen über die neuen Abfragetypen beschafft werden, die bislang zurecht den strengerden Regeln der rechtlich sichereren Informations-/Überwachungstypen «HD_» und «RT_» unterworfen waren. «IR_59» und «IR_60» ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne den erforderlichen Kontrollen dieser invasiven Überwachungstypen unterworfen zu sein.

Die Entwicklung, dass mittels «IR_»-Abfragen neu auch personenbezogene sensible Nutzungsdaten eingeholt werden können, widerspricht der Logik der unterschiedlichen Abfragetypen und öffnet Tür und Tor für missbräuchliche Abfragen und eine Echtzeitüberwachung von Millionen von Nutzer:innen. Auch hier stehen grundrechtlich geschützte Ansprüche auf dem Spiel, die mit einer solchen Regelung auf nicht nachvollziehbare Weise untergraben und missachtet werden.

Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind. Die AAKD müssten künftig gewisse Datenkategorien systematisch erheben, um dieser Pflicht nachzukommen. Art. 27 Abs. 2 BÜPF erklärt allerdings, dass AAKD «auf Verlangen die *ihnen zur Verfügung stehenden* Randdaten des Fernmeldeverkehrs der überwachten Person liefern» müssen. Bei einer dahingehenden Auslegung des Bestimmungen bedeutete dies einen weiteren Verstoss gegen das BÜPF.

Unter rechtsstaatlichen Gesichtspunkten gilt es ausserdem die geplante Schwächung der Institution des Zwangsmassnahmengerichts auf das Schärfste zu kritisieren. Mit der Schaffung der zwei neuen Auskunftstypen, die mittels einfacher Auskunftsanfrage automatisch abgerufen werden können, werden rechtliche Kontrollmechanismen wie das Zwangsmassnahmengericht umgangen und der Einflussbereich der Staatsanwaltschaft noch weiter ausgebaut. Art. 42a und 43a sind daher vollumfänglich zu streichen.

Antrag: Streichung der Artikel

Art. 50a

Art. 50a sieht vor, dass Anbieter:innen verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Auch diese Pflicht soll eine Vielzahl neuer Unternehmen erfassen: Betroffen sind nicht mehr nur FDA (Art. 26 BÜPF) und ausnahmsweise AAKD (Art. 27 BÜPF), sondern sämtliche Anbieter:innen mit mehr als 5'000 Nutzer:innen. Im Ergebnis wäre fast die gesamte Schweizer AAKD-Branche betroffen (kaum ein Produkt ist lebensfähig mit weniger als 5'000 Teilnehmer:innen).

Die Ausdehnung dieser Pflicht auf AAKD stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar: Es findet keine Einzelfallprüfung statt und die AAKD werden dieser Pflicht unterworfen, auch wenn sie keineswegs «Dienstleistungen von grosser

wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten», was jedoch gesetzliche Vorgabe ist (Art. 27 Abs. 3 BÜPF).

Problematisch ist zudem, dass aufgrund dieser Vorgabe Anbieter:innen ihrer Verschlüsselungen so konfigurieren müssen, dass sie von ihnen aufgehoben werden können – eine durch Anbieter:innen aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung allerdings in jedem Fall. Dies führt zu schwächeren Verschlüsselungen und der Abnahme der Sicherheit von Kommunikationsdiensten.

Daraus ergibt sich eine Grundrechtsproblematik von erheblicher Tragweite: Das Verhältnismässigkeitsgebot aus Art. 36 BV kann nicht eingehalten werden, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Die Interessenabwägung darf hier nicht zuungunsten der Grundrechtsträger:innen erfolgen, da es sich bei deren Interessen um solche von fundamentalem Gewicht – dem Zugang zu sicherer Kommunikation und damit direkt verbunden dem Recht auf freie Meinungsäusserung – handelt.

Wichtig ist, dass Verschlüsselungen, die auf dem Endgerät der Nutzer:innen erfolgen – also End-zu-End-Verschlüsselungen – nicht unter die Pflicht zur Aufhebung gemäss Art. 50a VE-VÜPF fallen dürfen. Diese Form der Verschlüsselung liegt ausschliesslich in der Sphäre der Nutzer:innen und es wäre untragbar, die Pflicht zur Aufhebung von Verschlüsselungen in dieser Sphäre zu verlangen. Die Anbieter:innen dürfen daher nicht dazu verpflichtet werden, diese Inhalte zu entschlüsseln und zugänglich zu machen. Im Gegensatz dazu betrifft die Transportverschlüsselung «lediglich» die Verbindung zwischen Client und Server und kann von Anbieter:innen kontrolliert werden. Es ist wichtig, dass diese technischen Unterscheidungen und unterschiedlichen Schutzwirkungen und -richtungen bei rechtlichen Umsetzungen beachtet werden. Wir begrüssen die Klarstellung im erläuternden Bericht, dass die End-zu-End-Verschlüsselung vom Anwendungsbereich ausgenommen ist. Es muss jedoch ebenso klar sein, dass das ganze Endgerät von Nutzer:innen aus dem Anwendungsbereich von Art. 50a VE-VÜPF ausgenommen ist.

Es braucht im Übrigen auch eine Klarstellung darüber, dass eine rückwirkende Möglichkeit zur Aufhebung klar ausgeschlossen ist. Eine solche würde de facto eine Vorratsdatenspeicherung verschlüsselter Inhalte und Keys darstellen, die mit dem Prinzip der Datenminimierung (Art. 6 Abs. 3 DSG) und dem Schutz der Privatsphäre (Art. 13 BV) unvereinbar ist.

Antrag: Streichung der «Anbieterin mit reduzierten Pflichten» aus dem Anwendungsbereich sowie eine Klarstellung darüber, dass die Aufhebung von Verschlüsselungen auf dem Endgerät der Nutzer:innen sowie eine rückwirkende Verpflichtung zur Aufhebung ausgeschlossen sind.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Art. 14 Abs. 3 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und wirtschaftlich nicht tragbar, was das Einführen von Fristen obsolet werden lässt. Der Absatz ist daher ersatzlos zu streichen.

Antrag: Streichung

Art. 14 Abs. 4 VD-ÜPF

Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der Unterworfenen AAKD – da auch AAKD mit reduzierten Pflichten erfasst sind – massiv. Dies ist wie bereits ausgeführt weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.

Antrag: Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten»

Art. 20 Abs. 1 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen, ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.

Antrag: Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»

Schlussbemerkung

Trotz des Umfangs dieser Stellungnahme gilt: Das Ausbleiben einer expliziten Bemerkung zu einzelnen Bestimmungen bedeutet keine Zustimmung der Digitalen Gesellschaft. Die Ablehnung der Revision bleibt volumnäiglich bestehen.

Freundliche Grüsse

Erik Schönenberger
Geschäftsleiter

Von: jcT3hpvLpjFxmjNzXnePUt

Gesendet: Montag, 5. Mai 2025 16:53:19 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zu den Vernehmlassungsentwürfen VÜPF/VD-ÜPF

Sehr geehrte Damen und Herren

Hiermit reiche ich meine Stellungnahme im Rahmen des Vernehmlassungsverfahrens zu den Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) ein.

Ich möchte meinen klaren und deutlichen Widerspruch gegen die vorgeschlagenen Änderungen ausdrücken.

Meine Bedenken konzentrieren sich insbesondere auf die Auswirkungen dieser Vorschläge auf die allgemeine Privatsphäre der Bürgerinnen und Bürger sowie auf die Cybersicherheit in der Schweiz. Insbesondere der Aktuellen Lage. Eine Ausweitung der Überwachungsmöglichkeiten birgt Risiken für die digitale Sicherheit und das Vertrauen in digitale Dienste.

Ich schliesse mich den Bedenken der Firmen Threema, Proton, NymVPN etc... an und verweise auf deren detaillierte Stellungnahme zu diesem Thema.

Ich bitte Sie dringend, meine Bedenken bei der weiteren Ausarbeitung der Gesetzesentwürfe zu berücksichtigen.

Vielen Dank für Ihre Zeit und Aufmerksamkeit.

Mit freundlichen Grüßen

Jonas M.

Opposition à la révision de la VÜPF

Madame, Monsieur,

En tant que citoyen suisse, je tiens à exprimer ma ferme opposition à la révision de la VÜPF. Cette révision représente une atteinte grave à nos droits fondamentaux, à notre économie et à notre sécurité.

1. Droits fondamentaux

La révision de la VÜPF viole plusieurs piliers de notre démocratie : la Constitution fédérale, la loi sur la protection des données (DSG) et le BÜPF. Elle introduit une surveillance généralisée, disproportionnée et incompatible avec l'équilibre entre sécurité et liberté individuelle. Nous ne vivons pas dans une dictature...

2. Économie et innovation

Les nouvelles obligations rendent la Suisse peu attractive pour les entreprises technologiques. Des acteurs clés comme Proton et Threema ont déjà menacé de quitter le pays. Cela nuirait gravement à notre écosystème numérique et à notre compétitivité.

3. Vie privée et sécurité

La révision compromet l'accès à des communications sécurisées, affectant non seulement les citoyens ordinaires, mais aussi les journalistes, avocats, lanceurs d'alerte et autres groupes vulnérables. Elle met en péril le droit à la confidentialité.

4. Problèmes techniques et juridiques

Les nouvelles règles sont complexes, peu claires et parfois inapplicables. Elles créent une insécurité juridique pour les entreprises et les citoyens, tout en élargissant de manière opaque les obligations de coopération.

En tant que citoyen suisse, je rejette fermement cette révision. Elle affaiblit nos droits, notre économie et notre sécurité. Elle doit être abandonnée dans son intégralité.

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

Léo Dias Almeida

Von: Balz Guenat

Gesendet: Dienstag, 6. Mai 2025 00:11:38 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm,
Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: VÜPF

Guten Tag

Hiermit bekenne ich meine Unterstützung der von der Digitalen Gesellschaft
veröffentlichten Stellungnahme:

<https://www.digitale-gesellschaft.ch/2025/05/02/bundesrat-will-ueberwachungsstaat-per-verordnung-massiv-ausbauen-stellungnahme-zur-teilrevision-vuepf-und-vd-uepf/>

Freundliche Grüsse,

Balz Guenat

Von: Nemanja Ilic
Gesendet: Dienstag, 6. Mai 2025 02:36:52 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Opposition à la révision des deux ordonnances d'exécution de la surveillance de la correspondance par poste et télécommunication (OSCPT et OME-SCPT)

Madame, Monsieur,

Je vous écris pour vous faire de mes inquiétudes et mon désaccord vis-à-vis des révisions OSCPT et OME-SCPT.

En effet, j'ai lu en détail tous les communiqués liés à ces révisions et je comprends que les auteurs de ces propositions désirent instaurer une processus de surveillance de masse en temps réel de la population Suisse, via les fournisseurs réseau entre autres. Pas besoin d'être un génie pour comprendre que cela ménera forcément à la collecte et le traitement des données personnelles de tous les individus sans raison valable.

A quoi les auteurs de ces propositions jouent-ils? Se croiraient-ils aux Etats-Unis? Rêvent-ils d'un Patriot Act 2.0? Une chose est certaine, ils ne connaissent pas bien les Suisses et leurs valeurs. Ou alors c'est l'inverse. Ils savent très bien que la grande majorité des Suisses s'opposeraient à de telles propositions et recourent alors « illégalement » et immoralement à des révisions d'ordonnances d'exécution qui ne peuvent être contestées par référendum?

Ces révisions sont profondément opposées à tout ce que la Suisse représente et les conséquences de telles révisions seraient très graves. Nous ne voulons pas d'une NSA en Suisse. Cela détruirait totalement l'image de la Suisse. Alors je vous prie, faites le nécessaire pour que ces révisions n'aient jamais lieu.

Cordialement,
NI

Mari Steiner



Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
3003 Bern

Winterthur, 05.05.2025

Stellungnahme zur geplanten Revision des VÜPF und VD-ÜPF

Sehr geehrte Damen und Herren

Ich möchte mich hiermit entschieden gegen die geplante Teilrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) sowie der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) aussprechen. Die folgenden Punkte bereiten mir grosse Sorge:

- **Verfassungsbruch:** Die geplante Ausweitung der digitalen Überwachung steht im klaren Widerspruch zu Artikel 13 der Bundesverfassung, der das Recht auf Achtung der Privatsphäre garantiert. Gerade in einem Staat wie der Schweiz, der international für Datenschutz und Bürgerrechte bekannt ist, muss diese Integrität gewahrt bleiben.
- **Imageschaden für die Schweiz:** Die Schweiz geniesst weltweit einen Ruf als sicherer Hafen für Privatsphäre und digitale Rechte. Ein Gesetz wie dieses würde diesen Ruf irreparabel beschädigen – zum Schaden der Bevölkerung, der Wirtschaft und der staatlichen Glaubwürdigkeit.
- **Gefährdung des Innovationsstandorts:** Besonders kleine Unternehmen und Startups im Bereich Cybersicherheit und Kommunikation würden durch die geplanten Massnahmen stark benachteiligt oder gar aus dem Land vertrieben. Der volkswirtschaftliche Schaden ist immens und untergräbt das Vertrauen in die Schweizer Tech-Branche.
- **Abschwächung sicherer Kommunikation:** Dienste wie Proton oder Threema bieten echte Sicherheit – auch für Behörden, Politiker und Bürger. Die Einführung von Hintertüren oder Staatstrojanern gefährdet nicht nur die Privatsphäre, sondern öffnet Tür und Tor für Missbrauch – durch in- und ausländische Akteure.
- **Nicht glaubwürdiges Behördenargument:** Die Behauptung, nur Kriminelle seien betroffen, ist angesichts internationaler Erfahrungen – z.B. durch die Snowden-Enthüllungen – nicht haltbar. Einmal eingeführte Überwachungsinstrumente werden selten restriktiv genutzt. Warum sollte es in der Schweiz anders sein?

Ich schliesse mich auch der kritischen **Stellungnahme der Digitalen Gesellschaft** an, die diese Teilrevision fundiert analysiert und klare verfassungsrechtliche sowie technische Bedenken äussert:

<https://www.digitale-gesellschaft.ch/2025/05/02/bundesrat-will-ueberwachungsstaat-per-verordnung-massiv-ausbauen-stellungnahme-zur-teilrevision-vuepf-und-vd-uepf/>

Ich fordere daher den Stopp der Teilrevision in ihrer aktuellen Form und eine Rückbesinnung auf die in der Verfassung verankerten Grundrechte.

Mit freundlichen Grüßen

Mari Steiner

Von: Eric Studer
Gesendet: Dienstag, 6. Mai 2025 07:25:14 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme Änderung Überwachungsgesetz

Guten Morgen

Gerne möchte ich eine persönliche Stellungnahme zur geplanten Änderung des Überwachungsgesetzes abgeben.

Freundliche Grüsse
Eric Studer

Stellungnahme zur geplanten Ausweitung der Überwachungspflichten durch den Bundesrat

Als jemand, der grossen Wert auf digitale Selbstbestimmung und den Schutz der Privatsphäre legt, halte ich die geplante Revision der Verordnungen VÜPF und VD-ÜPF für einen gefährlichen Schritt in die falsche Richtung. Die Ausweitung der Überwachungspflichten auf praktisch alle Kommunikationsdienste – selbst auf kleine, datenschutzfreundliche Anbieter – widerspricht meiner Überzeugung von einem freien, demokratischen und rechtsstaatlichen digitalen Raum.

Mich beunruhigt besonders, dass dieser tiefgreifende Eingriff ohne parlamentarische Debatte oder demokratische Legitimation erfolgen soll. Der Versuch, eine derart weitreichende Regelung per Verordnung durchzusetzen, verletzt das Legalitätsprinzip und entzieht sich der Mitsprache der Bevölkerung – obwohl genau diese in ihren Grundrechten betroffen ist.

Wenn Anbieter, die sichere und vertrauliche Kommunikation ermöglichen, durch überzogene Pflichten verdrängt werden, verliert nicht nur die Wirtschaft, sondern jede und jeder Einzelne einen Teil seiner Freiheit. Das betrifft auch sensible Berufsgruppen wie Journalistinnen, Anwälte oder Ärztinnen, für die Vertraulichkeit essenziell ist.

Ich lehne diese Revision deshalb entschieden ab – im Interesse der Grundrechte, der demokratischen Legitimation und einer vielfältigen, sicheren digitalen Schweiz.

Weiterführende Links

<https://www.digitale-gesellschaft.ch/2025/05/02/bundesrat-will-ueberwachungsstaat-per-verordnung-massiv-ausbauen-stellungnahme-zur-teilrevision-vuepf-und-vd-uepf/>

Von: Isabel Christen
Gesendet: Dienstag, 6. Mai 2025 08:59:59 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Freundliche Grüsse, Isabel Christen

Isabel Lina Christen

[REDACTED]

[REDACTED]

isabel.christen@bluewin.ch

Digitale Gesellschaft, CH-4000 Basel

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
CH-3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Basel, 2. Mai 2025

Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat Beat Jans
Sehr geehrte Empfänger:innen

Am 29. Januar 2025 eröffnete der Bundesrat die Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF). Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Vorentwurf wie folgt Stellung:

Vorbemerkung

Die geplante Revision der VÜPF ist ein Frontalangriff auf unsere Grundrechte, die Rechtsstaatlichkeit sowie den IT- und Innovationsstandort Schweiz.

Mit ihrer Umsetzung würde geltendes Recht in einem Ausmass verletzt, das alarmieren muss: Die Revision ist in vielerlei Hinsicht unvereinbar mit dem Bundesgesetz betreffend die Überwachung des

Post- und Fernmeldeverkehrs (BÜPF), verstösst gegen das Datenschutzgesetz (DSG), steht in klarem Widerspruch zu den verfassungsmässigen Grundrechten und verstösst gegen Völkerrecht. Die vorgesehenen Änderungen führen zu einer massiv ausgeweiteten Überwachung – ganz grundsätzlich und flächendeckend. Dies ist mit der Ausrichtung des BÜPF, das eine fein austarierte Interessenabwägung zwischen Freiheit und Privatsphäre einerseits und Sicherheit durch Überwachungsmassnahmen andererseits verfolgt, absolut nicht vereinbar.

Die Auswirkungen auf den Wirtschafts- und Innovationsstandort Schweiz wären verheerend: Die Ausweitung der Überwachung und die damit verbundenen, übermässigen Mitwirkungspflichten machen die Schweiz für IT-Anbieter äusserst unattraktiv. Renommierte Unternehmen wie Proton oder Threema, deren Geschäftsmodelle durch die Vorlage direkt ins Visier geraten, würden in ihrer Existenz bedroht. Die ersten Konsequenzen sind bereits sichtbar: Proton hat angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen (siehe [Tages-Anzeiger vom 1. April 2025](#)). Der Chef des Unternehmens erklärte in einem Interview: «Diese Entscheidung ist wirtschaftlicher Selbstmord für die Schweiz» ([watson.ch vom 9. April 2025](#)). Ähnlich äussert sich Threema-Chef Robin Simon: «Der Wirtschaftsstandort würde durch die Revision geschwächt und für Tech-Start-ups unattraktiv.» Aktuell lasse sich Threema alle Optionen offen ([Tages-Anzeiger vom 8. April 2025](#)). Diese Warnzeichen sind ernst zu nehmen und zeigen das verheerende Ausmass der geplanten Revision.

Neben den verheerenden wirtschaftlichen Auswirkungen wird gleichzeitig der grundrechtlich garantierte Anspruch auf sichere und vertrauliche Kommunikation ausgehöhlt. Wenn Anbieterinnen abwandern, bleibt jedoch – als wäre dies nicht genug – nicht nur privaten Nutzer:innen der Zugang zu geschützten Kommunikationsmitteln verwehrt.

Ebenso betroffen sind auch Personen, die einem Berufsgeheimnis unterstehen, wie Journalistinnen oder Anwälte. Die Änderungen treffen zudem schutzbedürftige Personengruppen besonders hart: Whistleblower:innen, Menschen mit ungeklärtem Aufenthaltsstatus oder ohne Papiere aber auch Aktivist:innen verlieren ebenso den Zugang zu vertraulichen Kommunikationsmitteln. Die Revision ignoriert diese Schutzbedürfnisse und erweitert stattdessen die Eingriffsbefugnisse des Staates in einer Weise, die hochgefährlich ist.

Besonders widersprüchlich erscheint das Vorgehen des Bundes angesichts der Tatsache, dass ausgerechnet der Bundesrat selbst Threema als Messenger nutzt – ein Dienst, den er nun faktisch aus dem Markt drängt. Damit sägt die Regierung ausgerechnet an jenem Ast, auf dem sie in Sachen sicherer Kommunikation bislang selbst sitzt.

Hinzu kommt: Die geplanten Regelungen sind technisch unausgereift, unnötig komplex und in Teilen schlüssig nicht umsetzbar. Vielmehr wird ein kaum noch durchschaubares Normengeflecht geschaffen, das weder den Mitwirkungspflichtigen noch den Betroffenen ein Mindestmass an Rechtsklarheit bietet. Die Revision wird ausserdem präsentiert, als handle es sich dabei um Änderungen zur besseren Überblickbarkeit der Rechtslage und zur Schaffung von mehr Rechtssicherheit - tatsächlich aber wird der persönliche Anwendungsbereich der Mitwirkungspflichtigen enorm erweitert und eine Vielzahl neuer Anbieterinnen in den Kreis der Mitwirkungspflichtigen einbezogen. Von Transparenz kann nicht die Rede sein.

Es ist im Übrigen nicht haltbar, dass eine dermassen breit angelegte Ausweitung von Pflichten auf Verordnungsstufe angelegt wird. Solch einschneidende Veränderungen mit weitreichenden Konsequenzen sind in Gesetzesform zu erlassen. Der Bundesrat überschreitet seine Kompetenzen hier um ein Weites.

Diese Vorlage schwächt nicht nur den Innovations- und Wirtschaftsstandort Schweiz – sie untergräbt gleichzeitig im grossen Stil verfassungsmässig geschützte Rechte. Aus grundrechtlicher, datenschutzrechtlicher und gesellschaftspolitischer Sicht ist sie schlicht inakzeptabel. Die geplanten Änderungen stehen dem erklärten Ziel von mehr Freundlichkeit sowie allgemeinen rechtsstaatlichen Grundsätzen sowie Schutzbedürfnissen Einzelner diametral entgegen.

Deshalb lehnen wir die Revision vollumfänglich und in aller Deutlichkeit ab.

Bemerkungen zu einzelnen Artikeln der VÜPF

Alle Artikel

Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung (Art. 6 Abs. 3 DSG) gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kund:innen auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.

Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.ä. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.

Antrag: Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.

Art. 16b Abs. 1

Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile (Art. 16b Abs. 1 lit. b Ziff. 2 VE-VÜPF) wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Mitwirkungspflichten in Kauf nehmen.

Dazu kommt, dass das Kriterium bezüglich der Überwachungsaufträge nicht vom BÜPF gestützt wird, denn: Die Anzahl von Überwachungsaufträgen ist von der wirtschaftlichen Bedeutung einer FDA völlig losgelöst. Die wirtschaftliche Bedeutung ist aber gemäss Art. 26 Abs. 6 BÜPF ausschlaggebend dafür, ob eine FDA von den vollen Pflichten (teilweise) befreit werden kann. Im Umkehrschluss ist die wirtschaftliche Bedeutsamkeit somit Erfordernis für die Auferlegung von vollen Pflichten. Wenn eine FDA nun aber rein aufgrund einer bestimmten Anzahl von Überwachungsaufträgen nach Art. 16b Abs. 1 lit. b Ziff. 1 VE-VÜPF als vollpflichtige FDA qualifiziert wird, steht dies im Widerspruch zum BÜPF und entbehrt damit einer Rechtsgrundlage.

Dieses bereits in der aktuellen Version der VÜPF vorhandene Problem sollte im Zuge einer Revision nicht bestehen bleiben, sondern muss behoben werden.

Antrag: Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter

Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.» Es ist auf die Regelung in Art. 26 Abs. 6 BÜPF abzustellen und eine Einzelfallbetrachtung zur Einstufung vorzunehmen.

Art. 16c Abs. 3

Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als «natürliche» Schutzmechanismen gegen eine übermässige oder missbräuchliche Nutzung solcher Massnahmen durch die Untersuchungsbehörden. Die automatisierte Erteilung von Auskünften ist unverhältnismässig und widerspricht dem Prinzip der Datenminimierung. Die pauschale und undifferenzierte Regel beeinträchtigt zwangsläufig den Grundrechtsschutz.

Der vorgesehene Umsetzungszeitraum von 12 Monaten zur Umsetzung eines dermassen komplexen Systems ist ausserdem völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.

Antrag: Streichung von lit. a «automatisierte Erteilung der Auskünfte» (ebenso in Art. 18 Abs. 2).

Art. 16d

Gemäss erläuterndem Bericht stellen Kommunikationsdienste, die nicht zu den in Art. 16a Abs. 1 aufgezählten Fernmeldediensten gehören und auf die die Ausnahmen nach Art. 16a Abs. 2 nicht zutreffen, abgeleitete Kommunikationsdienste dar. Diese klarere Definition des Begriffs AAKD ist begrüssenswert, doch ist die Konkretisierung der abgeleiteten Kommunikationsdienste im erläuternden Bericht einerseits rechtsstaatlich problematisch und andererseits geht die neue Auslegung nach den Ausführungen im erläuterndem Bericht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdielen wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter etc.) genutzt werden.

Art. 2 lit. c BÜPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft jedoch auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug in die Auslegung unrechtmässig ist – auch hier setzt sich die Revision inakzeptabel über die gesetzlichen Vorgaben des BÜPF hinweg. Onlinespeicherdielen sind deshalb aus Art. 16d zu streichen.

Zudem anerkennt der erläuternde Bericht zwar, dass VPNs zur Anonymisierung der Nutzer:innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil angebrachte Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Das Bedürfnis, auch künftig VPN-Dienste in Anspruch nehmen zu können, ist zu schützen und darf nicht vereitelt werden. Anbieter von VPNs sind daher ebenfalls aus Art. 16d auszunehmen.

Es ist irritierend, dass die bewusst separat ausgestalteten Kategorien AAKD und FDA einander zunehmend angeglichen werden, und zwar zuungunsten der AAKD, die als Kategorie mit grundsätzlich weniger weitreichenden Pflichten als die FDA konzipiert wurde. Dies missachtet den Willen des Gesetzgebers, den es zu wahren gilt.

Antrag: Streichung von Onlinespeicherdiensten und VPN-Anbieterinnen aus der Aufzählung der möglichen abgeleiteten Kommunikationsdienste in den Ausführungen zu Art. 16d im erläuternden Bericht und in der Auslegung.

Art. 16e, Art. 16f und Art. 16g

Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch komplett entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung mit deutlich erweiterten Pflichten. Entscheidend ist, dass neuerdings das Kriterium von 5'000 Nutzer:innen allein zum Auferlegen massiver Überwachungspflichten ausreicht: Erreicht eine AAKD diese Grösse, fällt sie neu in die Kategorie der AAKD mit reduzierten Pflichten und untersteht somit bereits sehr weitgehenden Mitwirkungspflichten, insbesondere der Identifikationspflicht.

Die Einführung von 5'000 Nutzer:innen als gesondert zu beurteilende Untergrenze verletzt Art. 27 Abs. 3 BÜPF, denn 5'000 Personen sind keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strengereren Überwachungsmassnahmen, gerechtfertigt wären. 5'000 Nutzer:innen werden in der digitalen Welt vielmehr sehr rasch erreicht – die Revision verkennt technische Realitäten.

Zusätzlich führt das Einführen eines Konzernatbestandes in Art. 16f Abs. 3 zu massiven Problemen: Produkte und Dienste müssen nicht mehr für sich allein bestimmte Schwellenwerte erreichen – es genügt, wenn das Mutterunternehmen oder verbundene Gesellschaften diese überschreiten. Insbesondere bei Unternehmen mit Beteiligungsstrukturen führt dies dazu, dass sämtliche Angebote pauschal der höchsten Überwachungsstufe unterstellt werden – unabhängig davon, ob sich einzelne Dienste noch im frühen Entwicklungsstadium befinden oder faktisch kaum genutzt werden. Somit müsste jedes neue Projekt von Beginn an mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden, was Innovation behindert. Zudem missachtet der Konzernatbestand das Verhältnismässigkeitsgebot: Unterschiedliche organisatorische Einheiten mit eigenständigen Angeboten werden unrechtmässig zusammengefasst, obwohl sie individuell zu prüfen wären. Die Anwendung starrer Schwellen auf ganze Konzerne statt auf einzelne Dienste umgeht eine notwendige Einzelfallprüfung.

Eine solche Regelung stünde sodann *im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali*, das die zu seltene Anwendung von Downgrades kritisierte:

«Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»

Statt KMU zu entlasten, führt die Revision neu zu einem «automatischen» *Upgrade per Verordnung ohne Verfügung* (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.

Eine Analyse der offiziellen VÜPF-Statistik unterstreicht diese offensichtliche Unverhältnismässigkeit. Im Jahr 2023 betrafen 98,97% der total 9'430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,03% für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,74% wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100% des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.

Die neue Vorlage schliesst nun ebenfalls sowohl die Registrierung via normaler E-Mail als auch die komplett anonyme Registrierung (z. B. Signal oder Telegram) aus, da AAKD bereits mit reduzierten Pflichten neu automatisch zwingend die Endnutzer:innen identifizieren müssen. Hiervon betroffen sind nicht nur alle AAKD mit reduzierten Pflichten, sondern auch all deren Wiederverkäufer. Faktisch resultiert das Gesetz somit darin, dass man sich bei keinem Dienst mehr anmelden können soll, ohne den Pass, Führerschein oder die ID entweder direkt oder indirekt zu hinterlegen. Dass Nutzer:innen künftig hierzu gezwungen wären, stellt einen massiven Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 BV) dar und ist unzumutbar.

Ein weiteres Kernproblem, das die automatische Hochstufung mit sich bringt, ist die Rechtsunsicherheit. Die Vorlage will mit klarer definierten Kategorien und Pflichten ein übersichtlichere Situation schaffen, verfehlt dieses Ziel jedoch gänzlich. Bislang fand die Hochstufung per Verfügung statt, wodurch es für die Mitwirkungspflichtigen klar erkennbar war, wann sie unter welche Pflichten fallen. Ausserdem bewirkt diese Praxis eine sinnvolle Einzelfallbetrachtung anstelle pauschaler und unzweckmässiger automatischer Hochstufungen. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den massgebenden Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes kann aber im Zweifelsfall nur schwer zu beantworten sein. Gerade deshalb besteht ein schutzwürdiges Interesse der Anbieter an Klarheit über ihre Pflichten, da sie fortan eventuell die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Diese Umstrukturierung lässt ich nicht mit der Funktionsweise von Verwaltungsverfahren vereinbaren. Die Pflicht zur Abklärung, wann eine Hochstufung vorliegt und was diese für das Unternehmen bedeutet, darf nicht in die Verantwortung der Unternehmen fallen. Der Staat zieht sich hier aus der Verantwortung und schiebt diese den Unternehmen zu, wodurch diesen zwangsläufig zeitlicher und finanzieller Mehraufwand entsteht. Von einer automatischen Hochstufung von AAKD ist daher abzusehen.

Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.

Gegenüber der geltenden VÜPF erweitert die Revision die Pflichten zur Automatisierung noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragetypen wie z. B. "IR_59" und "IR_60", welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.

Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 lit. b der geltenden VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grosse[n] Teil ihrer

Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. *Damit fallen auch Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz.*

Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Auch hiermit werden neue Hürden für Innovation geschaffen. Die Regelung ist unverhältnismässig und nicht sachdienlich.

Auch Non-Profit-Organisationen geraten unter die verschärften Vorgaben. Unter den neuen Kriterien wird aber allein auf die Anzahl der Nutzer:innen abgestellt für die Einstufung als AAKD. Dieses Kriterium greift jedoch zu kurz: Es berücksichtigt insbesondere nicht die wirtschaftliche Tragfähigkeit der Anbieter:innen. Gerade bei Open-Source- und Non-Profit-Lösungen mit grosser Reichweite, aber geringem Budget, führt dies zu einer verheerenden finanziellen Belastung: Anbieter:innen mit solchen Projekten würden gezwungen, umfangreiche Überwachungsmassnahmen einzuführen. Solche Anbieter:innen würden gezielt aus dem Schweizer Markt gedrängt, während gleichzeitig bestehende Monopole wie WhatsApp (96% Marktanteil in der Schweiz) gestärkt würden.

Es muss ausserdem klar festgehalten werden, dass sich das BÜPF und die VÜPF nur auf Anbieter:innen beziehen können, die in der Schweiz tatsächlich tätig sind. Die Erlasse dürfen nicht so ausgelegt werden, dass sie eine extraterritoriale Wirkung entfalten und internationale Dienste wie Signal, WhatsApp oder Microsoft Teams erfasst sind.

Das Kriterium der reinen Nutzer:innenzahl ist ungeeignet und muss gestrichen werden.

Die Regelung schwächt auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade us-amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger:innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, End-zu-End-verschlüsselter Kommunikation ist heute wichtiger denn je und fällt in den Bereich grundrechtlich geschützter Ansprüche, die es zu wahren gilt. Diese Ansprüche dürfen nicht aufs Spiel gesetzt werden, um ein knallhartes Überwachungsregime der Kommunikation in der Schweiz durchzusetzen – die Prioritäten werden höchst fragwürdig gesetzt.

Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade illegal ist (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer:innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, diese zu erhebenden Datenmengen sind von enormem Ausmass und bergen folglich massive Risiken für Hackerangriffe.

Des Weiteren ist nicht belegt, dass die Speicherung der betreffenden Daten zu spürbar mehr erfolgreichen Ermittlungen führt. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisshandlung via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfüge, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.

Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren. Diese Handhabe bedeutet einen Verstoss gegen das Legalitätsprinzip und untergräbt legislative Kompetenzen. Ausserdem verfügt die Schweiz bereits über reichlich Mittel zur Aufklärung und Verfolgung von Straftaten, die Behörden können bereits heute auf sicherheitsrelevante Daten zurückgreifen. Unternehmen wie Proton (s. «Positionspapier zur Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)» von Proton) kooperieren seit Jahren mit den Schweizer Strafverfolgungsbehörden und dem Nachrichtendienst des Bundes (NDB). Wenn nun solche Unternehmen aus bereits genannten Gründen zur Abwanderung gezwungen werden, bewirkt die Revision auch hier das genaue Gegenteil ihrer erklärten Ziele: Anstatt der Schaffung besserer Möglichkeiten zur Strafverfolgung würden die Schweizer Behörden wie etwa Fedpol den Zugriff auf wichtige Partner bei der Beschaffung sicherheitsrelevanter Daten verlieren.

Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Integrität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.

Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das DSG. Der Entwurf bringt nicht, wie der Begleitbericht den Leser:innen weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit, steht in direktem Gegensatz zum besagten Postulat 19.4031 und bedeutet massive Eingriffe in grundrechtlich geschützte Sphären, sowohl von Unternehmen als auch von Nutzer:innen.

Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen und das bestehende System muss beibehalten werden.

Antrag: Streichung der Artikel und Beibehaltung der bestehenden Kriterien und der zwei Kategorien von AAKD. + Ausnahmen für Pilotprojekte (auch von grossen Firmen) und Non-Profits per se. Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).

Art. 16h

Art. 16h konkretisiert die Kategorie der «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» aus Art. 2 lit. e BÜPF. Die Vorschrift verfehlt ihr Ziel – anstatt Unsicherheiten darüber zu beheben, wer unter diese Kategorie fällt, schafft sie weitere Unklarheiten. Der schwammig formulierte Verordnungstext könnte dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist:innen, Whistleblower:innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber:innen solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer:innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen.

Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt. Die Unklarheit bezüglich der Einordnung von TOR-Servers wirft weitere Fragen auf, denn wenn TOR nicht als PZD zu qualifizieren

ist, müsste TOR – gleich wie die VPNs – der Kategorie der AAKD zugeordnet werden. Somit stünden Betreiber:innen von TOR-Servern – wie etwa die Digitale Gesellschaft – unter der Identifikationspflicht. Diese ist jedoch, wie dargelegt, nicht umsetzbar.

Es braucht somit entweder die Zusicherung, dass Betreiberinnen von TOR-Nodes nicht dem BÜPF und der VÜPF unterstellt sind oder aber Kategorien von Mitwirkungspflichten, die so gestaltet sind, dass ein:e Betreiber:in eines TOR-Nodes nicht einer Identifikationspflicht unterstellt wird – z. B. indem die Schwelle für das Auferlegen der Identifikationspflicht auf 1 Mio. Nutzer:innen angehoben wird.

Wären Betreiber:innen von TOR-Nodes von der Identifikationspflicht erfasst, würde dies fundamentale Grundrechte wie das Recht auf Privatsphäre und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK), die Meinungs- und Informationsfreiheit (Art. 16 BV, Art. 10 EMRK) gefährden. Ebenso würde das datenschutzrechtliche Prinzip der Datensicherheit (Art. 8 DSG) komplett unterlaufen. Diese Eingriffe in national und international geschützte Rechtsansprüche sind nicht hinzunehmend.

Dieser potentielle Angriff auf die genannten Grundrechte ist hochproblematisch und setzt ein politisches Statement: Die Schweiz bewegt sich weg von Grundrechtsschutz hin zum hochgerüsteten Überwachungsstaat.

Antrag: Es muss sichergestellt werden, dass Technologien wie TOR oder I2P nicht vom Anwendungsbereich der VÜPF erfasst sind.

Art. 16h Abs. 2

Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Endbenutzer:innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 VE-VÜPF: Gemäss diesem Artikel trägt die das WLAN erschliessenden FDA die Verantwortung zur Identifikation der Nutzer:innen. Die Regelung führt also dazu, dass FDA, die einen Vertrag haben mit «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» (PZD), sehr schnell für die Identifikation der Endnutzer:innen ihrer Vertragspartner zuständig sind. Diese Regelung ist unsinnig und schlicht nicht umsetzbar.

Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer:innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24), die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22) oder der Verwendung von IPv6. Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDA unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden.

Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten: FDA resp. Anbieterinnen von öffentlichen WLAN-Zugängen dürfen nur unter einer Identifikationspflicht stehen, wenn die PZD, die den Zugang der FDA nutzt, «professionell betrieben» ist – und zwar nach der aktuellen Auslegungsform (s. Erläuternder Bericht zur (letzten)Totalrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs):

«Mit «professionell betrieben» ist gemeint, dass eine FDA oder eine auf öffentliche WLAN-Zugangspunkte spezialisierte IT-Dienstleisterin den technischen Betrieb des öffentlichen WLAN-

Zugangspunktes durchführt, die dies auch noch für andere öffentliche WLAN-Zugangspunkte an anderen Standorten macht. Wenn eine natürliche oder juristische Person an ihrem Internetzugang selbst einen öffentlichen WLAN-Zugangspunkt technisch betreibt und diesen Zugang Dritten zur Verfügung stellt, muss die FDA, die den Internetzugang anbietet, keine Identifikation der Endbenutzenden sicherstellen.»

So wird sichergestellt, dass FDA nicht unmöglich umzusetzenden Pflichten unterstellt werden.

Antrag: Streichung der Ausführung im erläuternden Bericht. Das Kriterium «professionell betrieben» ist nach der bislang geltenden Regelung zu verstehen. Art. 16h Abs. 2 ist ersatzlos zu streichen und im Zusammenhang mit Art. 19 Abs. 2 ist auf die aktuelle Definition von «professionell betrieben» abzustellen.

Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2

Bei Konzernen knüpft die VE-VÜPF nicht mehr an die Umsatz- und Nutzer:innenzahlen des betroffenen Unternehmens an, neu sind die Zahlen des Konzerns ausschlaggebend für eine Hoch- oder Herunterstufung. Die Begründung, dies diene der Vereinfachung, ist unlogisch und irreführend: Unternehmen müssen ihre Zahlen ohnehin produktbezogen ausweisen, die nötigen Daten liegen also längst vor. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.

Antrag: Streichung des «Konzernatbestand» und Beibehaltung der bestehenden Regelung.

Art. 19 Abs. 1

Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD – erfasst sind die AAKD mit reduzierten und mit vollen Pflichten – widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht. Durch die neuen Schwellenwerte zur Einstufung findet eine beachtliche Ausweitung der Identifikationspflicht statt.

Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des DSG, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch insbesondere der Grundrechtsschutz von Nutzer:innen in der Schweiz massiv beeinträchtigt wird. Die Identifikationspflicht greift immens in das Recht auf informationelle Selbstbestimmung ein und hält einer Grundrechtsprüfung nach Art. 36 BV schon allein aufgrund ihrer Unverhältnismässigkeit nicht stand.

Bezüglich einschneidender Pflichten, die potentiell schwere Grundrechtseingriffe bedeuten – wie es bei Identifikationspflichten zweifellos der Fall ist – muss Rechtsetzung in jedem Fall mit äusserster Sorgfalt und unter strenger Beachtung des Verhältnismässigkeitsgebots erfolgen. Außerdem darf sich eine solche Pflicht nicht über gesetzliche Vorgaben, wie in diesem Fall vom BÜPF vorgegeben, hinwegsetzen.

Durch die breite Auferlegung einer solchen Pflicht werden datenschutzfreundliche Unternehmen bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird. Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Nur so können datenschutzrechtliche Vorgaben und die Rechte Betroffener gewahrt werden.

Antrag: Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation von Teilnehmenden.

Art. 18

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 19 Abs. 2

Das Kriterium «professionell betrieben» ist nach der bestehenden Regelung auszulegen (s. vorstehen). Es sei ausserdem darauf hingewiesen, dass sich aus dieser Regelung eine vertragsrechtliche Problematik zwischen den FDA und den PZD ergeben würde, die nicht tragbar ist.

Antrag: Auslegung des Kriteriums «professionell betrieben» nach der bestehenden Regelung und nicht i. S. v. Art. 16h Abs. 2.

Art. 21 Abs. 1 lit. a

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.

Antrag: Streichung

Art. 22

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.

Antrag: beibehalten

Art. 11 Abs. 4

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.

Antrag: Streichung

Art. 16b

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.

Antrag: Streichung

Art. 31 Abs. 1

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 51 und 52

Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.

Antrag: beibehalten

Art. 60a

Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde laut den Erläuterungen bewusst auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten. Art. 60a ist zu streichen.

Antrag: Streichung des Artikels

Art. 42a und 43a

Die Art. 42a und 43a führen neu die Abfragetypen «IR_59» und «IR_60» ein, über die sensible Daten automatisiert abgefragt werden können. Sie verlangen von Anbietern, dass sie jederzeit Auskunft geben können bezüglich des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Auch für das Auferlegen dieser Pflicht gilt die fragliche Schwelle von 5'000 Nutzer:innen. Erfasst ist somit nahezu die gesamte AAKD-Landschaft der Schweiz.

Das Problem liegt darin, dass die «IR_»-Abfragen zu Informationen nach Art. 42a und 43a neu automatisiert abgerufen werden können – im Gegensatz zu den «HD_»- (historische Daten) und «RT»- (Echtzeitüberwachung) Abfragen, die strengeren Regeln und einer juristischen Kontrolle unterliegen.

Bei den «IR_59»- und «IR_60»-Abfragen handelt es sich allerdings um sensible Informationen wie etwa das Abrufen einer IP-Adresse. Solche Informationen mussten bislang zurecht über strengere Abfragetypen eingeholt werden. Es ist nicht nachvollziehbar, warum Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber. Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser automatisierten Auskünfte ergibt. Unternehmen sind daher nur unzulänglich geschützt vor missbräuchlichen Anfragen und vor Kosten, die ihnen durch die Pflicht, diese Auskünfte automatisch weiterzugeben, entstehen wird.

Künftig könnten so umfangreiche Informationen über die neuen Abfragetypen beschafft werden, die bislang zurecht den strengerem Regeln der rechtlich sichereren Informations-/Überwachungstypen «HD_» und «RT_» unterworfen waren. «IR_59» und «IR_60» ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne den erforderlichen Kontrollen dieser invasiven Überwachungstypen unterworfen zu sein.

Die Entwicklung, dass mittels «IR_»-Abfragen neu auch personenbezogene sensible Nutzungsdaten eingeholt werden können, widerspricht der Logik der unterschiedlichen Abfragetypen und öffnet Tür und Tor für missbräuchliche Abfragen und eine Echtzeitüberwachung von Millionen von Nutzer:innen. Auch hier stehen grundrechtlich geschützte Ansprüche auf dem Spiel, die mit einer solchen Regelung auf nicht nachvollziehbare Weise untergraben und missachtet werden.

Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind. Die AAKD müssten künftig gewisse Datenkategorien systematisch erheben, um dieser Pflicht nachzukommen. Art. 27 Abs. 2 BÜPF erklärt allerdings, dass AAKD «auf Verlangen die *ihnen zur Verfügung stehenden* Randdaten des Fernmeldeverkehrs der überwachten Person liefern» müssen. Bei einer dahingehenden Auslegung des Bestimmungen bedeutete dies einen weiteren Verstoss gegen das BÜPF.

Unter rechtsstaatlichen Gesichtspunkten gilt es ausserdem die geplante Schwächung der Institution des Zwangsmassnahmengerichts auf das Schärfste zu kritisieren. Mit der Schaffung der zwei neuen Auskunftstypen, die mittels einfacher Auskunftsanfrage automatisch abgerufen werden können, werden rechtliche Kontrollmechanismen wie das Zwangsmassnahmengericht umgangen und der Einflussbereich der Staatsanwaltschaft noch weiter ausgebaut. Art. 42a und 43a sind daher vollumfänglich zu streichen.

Antrag: Streichung der Artikel

Art. 50a

Art. 50a sieht vor, dass Anbieter:innen verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Auch diese Pflicht soll eine Vielzahl neuer Unternehmen erfassen: Betroffen sind nicht mehr nur FDA (Art. 26 BÜPF) und ausnahmsweise AAKD (Art. 27 BÜPF), sondern sämtliche Anbieter:innen mit mehr als 5'000 Nutzer:innen. Im Ergebnis wäre fast die gesamte Schweizer AAKD-Branche betroffen (kaum ein Produkt ist lebensfähig mit weniger als 5'000 Teilnehmer:innen).

Die Ausdehnung dieser Pflicht auf AAKD stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar: Es findet keine Einzelfallprüfung statt und die AAKD werden dieser Pflicht unterworfen, auch wenn sie keineswegs «Dienstleistungen von grosser

wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten», was jedoch gesetzliche Vorgabe ist (Art. 27 Abs. 3 BÜPF).

Problematisch ist zudem, dass aufgrund dieser Vorgabe Anbieter:innen ihrer Verschlüsselungen so konfigurieren müssen, dass sie von ihnen aufgehoben werden können – eine durch Anbieter:innen aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung allerdings in jedem Fall. Dies führt zu schwächeren Verschlüsselungen und der Abnahme der Sicherheit von Kommunikationsdiensten.

Daraus ergibt sich eine Grundrechtsproblematik von erheblicher Tragweite: Das Verhältnismässigkeitsgebot aus Art. 36 BV kann nicht eingehalten werden, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Die Interessenabwägung darf hier nicht zuungunsten der Grundrechtsträger:innen erfolgen, da es sich bei deren Interessen um solche von fundamentalem Gewicht – dem Zugang zu sicherer Kommunikation und damit direkt verbunden dem Recht auf freie Meinungsäusserung – handelt.

Wichtig ist, dass Verschlüsselungen, die auf dem Endgerät der Nutzer:innen erfolgen – also End-zu-End-Verschlüsselungen – nicht unter die Pflicht zur Aufhebung gemäss Art. 50a VE-VÜPF fallen dürfen. Diese Form der Verschlüsselung liegt ausschliesslich in der Sphäre der Nutzer:innen und es wäre untragbar, die Pflicht zur Aufhebung von Verschlüsselungen in dieser Sphäre zu verlangen. Die Anbieter:innen dürfen daher nicht dazu verpflichtet werden, diese Inhalte zu entschlüsseln und zugänglich zu machen. Im Gegensatz dazu betrifft die Transportverschlüsselung «lediglich» die Verbindung zwischen Client und Server und kann von Anbieter:innen kontrolliert werden. Es ist wichtig, dass diese technischen Unterscheidungen und unterschiedlichen Schutzwirkungen und -richtungen bei rechtlichen Umsetzungen beachtet werden. Wir begrüssen die Klarstellung im erläuternden Bericht, dass die End-zu-End-Verschlüsselung vom Anwendungsbereich ausgenommen ist. Es muss jedoch ebenso klar sein, dass das ganze Endgerät von Nutzer:innen aus dem Anwendungsbereich von Art. 50a VE-VÜPF ausgenommen ist.

Es braucht im Übrigen auch eine Klarstellung darüber, dass eine rückwirkende Möglichkeit zur Aufhebung klar ausgeschlossen ist. Eine solche würde de facto eine Vorratsdatenspeicherung verschlüsselter Inhalte und Keys darstellen, die mit dem Prinzip der Datenminimierung (Art. 6 Abs. 3 DSG) und dem Schutz der Privatsphäre (Art. 13 BV) unvereinbar ist.

Antrag: Streichung der «Anbieterin mit reduzierten Pflichten» aus dem Anwendungsbereich sowie eine Klarstellung darüber, dass die Aufhebung von Verschlüsselungen auf dem Endgerät der Nutzer:innen sowie eine rückwirkende Verpflichtung zur Aufhebung ausgeschlossen sind.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Art. 14 Abs. 3 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und wirtschaftlich nicht tragbar, was das Einführen von Fristen obsolet werden lässt. Der Absatz ist daher ersatzlos zu streichen.

Antrag: Streichung

Art. 14 Abs. 4 VD-ÜPF

Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der Unterworfenen AAKD – da auch AAKD mit reduzierten Pflichten erfasst sind – massiv. Dies ist wie bereits ausgeführt weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.

Antrag: Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten»

Art. 20 Abs. 1 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen, ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.

Antrag: Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»

Schlussbemerkung

Trotz des Umfangs dieser Stellungnahme gilt: Das Ausbleiben einer expliziten Bemerkung zu einzelnen Bestimmungen bedeutet keine Zustimmung der Digitalen Gesellschaft. Die Ablehnung der Revision bleibt volumnäiglich bestehen.

Freundliche Grüsse

Erik Schönenberger
Geschäftsleiter

Vernehmlassung

Fernmeldeüberwachung und

mitwirkungspflichtige

Unternehmen

Sehr geehrter Herr Bundesrat Beat Jans,
Sehr geehrte Empfänger,

als sogenannter „Digital Native“ widerspreche ich den gewünschten Forderungen. Sie entsprechen nicht der Art und Weise, wie die Schweiz arbeitet.

Inhaltlich bemängle ich, dass dieser Ausführungserlass ohne Verdacht angewendet werden kann. Es ist für mich akzeptabel, nach Verdacht ein Verfahren analog „Fangschaltungen“ aufzustellen. Allerdings würde hierbei jedermann unter Verdacht gestellt und müsste seine Daten preisgeben.

Formell bemängle ich die Art und Weise, wie dieser Ausführungserlass ohne demokratische Mitwirkung und Referendumsmöglichkeit erlassen wurde. Dass er inhaltlich problematisch ist, zeigt der Fall vor dem Bundesgericht.

Ich wünsche mir, dass wir als Volk (oder zumindest im Parlament) darüber abstimmen können, womit die wichtigen demokratischen Grundwerte der Schweiz gepflegt werden. So kann auch eine notwendige Debatte dazu geführt werden.

Im Weiteren verweise ich auf die Stellungnahme der Digitalen Gesellschaft, welcher ich zustimme. Abrufbar unter: <https://www.digitale-gesellschaft.ch/2025/05/02/bundesrat-will-ueberwachungsstaat-per-verordnung-massiv-ausbauen-stellungnahme-zur-teilrevision-vuepf-und-vd-uepf/>

Freundliche Grüsse
Lukas Röllin

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
CH-3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Solothurn, 6. Mai 2025

Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat Beat Jans
Sehr geehrte Damen und Herren,

Nehmen Bestrebungen zum Datenschutz in Europa allgemein zu, wollen Sie diese in der Schweiz mit Füssen treten. Die Geplanten Änderungen sind weder mit dem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), noch mit dem Datenschutzgesetz (DSG) vereinbar. Ausserdem verstossen sie gegen die Verfassung, die Grundrechte und die Europäische Menschenrechtskonvention (EMRK).

Insbesondere störe ich mich an der Vorratsdatenspeicherung, welche in direktem Widerspruch mit Artikel 6 Abs. 3 des DSG steht, in welchem der Grundatz der Datenminimierung festgehalten ist.

Auch die vorgesehene automatisierung der Abfrage von Auskünften steht in komplettem Widerspruch zur Datenminimierung, da bestehende Hürden abgebaut und voreilige, unter Umständen ungerechtfertige Abfragen gefördert würden.

Als Softwareingenieur in der Branche der Medizinaltechnik bin ich auf sichere Kommunikation angewiesen. Unsere Kunden müssen sich zu hundert Prozent sicher sein, dass unsere Kommunikationskanäle die Privatsphäre einhalten und die Daten nirgendwo anders als bei uns gespeichert werden. Dies würde mit der geplanten Vorratsdatenspeicherung komplett ausgehebelt.

Die Identifizierung der Endnutzer ist bei solch hochsensiblen Daten bereits genügend, damit sich unsere Kunden nicht mehr sicher fühlen würden unsere Kommunikations-kanäle zu nutzen.

Ich Verweise hiermit ebenfalls auf die Stellungnahme der Digitalen Gesellschaft, welche die geplanten Änderungen noch viel Detaillierter kommentiert als ich es könnte und welche ich vollumfänglich unterstütze.

<https://www.digitale-gesellschaft.ch/2025/05/02/bundesrat-will-ueberwachungsstaat-per-verordnung-massiv-ausbauen-stellungnahme-zur-teilrevision-vuepf-und-vd-uepf/>

Aus oben genannten Gründen lehne ich die Revision vollumfänglich und deutlich ab.

Freundliche Grüsse
Mathieu Bourquin

Softwareingenieur für eingebettete Systeme
BSc BFH Elektro- und Kommunikationstechnik

Beni Wattenhofer

[REDACTED]

Dienst Überwachung Post- und Fernmeldeverkehr

Eidgenössisches Justiz- und Polizeidepartement
Bundeshaus West
CH-3003 Bern

Steinhausen, 06.05.2025

Vernehmlassungsantwort Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Ich äussere mich kritisch zur vorgeschlagenen Teilrevision der Verordnungen VÜPF und VD-ÜPF. Zwar ist die Mitwirkung von Fernmelddenstanbietern bei der Strafverfolgung in gewissen Fällen gerechtfertigt, doch die vorgelegte Revision geht zu weit und birgt erhebliche Risiken für den Schutz der Privatsphäre und die digitale Sicherheit in der Schweiz. Die Ausweitung der Überwachungsbefugnisse – insbesondere die neuen Überwachungs- und Auskunftstypen – führt zu einer weiteren Normalisierung tiefgreifender Eingriffe in die Grundrechte.

Zitat Digitale Gesellschaft: "Eine Ausweitung der Überwachung von solch erheblicher Tragweite darf zudem nicht einfach auf Verordnungsstufe geregelt werden. Die Regelungen gehören zwingend in ein Gesetz, müssen vom Parlament erlassen und einer demokratischen Legitimation mittels Referendum unterstellt werden. Der Versuch, dermassen weitreichende Überwachungspflichten auf dem Verordnungsweg einzuführen, stellt einen klaren Verstoss gegen das Legalitätsprinzip dar und untergräbt die Kompetenzordnung."

Ich unterstütze die in der Stellungnahme der "Digitalen Gesellschaft" dargelegten Forderungen nach einer klaren gesetzlichen Verankerung der Netzneutralität in der Schweiz. Ein diskriminierungsfreier Zugang zu Internetdiensten ist grundlegend für Innovation, Meinungsfreiheit und fairen Wettbewerb. Die vorgeschlagenen Massnahmen sind sachlich gut begründet und im Interesse der Allgemeinheit. Ich bitte Sie daher, dieses Anliegen im weiteren Gesetzgebungsprozess zu berücksichtigen.

Ich fordere deshalb den Bundesrat auf, den Schutz der Grundrechte, insbesondere das Fernmeldegeheimnis und die informationelle Selbstbestimmung, in den Vordergrund zu stellen und die Vorlage grundlegend zu überarbeiten.

Besten Dank und freundliche Grüsse,

Beni Wattenhofer

Kantonsrat ALG, Zug

Von: Anselm GMX
Gesendet: Dienstag, 6. Mai 2025 15:08:57 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme Überwachungsgesetz

Guten Tag

Ich halte die Änderung des Überwachungsgesetzes für übertrieben und schädlich.
Folgender Stellungnahme kann ich nur zustimmen.



Freundliche Grüsse
Anselm Püntener

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Allschwil, 06.05.2025

Stellungnahme zu den geplanten Änderungen des Schweizer Überwachungsgesetzes

Sehr geehrter Herr Bundesrat Jans,
Sehr geehrte Damen und Herren

Hiermit möchte ich meine Ablehnung gegenüber der geplanten Änderung des Schweizer Überwachungsgesetzes (VÜPF, VD-ÜPF) zum Ausdruck bringen.

Das geplante Vorhaben zur Änderung ist ein direkter Eingriff, wenn nicht sogar ein Angriff auf den IT-Standort Schweiz. Damit einhergehend werden die Rechtsstaatlichkeit ausgehebelt und Grundrechte aller angegangen. Dies kann nicht im Sinne der Schweiz als Nation, noch als Wirtschaftsstandort sein.

Ich selbst, professionell mit dem Thema Informations- und Cybersicherheit verbunden, sehe keinen Mehrwert der Revision. Technisch gesehen sind die Massnahmen zum grössten Teil nicht umsetzbar. Ethisch sind die Anpassungen keineswegs vertretbar, und in gleichem Zuge eine Gefahr für die Gesellschaft.

Viele in der Schweiz ansässige Technologieunternehmen, welche momentan – durch den international gut positionierten Datenschutz und Schutz der Privatsphäre – den Ruf besitzen besonders die Daten der Benutzerbasis schützen wären vor dem Aus. Dabei geht es nicht nur um Proton oder Threema. Auch firmen wie Tresorit würden sich einen Wegzug nicht bloss in Betracht ziehen, sondern handeln. Zusätzlich – mit der Abwesenheit von Planungssicherheit mit unserem alten Partner USA – wird es künftig eines der wertvollsten Argumente für den Technologie- und Startup-Standort Schweiz sein: Von den USA unabhängig entwickelte Plattformen und Lösungen, welche der restlichen Welt eine Abnabelung von den USA ermöglicht falls gewünscht.

Dies und vieles mehr wird sich mit der geplanten Änderung an den Gesetzen "in Luft auflösen".

Es kann nicht sein, dass ein Staat sich dermassen über die effektive Rechtsstaatlichkeit hinwegsetzen will und dermassen bereitwillig gegen das "hauseigene" Datenschutzgesetz verstossen würde.

Der vorgeschobene Zweck heiligt in diesem Falle keineswegs die Mittel. Man setzt die Zukunft der Kredibilität einer ganzen Nation auf das Spiel.

Freundliche Grüsse

Fabio Lüdi

Von: Mathias Nicolet
Gesendet: Dienstag, 6. Mai 2025 15:42:39 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Vernehmlassungsantwort betreffend VÜPF/VD-ÜPF

Sehr geehrte Empfänger:innen

Anbei erhalten Sie angehängt meine Vernehmlassungsantwort bzw. Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Ich danke Ihnen vielmals für die Kenntnisnahme.

Freundliche Grüsse
Mathias Nicolet

Eidgenössisches Justiz- und Polizeidepartement
(EJPD)
Bundeshaus West
CH-3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Ueberstorf, 06.05.2025

Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat Beat Jans
Sehr geehrte Empfänger:innen

Die geplante Revision der VÜPF ist ein Frontalangriff auf unsere Grundrechte, die Rechtsstaatlichkeit sowie den IT- und Innovationsstandort Schweiz. Deshalb lehne ich die Revision vollumfänglich und in aller Deutlichkeit ab. Zudem ist diese Revision im Widerspruch mit dem Push für eine bessere europäische digitale Souveränität und zerstörerisch schädlich für den Wirtschaftsstandort Schweiz, für Privatsphären fokussierte Unternehmen. Unternehmen wie Proton oder Threema müssten die Schweiz verlassen, welches sicherlich nicht im Sinne der Schweiz ist. Zudem ist die Schweizer Regierung ebenfalls Nutzerin von Threema, das müsste ebenfalls zu bedenken geben, wenn Threema ins Ausland ziehen müsste.

Für vertiefte Informationen, möchte ich auf die Vernehmlassungsantwort der Digitalen Gesellschaft verweisen:

<https://www.digitale-gesellschaft.ch/uploads/2025/05/Stellungnahme-Digitale-Gesellschaft-VUePF-VD-UePF.pdf>

Freundliche Grüsse

Von: Yannic Charlon

Gesendet: Dienstag, 6. Mai 2025 15:57:08 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Vernehmlassungsantwort zu den geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. API-basierte Echtzeit-Überwachung ohne Rechtsschutz

Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmäßigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmäßige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

2. KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich

Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung.

Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat?

Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten compromittieren.

In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

3. Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote

Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

4. Massenüberwachung durch Pattern Matching

„Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

- Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
- Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden?
Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/07/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).

5. Kriminelle umgehen die Massnahmen – Kollaterale Überwachung

Unschuldiger

Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

- Ausländische Dienste ohne solche Vorschriften nutzen.
- Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
- Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

6. Ökonomische Selbstzerstörung und Abwanderung

«Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

- **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
- **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter

- werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
 - **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
 - **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
 - **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen.
Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

7. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

8. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit

Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie

eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Yannic Charlon

Von: Laura Di Giorgio

Gesendet: Dienstag, 6. Mai 2025 16:08:03 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Überwachungsgesetz

Guten Tag

Ich bin als junge Person mit dem Internet aufgewachsen, und habe gesehen, wie meine Mitmenschen ihr Verhalten an die Tatsache angepasst haben, dass das Internet nie vergisst. Ich habe selbst versucht, immer möglichst wenig Informationen von mir irgendwelchen Online-Unternehmen, „Onlinefremden“ oder sonstigen Datenkraken zu überlassen. Aber das ist leider meist zwecklos, irgendetwas gebe ich wohl immer preis.

Aber es ist Grund undemokratisch, wenn die Vertreter, die ich in den Staatsapparat wähle, sich anmasse darüber zu entscheiden, welche Informationen sie von mir abschöpfen wollen. Der Fichen-Skandal war nicht umsonst ein „Skandal“.

Dieser Staat hat seine Bürger zu beschützen, dass gilt auch für unsere Informationen, die sich heute mit AI und Programmen wie Palatir, fröhlich zusammentragen lassen. Ich möchte eben nicht in einem Überwachungsstaat leben. Das Buch „1984“ war als Warnung vor einer Dystopie gemeint, nicht als Anleitung um dahin zu kommen.

Ich lehne grundlose Überwachung von Bürgern als einen massiven Einschnitt in meine Rechte war. Umso mehr, wenn eine solche Überwachung gänzlich undemokratisch am Bürger vorbei entschieden wird. Ich habe nie eingewilligt, dass Datenkraken wie Amazon und Facebook überall meine Daten zusammenkratzen und genauso wenig habe ich Verständnis für diese Entscheidung. Im Gegenteil; ich wünsche mir ein einer digitalen Welt, die immer mehr überwacht wird, einen Staat der meine persönlichen Daten vor anderen UND vor sich schützt.

Zutiefst enttäuscht,
Laura Di Giorgio

Marc Steinmann



marcsteinmann@gmx.net

Eidgenössisches Justiz- und Polizeidepartement EJPD
Informations- und Kommunikationssysteme der Bundesverwaltung (ISC-EJPD)
aemterkonsultationen-uepf@isc-ejpd.admin.ch

Steinach, 06. Mai 2025

Stellungnahme zur Teilrevision VÜPF und VD-ÜPF

Sehr geehrte Damen und Herren

Mit grosser Sorge nehme ich die geplanten Anpassungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) sowie der Verordnung des EJPD über die Durchführung der Überwachung (VD-ÜPF) zur Kenntnis. Ich spreche mich entschieden gegen die Ausweitung der Überwachungspflichten aus und möchte meine Bedenken im Folgenden begründen:

1. Historische Verantwortung und der Fichen-Skandal

Die Schweiz hat in ihrer jüngeren Geschichte bereits schmerhaft erfahren, wohin ausufernde Überwachung führen kann: Der Fichen-Skandal der 1980er Jahre offenbarte, dass unzählige Bürgerinnen und Bürger – insbesondere politisch aktive Menschen – vom Staat ohne hinreichende rechtliche Grundlage überwacht wurden. Dieses historische Beispiel sollte uns Mahnung sein, dass Sicherheitsinteressen niemals die grundrechtlichen Schranken überschreiten dürfen.

2. Eingriffe in Grundrechte

Die geplante Ausweitung der Mitwirkungspflichten auf sogenannte Anbieter abgeleiteter Kommunikationsdienste stellt einen erheblichen Eingriff in die Grundrechte dar, insbesondere in die Privatsphäre (Art. 13 BV) sowie in die Meinungs- und Informationsfreiheit (Art. 16 und 17 BV). Derartige Eingriffe bedürfen einer klaren und spezifischen gesetzlichen Grundlage sowie einer wirksamen demokratischen Kontrolle.

3. Missachtung des Bundesgerichtsurteils

Besonders stossend ist der Umstand, dass der Bundesrat mit dieser Revision offenbar versucht, Regelungen durchzusetzen, die in einem früheren Informationsblatt des Dienstes ÜPF bereits enthalten waren – und vom Bundesgericht im Urteil 2C_544/2020 ausdrücklich als rechtswidrig zurückgewiesen wurden. Dass nun versucht wird, diese Regelungen auf Verordnungsstufe doch noch umzusetzen, wirkt wie eine Umgehung des höchsten Gerichts des Landes.

4. Unterstützung zivilgesellschaftlicher Kritik

Ich schliesse mich den fundierten Bedenken an, die von der Digitalen Gesellschaft in ihrer ausführlichen Stellungnahme vom 2. Mai 2025 geäussert wurden (vgl.

<https://www.digitale-gesellschaft.ch/2025/05/02/bundesrat-will-ueberwachungsstaat-per-verordnung-massiv-ausbauen-stellungnahme-zur-teilrevision-vuepf-und-vd-uepf/>).

Insbesondere teile ich deren Einschätzung, dass die geplante Ausdehnung der Überwachungspflichten einen klaren Gesetzesvorbehalt verletzt und in wesentlichen Punkten weder notwendig noch verhältnismässig ist.

Ich fordere den Bundesrat auf, von der geplanten Revision Abstand zu nehmen. Sollte ein tatsächlicher gesetzgeberischer Handlungsbedarf bestehen, so ist der richtige Weg die Revision des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) unter Einbezug des Parlaments – und damit auch unter dem möglichen Referendum durch die Bevölkerung.

Mit freundlichen Grüßen

Marc Steinmann

Von: Lorenzo Barcarolo
Gesendet: Dienstag, 6. Mai 2025 16:44:05 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

API-basierte Echtzeit-Überwachung ohne Rechtsschutz Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ohne nationale eID. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).

Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.

In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

Massenüberwachung durch Pattern Matching „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. Keyword-Filter (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?

Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren (EFF: Google’s Scans of Private Photos Led to False Accusations of Child Abuse).

Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

Ausländische Dienste ohne solche Vorschriften nutzen.

Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).

Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

Ökonomische Selbstzerstörung und Abwanderung «Diese Verordnung ist wirtschaftlicher Selbstdmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

Kostendruck durch technische Nachrüstung: Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

Abwanderung von Unternehmen: Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und

Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.

Investitionsstopp: Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.

Ausfall von Arbeitsplätzen: Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz: Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.

Rechtliche Risiken und Klagen: Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

Demokratische und rechtliche Missachtung

Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.

Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.

Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos
Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt.
Dieser Widerspruch erzeugt folgende Effekte:

Massive Verlagerung zu E2EE und Self-Hosting: Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.

Verschlüsselung der Metadaten: Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.

Weniger statt mehr Zugriff für Behörden: Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse,

Lorenzo Barcarolo

Von: Marc Berchtold

Gesendet: Dienstag, 6. Mai 2025 16:47:13 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. API-basierte Echtzeit-Überwachung ohne Rechtsschutz Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

2. KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ohne nationale eID. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. Massenüberwachung durch Pattern Matching „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. Keyword-Filter (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

- Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren (EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse).

6. Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

- Ausländische Dienste ohne solche Vorschriften nutzen.
- Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
- Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

8. Ökonomische Selbstzerstörung und Abwanderung «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

- Kostendruck durch technische Nachrüstung: Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
- Abwanderung von Unternehmen: Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- Investitionsstop: Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- Ausfall von Arbeitsplätzen: Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz: Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- Rechtliche Risiken und Klagen: Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmäßige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- Massive Verlagerung zu E2EE und Self-Hosting: Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- Verschlüsselung der Metadaten: Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- Weniger statt mehr Zugriff für Behörden: Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische

Kontrolle und beschädigen die Rechtsstaatlichkeit.

Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Marc Berchtold

Von: Matteo Bossi
Gesendet: Dienstag, 6. Mai 2025 17:09:25 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:
 1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
 2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote** Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal

Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](#)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger** Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleieren (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch](#)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
 - **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
 - **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
 - **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
 - **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
 - **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.
9. **Demokratische und rechtliche Missachtung**
 - Der Verordnungsweg umgeht das Referendumrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
 - Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung

dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.

- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und

wirkungslos Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Matteo Bossi

Von: develmusa

Gesendet: Dienstag, 6. Mai 2025 17:14:51 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

API-basierte Echtzeit-Überwachung ohne Rechtsschutz Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ohne nationale eID. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).

Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.

In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört

das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

Massenüberwachung durch Pattern Matching „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. Keyword-Filter (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?

Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren (EFF: Google’s Scans of Private Photos Led to False Accusations of Child Abuse).

Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

Ausländische Dienste ohne solche Vorschriften nutzen.

Metadaten fälschen oder verschleieren (z. B. IP-Adressen, Standortdaten).

Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

Ökonomische Selbstzerstörung und Abwanderung «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

Kostendruck durch technische Nachrüstung: Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

Abwanderung von Unternehmen: Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.

Investitionsstopp: Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.

Ausfall von Arbeitsplätzen: Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz: Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.

Rechtliche Risiken und Klagen: Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmäßige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

Demokratische und rechtliche Missachtung

Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.

Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmasses würde im Referendum voraussichtlich abgelehnt werden.

Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

Massive Verlagerung zu E2EE und Self-Hosting: Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.

Verschlüsselung der Metadaten: Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.

Weniger statt mehr Zugriff für Behörden: Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse
Dev

Von: Lorenz Bäni
Gesendet: Dienstag, 6. Mai 2025 17:24:32 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren

Die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmäßigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmäßige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:
 1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
 2. Größere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.

3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote** Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](#)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger**
Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch](#)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
 - **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
 - **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
 - **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen

Projekte starten.

- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit:

Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Lorenz Bäni

Von: derya cogendez

Gesendet: Dienstag, 6. Mai 2025 17:28:06 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Consultation sur la révision partielle de l'OSCPT et de l'OME-SCPT – Opposition aux propositions sur le chiffrement et la surveillance

Monsieur Biberstein,

Veuillez trouver ci-dessous ma contribution dans le cadre de la procédure de consultation relative à la révision partielle de l'Ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT) ainsi que de l'Ordonnance sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT).

Je tiens à exprimer mon opposition ferme aux révisions proposées.

L'exigence de suppression des chiffrements appliqués par les fournisseurs — même si les chiffrements de bout en bout sont explicitement exclus — constitue une menace grave pour la vie privée des utilisateurs et pour la sécurité numérique en général. Des données non chiffrées sont, par définition, vulnérables, quel que soit l'acteur qui y a accès. Affaiblir la protection offerte par le chiffrement, même indirectement, augmente considérablement les risques de surveillance abusive, de fuites de données et de cyberattaques. Ce projet va donc à l'encontre du consensus international qui considère le chiffrement comme une pierre angulaire de la confiance dans les communications numériques.

La vie privée est un droit fondamental, protégé par la Constitution fédérale suisse ainsi que par les engagements internationaux de la Suisse en matière de droits humains. Toute extension des pouvoirs de surveillance doit être rigoureusement encadrée, fondée sur un besoin proportionné et clairement démontré — ce qui, en l'état, n'est pas le cas.

Ce projet représente également une menace sérieuse pour l'écosystème technologique suisse. Des entreprises telles que Proton, qui dépassent probablement le seuil de chiffre d'affaires de 100 millions de francs suisses et seraient donc classées dans la catégorie des fournisseurs de services de télécommunication (FST) avec obligations complètes, ainsi que des startups innovantes comme NYMVPN, qui appliquent des principes de « privacy-by-design », pourraient être contraintes de se relocaliser ou de modifier profondément leur modèle économique. Cela porterait atteinte à leur crédibilité, nuirait à l'attractivité du secteur suisse des technologies de la confidentialité, et éroderait la réputation internationale de la Suisse en tant que nation respectueuse de la vie privée.

Avant d'aller plus loin, j'exalte le Département fédéral de justice et police à consulter des acteurs scientifiques et citoyens indépendants, tels que [la Société Numérique](#) et [le Conseil suisse de la science \(CSS\)](#). Leur expertise est essentielle pour garantir que toute évolution législative dans ce domaine reste équilibrée, techniquement fondée et conforme aux valeurs démocratiques de notre pays.

Je vous remercie de l'attention portée à cette contribution.

Cordialement,
Derya Cögendez

Von: Leopold Kohle

Gesendet: Dienstag, 6. Mai 2025 17:39:23 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. API-basierte Echtzeit-Überwachung ohne Rechtsschutz Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ohne nationale eID. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:
 1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
 2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
 3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
 4. Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
 5. Massenüberwachung durch Pattern Matching „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. Keyword-Filter (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie

oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?

- Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren (EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse).

6. Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

- Ausländische Dienste ohne solche Vorschriften nutzen.
- Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
- Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

8. Ökonomische Selbstzerstörung und Abwanderung «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

- Kostendruck durch technische Nachrüstung: Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

• Abwanderung von Unternehmen: Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.

• Investitionsstopp: Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.

• Ausfall von Arbeitsplätzen: Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

• Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz: Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.

• Rechtliche Risiken und Klagen: Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmäßige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

• Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.

• Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.

• Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unaugestattet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- Massive Verlagerung zu E2EE und Self-Hosting: Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- Verschlüsselung der Metadaten: Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- Weniger statt mehr Zugriff für Behörden: Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen

zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Leopold Kohle

Von: paul.gillet@bluewin.ch

Gesendet: Dienstag, 6. Mai 2025 16:43:56 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht

bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Größere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten compromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

4. **Erzwungene Metadaten-Log-Speicherung zerstört**

Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/03/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).

6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung**

Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

- Ausländische Dienste ohne solche Vorschriften nutzen.
- Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
- Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal

Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

- **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
- **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Paul Gillet

Von: Michael Stockler
Gesendet: Dienstag, 6. Mai 2025 17:45:54 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zu den geplanten Änderungen des Schweizer Überwachungsgesetzes

Sehr geehrtes EJPD,

In der heutigen Zeit gibt es nur wenige Möglichkeiten für Privatpersonen, der Massenüberwachung durch Google, Meta und andere Grosskonzerne zu entgehen. Viele der heutigen Privacy-First Anbieter, wie zum Beispiel jener der Email-Adresse, die ich hier verwende, Proton, haben ihren Sitz in der Schweiz und müssten bei Einführung der beiden Ausführungserlasse VÜPF und VD-ÜPF die Schweiz verlassen, was nicht nur das Schweizer Image als Vorreiterin in Sachen Datenschutz schwer schädigen könnte, sondern auch verfolgte Menschen Weltweit gefährdet.

Nach einem Bericht der Netzgesellschaft vom 20.04.2025 würde diese Gesetzesänderung zudem gegen die Bundesverfassung und diverse Gesetze verstossen und dürfte nich einmal umgesetzt werden.

Ich kann den Wunsch der zuständigen Behörden verstehen, kriminelle Vereinigungen einfacher überwachen und ausschalten zu können, aber es ist gerade zu scheinheilig, wenn diese Behörden dabei selbst gegen geltendes Recht verstossen. Eine Überwachung muss möglich sein, ja, aber nicht um jeden Preis und nicht unter Bedingungen, die hunderte Menschenleben und das Selbstbestimmungsrecht von Millionen Menschen weltweit gefährden.

Wenn Sie ein solches Gesetz wollen, machen sie es auf eine Art, die Gesetzeskonform ist und ein Referendum ermöglicht. Es gibt Grenzen in unserer Gesellschaft und hier wurden soeben welche ganz deutlich überschritten.

Vielen Dank für Ihre Kenntnisnahme
Freundliche Grüsse
Michael Stockler

Von: michel

Gesendet: Dienstag, 6. Mai 2025 17:49:04 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:
 1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
 2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote** Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal

Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](#)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger** Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch](#)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
 - **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
 - **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
 - **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
 - **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
 - **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmäßige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.
9. **Demokratische und rechtliche Missachtung**
 - Der Verordnungsweg umgeht das Referendumrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
 - Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung

dieses Ausmasses würde im Referendum voraussichtlich abgelehnt werden.

- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und

wirkungslos Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Michel Müller

Co-Founder & CEO

michel@octigen.com

octigen logo



[LinkedIn](#)

Von: Paul Extermann

Gesendet: Dienstag, 6. Mai 2025 18:02:59 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. ****API-basierte Echtzeit-Überwachung ohne Rechtsschutz**** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation.

Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

2. ****KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich**** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ****ohne nationale eID****. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Größere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) ([\[en.wikipedia.org\]\(https://en.wikipedia.org/wiki/2017_Equifax_data_breach?utm_source=chatgpt.com\)](https://en.wikipedia.org/wiki/2017_Equifax_data_breach?utm_source=chatgpt.com)) würde Nutzerdaten kompromittieren.

3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote**
Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

* Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?

* Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse] (<https://www.eff.org/deeplinks/2022/08/googles-scans-private-photos-led-false-accusations-child-abuse>)).

6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger***
Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

* Ausländische Dienste ohne solche Vorschriften nutzen.

* Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).

* Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch] (<https://www.watson.ch/digital/wirtschaft/517198902-proton-schweiz-chef-andy-yen-zum-ausbau-der-staatlichen-ueberwachung>)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

* **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

* **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.

* **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.

* **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

* **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das

fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.

* **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. **Demokratische und rechtliche Missachtung**

* Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.

* Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.

* Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. **Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos**: Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

* **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.

* **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.

* **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit: Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Paul Extermann

Von: Ben O'Sullivan

Gesendet: Dienstag, 6. Mai 2025 18:20:36 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmäßigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmäßige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:
 1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
 2. Größere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote** Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartner** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal

Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](#)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger Terroristen** und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch](#)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
 - **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
 - **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
 - **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
 - **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
 - **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmäßige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.
9. **Demokratische und rechtliche Missachtung**
 - Der Verordnungsweg umgeht das Referendumrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
 - Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung

dieses Ausmasses würde im Referendum voraussichtlich abgelehnt werden.

- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Benjamin O'Sullivan

Von: Nils Zbinden

Gesendet: Dienstag, 6. Mai 2025 18:14:54 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden die Grundrechte der Bevölkerung und den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob sich die Schwelle auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:
 1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
 2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio.

betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.

3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote**
Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. **Massenüberwachung durch Pattern Matching**, „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/07/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung**
Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken.
8. **Ökonomischer Schaden und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
 - **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
 - **Investitionsstopp:** Risikokapitalgeber ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
 - **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
 - **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne

flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.

- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle und beschädigen die Rechtsstaatlichkeit. Ich bitte Sie um Prüfung, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Nils Zbinden

Von: Koen Bruijn

Gesendet: Dienstag, 6. Mai 2025 18:30:34 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Vernehmlassung zur Teilrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und der Verordnung des EJPD über deren Durchführung (VD-ÜPF)

Sehr geehrte Damen und Herren

Als technikaffiner Bürger und Lernender im Bereich Elektronik und Informatik nehme ich mit grosser Sorge Kenntnis von der geplanten Ausweitung der Überwachungspflichten im Rahmen der Teilrevision der VÜPF und VD-ÜPF.

Die vorgesehenen Änderungen stellen nicht nur einen eklatanten Verstoss gegen Grundrechte wie den Schutz der Privatsphäre (Art. 13 BV, Art. 8 EMRK) dar, sondern bedrohen auch den Innovations- und Wirtschaftsstandort Schweiz nachhaltig. Die Schwellenwerte von lediglich 5'000 Nutzer:innen, ab denen bereits massive Überwachungspflichten greifen sollen, sind vollkommen unverhältnismässig und realitätsfremd. Sie treffen nicht nur Konzerne, sondern auch Open-Source-Projekte, Non-Profits, Start-ups und datenschutzfreundliche Dienste – also genau jene Akteure, die eine demokratische und digitale Gesellschaft stärken sollten.

Ich schliesse mich der fundierten Stellungnahme der **Digitalen Gesellschaft** (siehe Anhang) vollumfänglich an und lehne die geplanten Revisionen entschieden ab. Der Versuch, einen derart weitreichenden Umbau unseres Kommunikationsrechts **per Verordnung statt durch Gesetzgebung** zu erzwingen, ist ein verfassungswidriger Missbrauch der politischen Verfahren und untergräbt die demokratische Kontrolle.

Es braucht mehr Rechtsstaatlichkeit, nicht weniger. Sicher in unserem gegenwärtigen geopolitischen Klima. Ich fordere den Bundesrat daher auf, die geplanten Änderungen zurückzuziehen und eine offene politische Debatte im Rahmen des ordentlichen Gesetzgebungsverfahrens zu führen.

Freundliche Grüsse

Koen Bruijn

Anhang: Stellungnahme der Digitalen Gesellschaft vom 2. Mai 2025

Digitale Gesellschaft, CH-4000 Basel

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
CH-3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Basel, 2. Mai 2025

Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat Beat Jans
Sehr geehrte Empfänger:innen

Am 29. Januar 2025 eröffnete der Bundesrat die Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF). Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Vorentwurf wie folgt Stellung:

Vorbemerkung

Die geplante Revision der VÜPF ist ein Frontalangriff auf unsere Grundrechte, die Rechtsstaatlichkeit sowie den IT- und Innovationsstandort Schweiz.

Mit ihrer Umsetzung würde geltendes Recht in einem Ausmass verletzt, das alarmieren muss: Die Revision ist in vielerlei Hinsicht unvereinbar mit dem Bundesgesetz betreffend die Überwachung des

Post- und Fernmeldeverkehrs (BÜPF), verstösst gegen das Datenschutzgesetz (DSG), steht in klarem Widerspruch zu den verfassungsmässigen Grundrechten und verstösst gegen Völkerrecht. Die vorgesehenen Änderungen führen zu einer massiv ausgeweiteten Überwachung – ganz grundsätzlich und flächendeckend. Dies ist mit der Ausrichtung des BÜPF, das eine fein austarierte Interessenabwägung zwischen Freiheit und Privatsphäre einerseits und Sicherheit durch Überwachungsmassnahmen andererseits verfolgt, absolut nicht vereinbar.

Die Auswirkungen auf den Wirtschafts- und Innovationsstandort Schweiz wären verheerend: Die Ausweitung der Überwachung und die damit verbundenen, übermässigen Mitwirkungspflichten machen die Schweiz für IT-Anbieter äusserst unattraktiv. Renommierte Unternehmen wie Proton oder Threema, deren Geschäftsmodelle durch die Vorlage direkt ins Visier geraten, würden in ihrer Existenz bedroht. Die ersten Konsequenzen sind bereits sichtbar: Proton hat angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen (siehe [Tages-Anzeiger vom 1. April 2025](#)). Der Chef des Unternehmens erklärte in einem Interview: «Diese Entscheidung ist wirtschaftlicher Selbstmord für die Schweiz» ([watson.ch vom 9. April 2025](#)). Ähnlich äussert sich Threema-Chef Robin Simon: «Der Wirtschaftsstandort würde durch die Revision geschwächt und für Tech-Start-ups unattraktiv.» Aktuell lasse sich Threema alle Optionen offen ([Tages-Anzeiger vom 8. April 2025](#)). Diese Warnzeichen sind ernst zu nehmen und zeigen das verheerende Ausmass der geplanten Revision.

Neben den verheerenden wirtschaftlichen Auswirkungen wird gleichzeitig der grundrechtlich garantierte Anspruch auf sichere und vertrauliche Kommunikation ausgehöhlt. Wenn Anbieterinnen abwandern, bleibt jedoch – als wäre dies nicht genug – nicht nur privaten Nutzer:innen der Zugang zu geschützten Kommunikationsmitteln verwehrt.

Ebenso betroffen sind auch Personen, die einem Berufsgeheimnis unterstehen, wie Journalistinnen oder Anwälte. Die Änderungen treffen zudem schutzbedürftige Personengruppen besonders hart: Whistleblower:innen, Menschen mit ungeklärtem Aufenthaltsstatus oder ohne Papiere aber auch Aktivist:innen verlieren ebenso den Zugang zu vertraulichen Kommunikationsmitteln. Die Revision ignoriert diese Schutzbedürfnisse und erweitert stattdessen die Eingriffsbefugnisse des Staates in einer Weise, die hochgefährlich ist.

Besonders widersprüchlich erscheint das Vorgehen des Bundes angesichts der Tatsache, dass ausgerechnet der Bundesrat selbst Threema als Messenger nutzt – ein Dienst, den er nun faktisch aus dem Markt drängt. Damit sägt die Regierung ausgerechnet an jenem Ast, auf dem sie in Sachen sicherer Kommunikation bislang selbst sitzt.

Hinzu kommt: Die geplanten Regelungen sind technisch unausgereift, unnötig komplex und in Teilen schlüssig nicht umsetzbar. Vielmehr wird ein kaum noch durchschaubares Normengeflecht geschaffen, das weder den Mitwirkungspflichtigen noch den Betroffenen ein Mindestmass an Rechtsklarheit bietet. Die Revision wird ausserdem präsentiert, als handle es sich dabei um Änderungen zur besseren Überblickbarkeit der Rechtslage und zur Schaffung von mehr Rechtssicherheit - tatsächlich aber wird der persönliche Anwendungsbereich der Mitwirkungspflichtigen enorm erweitert und eine Vielzahl neuer Anbieterinnen in den Kreis der Mitwirkungspflichtigen einbezogen. Von Transparenz kann nicht die Rede sein.

Es ist im Übrigen nicht haltbar, dass eine dermassen breit angelegte Ausweitung von Pflichten auf Verordnungsstufe angelegt wird. Solch einschneidende Veränderungen mit weitreichenden Konsequenzen sind in Gesetzesform zu erlassen. Der Bundesrat überschreitet seine Kompetenzen hier um ein Weites.

Diese Vorlage schwächt nicht nur den Innovations- und Wirtschaftsstandort Schweiz – sie untergräbt gleichzeitig im grossen Stil verfassungsmässig geschützte Rechte. Aus grundrechtlicher, datenschutzrechtlicher und gesellschaftspolitischer Sicht ist sie schlicht inakzeptabel. Die geplanten Änderungen stehen dem erklärten Ziel von mehr Freundlichkeit sowie allgemeinen rechtsstaatlichen Grundsätzen sowie Schutzbedürfnissen Einzelner diametral entgegen.

Deshalb lehnen wir die Revision vollumfänglich und in aller Deutlichkeit ab.

Bemerkungen zu einzelnen Artikeln der VÜPF

Alle Artikel

Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung (Art. 6 Abs. 3 DSG) gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kund:innen auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.

Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.ä. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.

Antrag: Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.

Art. 16b Abs. 1

Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile (Art. 16b Abs. 1 lit. b Ziff. 2 VE-VÜPF) wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Mitwirkungspflichten in Kauf nehmen.

Dazu kommt, dass das Kriterium bezüglich der Überwachungsaufträge nicht vom BÜPF gestützt wird, denn: Die Anzahl von Überwachungsaufträgen ist von der wirtschaftlichen Bedeutung einer FDA völlig losgelöst. Die wirtschaftliche Bedeutung ist aber gemäss Art. 26 Abs. 6 BÜPF ausschlaggebend dafür, ob eine FDA von den vollen Pflichten (teilweise) befreit werden kann. Im Umkehrschluss ist die wirtschaftliche Bedeutsamkeit somit Erfordernis für die Auferlegung von vollen Pflichten. Wenn eine FDA nun aber rein aufgrund einer bestimmten Anzahl von Überwachungsaufträgen nach Art. 16b Abs. 1 lit. b Ziff. 1 VE-VÜPF als vollpflichtige FDA qualifiziert wird, steht dies im Widerspruch zum BÜPF und entbehrt damit einer Rechtsgrundlage.

Dieses bereits in der aktuellen Version der VÜPF vorhandene Problem sollte im Zuge einer Revision nicht bestehen bleiben, sondern muss behoben werden.

Antrag: Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter

Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.» Es ist auf die Regelung in Art. 26 Abs. 6 BÜPF abzustellen und eine Einzelfallbetrachtung zur Einstufung vorzunehmen.

Art. 16c Abs. 3

Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als «natürliche» Schutzmechanismen gegen eine übermässige oder missbräuchliche Nutzung solcher Massnahmen durch die Untersuchungsbehörden. Die automatisierte Erteilung von Auskünften ist unverhältnismässig und widerspricht dem Prinzip der Datenminimierung. Die pauschale und undifferenzierte Regel beeinträchtigt zwangsläufig den Grundrechtsschutz.

Der vorgesehene Umsetzungszeitraum von 12 Monaten zur Umsetzung eines dermassen komplexen Systems ist ausserdem völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.

Antrag: Streichung von lit. a «automatisierte Erteilung der Auskünfte» (ebenso in Art. 18 Abs. 2).

Art. 16d

Gemäss erläuterndem Bericht stellen Kommunikationsdienste, die nicht zu den in Art. 16a Abs. 1 aufgezählten Fernmeldediensten gehören und auf die die Ausnahmen nach Art. 16a Abs. 2 nicht zutreffen, abgeleitete Kommunikationsdienste dar. Diese klarere Definition des Begriffs AAKD ist begrüssenswert, doch ist die Konkretisierung der abgeleiteten Kommunikationsdienste im erläuternden Bericht einerseits rechtsstaatlich problematisch und andererseits geht die neue Auslegung nach den Ausführungen im erläuterndem Bericht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdielen wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter etc.) genutzt werden.

Art. 2 lit. c BÜPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft jedoch auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug in die Auslegung unrechtmässig ist – auch hier setzt sich die Revision inakzeptabel über die gesetzlichen Vorgaben des BÜPF hinweg. Onlinespeicherdielen sind deshalb aus Art. 16d zu streichen.

Zudem anerkennt der erläuternde Bericht zwar, dass VPNs zur Anonymisierung der Nutzer:innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil angebrachte Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Das Bedürfnis, auch künftig VPN-Dienste in Anspruch nehmen zu können, ist zu schützen und darf nicht vereitelt werden. Anbieter von VPNs sind daher ebenfalls aus Art. 16d auszunehmen.

Es ist irritierend, dass die bewusst separat ausgestalteten Kategorien AAKD und FDA einander zunehmend angeglichen werden, und zwar zuungunsten der AAKD, die als Kategorie mit grundsätzlich weniger weitreichenden Pflichten als die FDA konzipiert wurde. Dies missachtet den Willen des Gesetzgebers, den es zu wahren gilt.

Antrag: Streichung von Onlinespeicherdiensten und VPN-Anbieterinnen aus der Aufzählung der möglichen abgeleiteten Kommunikationsdienste in den Ausführungen zu Art. 16d im erläuternden Bericht und in der Auslegung.

Art. 16e, Art. 16f und Art. 16g

Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch komplett entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung mit deutlich erweiterten Pflichten. Entscheidend ist, dass neuerdings das Kriterium von 5'000 Nutzer:innen allein zum Auferlegen massiver Überwachungspflichten ausreicht: Erreicht eine AAKD diese Grösse, fällt sie neu in die Kategorie der AAKD mit reduzierten Pflichten und untersteht somit bereits sehr weitgehenden Mitwirkungspflichten, insbesondere der Identifikationspflicht.

Die Einführung von 5'000 Nutzer:innen als gesondert zu beurteilende Untergrenze verletzt Art. 27 Abs. 3 BÜPF, denn 5'000 Personen sind keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strengereren Überwachungsmassnahmen, gerechtfertigt wären. 5'000 Nutzer:innen werden in der digitalen Welt vielmehr sehr rasch erreicht – die Revision verkennt technische Realitäten.

Zusätzlich führt das Einführen eines Konzernatbestandes in Art. 16f Abs. 3 zu massiven Problemen: Produkte und Dienste müssen nicht mehr für sich allein bestimmte Schwellenwerte erreichen – es genügt, wenn das Mutterunternehmen oder verbundene Gesellschaften diese überschreiten. Insbesondere bei Unternehmen mit Beteiligungsstrukturen führt dies dazu, dass sämtliche Angebote pauschal der höchsten Überwachungsstufe unterstellt werden – unabhängig davon, ob sich einzelne Dienste noch im frühen Entwicklungsstadium befinden oder faktisch kaum genutzt werden. Somit müsste jedes neue Projekt von Beginn an mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden, was Innovation behindert. Zudem missachtet der Konzernatbestand das Verhältnismässigkeitsgebot: Unterschiedliche organisatorische Einheiten mit eigenständigen Angeboten werden unrechtmässig zusammengefasst, obwohl sie individuell zu prüfen wären. Die Anwendung starrer Schwellen auf ganze Konzerne statt auf einzelne Dienste umgeht eine notwendige Einzelfallprüfung.

Eine solche Regelung stünde sodann *im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali*, das die zu seltene Anwendung von Downgrades kritisierte:

«Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»

Statt KMU zu entlasten, führt die Revision neu zu einem «automatischen» *Upgrade per Verordnung ohne Verfügung* (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.

Eine Analyse der offiziellen VÜPF-Statistik unterstreicht diese offensichtliche Unverhältnismässigkeit. Im Jahr 2023 betrafen 98,97% der total 9'430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,03% für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,74% wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100% des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.

Die neue Vorlage schliesst nun ebenfalls sowohl die Registrierung via normaler E-Mail als auch die komplett anonyme Registrierung (z. B. Signal oder Telegram) aus, da AAKD bereits mit reduzierten Pflichten neu automatisch zwingend die Endnutzer:innen identifizieren müssen. Hiervon betroffen sind nicht nur alle AAKD mit reduzierten Pflichten, sondern auch all deren Wiederverkäufer. Faktisch resultiert das Gesetz somit darin, dass man sich bei keinem Dienst mehr anmelden können soll, ohne den Pass, Führerschein oder die ID entweder direkt oder indirekt zu hinterlegen. Dass Nutzer:innen künftig hierzu gezwungen wären, stellt einen massiven Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 BV) dar und ist unzumutbar.

Ein weiteres Kernproblem, das die automatische Hochstufung mit sich bringt, ist die Rechtsunsicherheit. Die Vorlage will mit klarer definierten Kategorien und Pflichten ein übersichtlichere Situation schaffen, verfehlt dieses Ziel jedoch gänzlich. Bislang fand die Hochstufung per Verfügung statt, wodurch es für die Mitwirkungspflichtigen klar erkennbar war, wann sie unter welche Pflichten fallen. Ausserdem bewirkt diese Praxis eine sinnvolle Einzelfallbetrachtung anstelle pauschaler und unzweckmässiger automatischer Hochstufungen. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den massgebenden Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes kann aber im Zweifelsfall nur schwer zu beantworten sein. Gerade deshalb besteht ein schutzwürdiges Interesse der Anbieter an Klarheit über ihre Pflichten, da sie fortan eventuell die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Diese Umstrukturierung lässt ich nicht mit der Funktionsweise von Verwaltungsverfahren vereinbaren. Die Pflicht zur Abklärung, wann eine Hochstufung vorliegt und was diese für das Unternehmen bedeutet, darf nicht in die Verantwortung der Unternehmen fallen. Der Staat zieht sich hier aus der Verantwortung und schiebt diese den Unternehmen zu, wodurch diesen zwangsläufig zeitlicher und finanzieller Mehraufwand entsteht. Von einer automatischen Hochstufung von AAKD ist daher abzusehen.

Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.

Gegenüber der geltenden VÜPF *erweitert die Revision die Pflichten zur Automatisierung noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragetypen wie z. B. "IR_59" und "IR_60", welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen.* Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.

Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 lit. b der geltenden VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grosse[n] Teil ihrer

Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. *Damit fallen auch Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz.*

Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Auch hiermit werden neue Hürden für Innovation geschaffen. Die Regelung ist unverhältnismässig und nicht sachdienlich.

Auch Non-Profit-Organisationen geraten unter die verschärften Vorgaben. Unter den neuen Kriterien wird aber allein auf die Anzahl der Nutzer:innen abgestellt für die Einstufung als AAKD. Dieses Kriterium greift jedoch zu kurz: Es berücksichtigt insbesondere nicht die wirtschaftliche Tragfähigkeit der Anbieter:innen. Gerade bei Open-Source- und Non-Profit-Lösungen mit grosser Reichweite, aber geringem Budget, führt dies zu einer verheerenden finanziellen Belastung: Anbieter:innen mit solchen Projekten würden gezwungen, umfangreiche Überwachungsmassnahmen einzuführen. Solche Anbieter:innen würden gezielt aus dem Schweizer Markt gedrängt, während gleichzeitig bestehende Monopole wie WhatsApp (96% Marktanteil in der Schweiz) gestärkt würden.

Es muss ausserdem klar festgehalten werden, dass sich das BÜPF und die VÜPF nur auf Anbieter:innen beziehen können, die in der Schweiz tatsächlich tätig sind. Die Erlasse dürfen nicht so ausgelegt werden, dass sie eine extraterritoriale Wirkung entfalten und internationale Dienste wie Signal, WhatsApp oder Microsoft Teams erfasst sind.

Das Kriterium der reinen Nutzer:innenzahl ist ungeeignet und muss gestrichen werden.

Die Regelung schwächt auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade us-amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger:innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, End-zu-End-verschlüsselter Kommunikation ist heute wichtiger denn je und fällt in den Bereich grundrechtlich geschützter Ansprüche, die es zu wahren gilt. Diese Ansprüche dürfen nicht aufs Spiel gesetzt werden, um ein knallhartes Überwachungsregime der Kommunikation in der Schweiz durchzusetzen – die Prioritäten werden höchst fragwürdig gesetzt.

Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade illegal ist (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer:innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, diese zu erhebenden Datenmengen sind von enormem Ausmass und bergen folglich massive Risiken für Hackerangriffe.

Des Weiteren ist nicht belegt, dass die Speicherung der betreffenden Daten zu spürbar mehr erfolgreichen Ermittlungen führt. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmisshandlung via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfüge, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.

Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren. Diese Handhabe bedeutet einen Verstoss gegen das Legalitätsprinzip und untergräbt legislative Kompetenzen. Ausserdem verfügt die Schweiz bereits über reichlich Mittel zur Aufklärung und Verfolgung von Straftaten, die Behörden können bereits heute auf sicherheitsrelevante Daten zurückgreifen. Unternehmen wie Proton (s. «Positionspapier zur Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)» von Proton) kooperieren seit Jahren mit den Schweizer Strafverfolgungsbehörden und dem Nachrichtendienst des Bundes (NDB). Wenn nun solche Unternehmen aus bereits genannten Gründen zur Abwanderung gezwungen werden, bewirkt die Revision auch hier das genaue Gegenteil ihrer erklärten Ziele: Anstatt der Schaffung besserer Möglichkeiten zur Strafverfolgung würden die Schweizer Behörden wie etwa Fedpol den Zugriff auf wichtige Partner bei der Beschaffung sicherheitsrelevanter Daten verlieren.

Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Integrität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.

Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das DSG. Der Entwurf bringt nicht, wie der Begleitbericht den Leser:innen weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit, steht in direktem Gegensatz zum besagten Postulat 19.4031 und bedeutet massive Eingriffe in grundrechtlich geschützte Sphären, sowohl von Unternehmen als auch von Nutzer:innen.

Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen und das bestehende System muss beibehalten werden.

Antrag: Streichung der Artikel und Beibehaltung der bestehenden Kriterien und der zwei Kategorien von AAKD. + Ausnahmen für Pilotprojekte (auch von grossen Firmen) und Non-Profits per se. Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).

Art. 16h

Art. 16h konkretisiert die Kategorie der «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» aus Art. 2 lit. e BÜPF. Die Vorschrift verfehlt ihr Ziel – anstatt Unsicherheiten darüber zu beheben, wer unter diese Kategorie fällt, schafft sie weitere Unklarheiten. Der schwammig formulierte Verordnungstext könnte dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist:innen, Whistleblower:innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber:innen solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer:innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen.

Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt. Die Unklarheit bezüglich der Einordnung von TOR-Servers wirft weitere Fragen auf, denn wenn TOR nicht als PZD zu qualifizieren

ist, müsste TOR – gleich wie die VPNs – der Kategorie der AAKD zugeordnet werden. Somit stünden Betreiber:innen von TOR-Servern – wie etwa die Digitale Gesellschaft – unter der Identifikationspflicht. Diese ist jedoch, wie dargelegt, nicht umsetzbar.

Es braucht somit entweder die Zusicherung, dass Betreiberinnen von TOR-Nodes nicht dem BÜPF und der VÜPF unterstellt sind oder aber Kategorien von Mitwirkungspflichten, die so gestaltet sind, dass ein:e Betreiber:in eines TOR-Nodes nicht einer Identifikationspflicht unterstellt wird – z. B. indem die Schwelle für das Auferlegen der Identifikationspflicht auf 1 Mio. Nutzer:innen angehoben wird.

Wären Betreiber:innen von TOR-Nodes von der Identifikationspflicht erfasst, würde dies fundamentale Grundrechte wie das Recht auf Privatsphäre und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK), die Meinungs- und Informationsfreiheit (Art. 16 BV, Art. 10 EMRK) gefährden. Ebenso würde das datenschutzrechtliche Prinzip der Datensicherheit (Art. 8 DSG) komplett unterlaufen. Diese Eingriffe in national und international geschützte Rechtsansprüche sind nicht hinzunehmend.

Dieser potentielle Angriff auf die genannten Grundrechte ist hochproblematisch und setzt ein politisches Statement: Die Schweiz bewegt sich weg von Grundrechtsschutz hin zum hochgerüsteten Überwachungsstaat.

Antrag: Es muss sichergestellt werden, dass Technologien wie TOR oder I2P nicht vom Anwendungsbereich der VÜPF erfasst sind.

Art. 16h Abs. 2

Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Endbenutzer:innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 VE-VÜPF: Gemäss diesem Artikel trägt die das WLAN erschliessenden FDA die Verantwortung zur Identifikation der Nutzer:innen. Die Regelung führt also dazu, dass FDA, die einen Vertrag haben mit «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» (PZD), sehr schnell für die Identifikation der Endnutzer:innen ihrer Vertragspartner zuständig sind. Diese Regelung ist unsinnig und schlicht nicht umsetzbar.

Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer:innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24), die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22) oder der Verwendung von IPv6. Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDA unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden.

Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten: FDA resp. Anbieterinnen von öffentlichen WLAN-Zugängen dürfen nur unter einer Identifikationspflicht stehen, wenn die PZD, die den Zugang der FDA nutzt, «professionell betrieben» ist – und zwar nach der aktuellen Auslegungsform (s. Erläuternder Bericht zur (letzten)Totalrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs):

«Mit «professionell betrieben» ist gemeint, dass eine FDA oder eine auf öffentliche WLAN-Zugangspunkte spezialisierte IT-Dienstleisterin den technischen Betrieb des öffentlichen WLAN-

Zugangspunktes durchführt, die dies auch noch für andere öffentliche WLAN-Zugangspunkte an anderen Standorten macht. Wenn eine natürliche oder juristische Person an ihrem Internetzugang selbst einen öffentlichen WLAN-Zugangspunkt technisch betreibt und diesen Zugang Dritten zur Verfügung stellt, muss die FDA, die den Internetzugang anbietet, keine Identifikation der Endbenutzenden sicherstellen.»

So wird sichergestellt, dass FDA nicht unmöglich umzusetzenden Pflichten unterstellt werden.

Antrag: Streichung der Ausführung im erläuternden Bericht. Das Kriterium «professionell betrieben» ist nach der bislang geltenden Regelung zu verstehen. Art. 16h Abs. 2 ist ersatzlos zu streichen und im Zusammenhang mit Art. 19 Abs. 2 ist auf die aktuelle Definition von «professionell betrieben» abzustellen.

Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2

Bei Konzernen knüpft die VE-VÜPF nicht mehr an die Umsatz- und Nutzer:innenzahlen des betroffenen Unternehmens an, neu sind die Zahlen des Konzerns ausschlaggebend für eine Hoch- oder Herunterstufung. Die Begründung, dies diene der Vereinfachung, ist unlogisch und irreführend: Unternehmen müssen ihre Zahlen ohnehin produktbezogen ausweisen, die nötigen Daten liegen also längst vor. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.

Antrag: Streichung des «Konzernatbestand» und Beibehaltung der bestehenden Regelung.

Art. 19 Abs. 1

Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD – erfasst sind die AAKD mit reduzierten und mit vollen Pflichten – widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht. Durch die neuen Schwellenwerte zur Einstufung findet eine beachtliche Ausweitung der Identifikationspflicht statt.

Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des DSG, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch insbesondere der Grundrechtsschutz von Nutzer:innen in der Schweiz massiv beeinträchtigt wird. Die Identifikationspflicht greift immens in das Recht auf informationelle Selbstbestimmung ein und hält einer Grundrechtsprüfung nach Art. 36 BV schon allein aufgrund ihrer Unverhältnismässigkeit nicht stand.

Bezüglich einschneidender Pflichten, die potentiell schwere Grundrechtseingriffe bedeuten – wie es bei Identifikationspflichten zweifellos der Fall ist – muss Rechtsetzung in jedem Fall mit äusserster Sorgfalt und unter strenger Beachtung des Verhältnismässigkeitsgebots erfolgen. Außerdem darf sich eine solche Pflicht nicht über gesetzliche Vorgaben, wie in diesem Fall vom BÜPF vorgegeben, hinwegsetzen.

Durch die breite Auferlegung einer solchen Pflicht werden datenschutzfreundliche Unternehmen bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird. Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Nur so können datenschutzrechtliche Vorgaben und die Rechte Betroffener gewahrt werden.

Antrag: Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation von Teilnehmenden.

Art. 18

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 19 Abs. 2

Das Kriterium «professionell betrieben» ist nach der bestehenden Regelung auszulegen (s. vorstehen). Es sei ausserdem darauf hingewiesen, dass sich aus dieser Regelung eine vertragsrechtliche Problematik zwischen den FDA und den PZD ergeben würde, die nicht tragbar ist.

Antrag: Auslegung des Kriteriums «professionell betrieben» nach der bestehenden Regelung und nicht i. S. v. Art. 16h Abs. 2.

Art. 21 Abs. 1 lit. a

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.

Antrag: Streichung

Art. 22

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.

Antrag: beibehalten

Art. 11 Abs. 4

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.

Antrag: Streichung

Art. 16b

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.

Antrag: Streichung

Art. 31 Abs. 1

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 51 und 52

Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.

Antrag: beibehalten

Art. 60a

Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde laut den Erläuterungen bewusst auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorverurteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten. Art. 60a ist zu streichen.

Antrag: Streichung des Artikels

Art. 42a und 43a

Die Art. 42a und 43a führen neu die Abfragetypen «IR_59» und «IR_60» ein, über die sensible Daten automatisiert abgefragt werden können. Sie verlangen von Anbietern, dass sie jederzeit Auskunft geben können bezüglich des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Auch für das Auferlegen dieser Pflicht gilt die fragliche Schwelle von 5'000 Nutzer:innen. Erfasst ist somit nahezu die gesamte AAKD-Landschaft der Schweiz.

Das Problem liegt darin, dass die «IR_»-Abfragen zu Informationen nach Art. 42a und 43a neu automatisiert abgerufen werden können – im Gegensatz zu den «HD_»- (historische Daten) und «RT»- (Echtzeitüberwachung) Abfragen, die strengeren Regeln und einer juristischen Kontrolle unterliegen.

Bei den «IR_59»- und «IR_60»-Abfragen handelt es sich allerdings um sensible Informationen wie etwa das Abrufen einer IP-Adresse. Solche Informationen mussten bislang zurecht über strengere Abfragetypen eingeholt werden. Es ist nicht nachvollziehbar, warum Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber. Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser automatisierten Auskünfte ergibt. Unternehmen sind daher nur unzulänglich geschützt vor missbräuchlichen Anfragen und vor Kosten, die ihnen durch die Pflicht, diese Auskünfte automatisch weiterzugeben, entstehen wird.

Künftig könnten so umfangreiche Informationen über die neuen Abfragetypen beschafft werden, die bislang zurecht den strengerem Regeln der rechtlich sichereren Informations-/Überwachungstypen «HD_» und «RT_» unterworfen waren. «IR_59» und «IR_60» ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne den erforderlichen Kontrollen dieser invasiven Überwachungstypen unterworfen zu sein.

Die Entwicklung, dass mittels «IR_»-Abfragen neu auch personenbezogene sensible Nutzungsdaten eingeholt werden können, widerspricht der Logik der unterschiedlichen Abfragetypen und öffnet Tür und Tor für missbräuchliche Abfragen und eine Echtzeitüberwachung von Millionen von Nutzer:innen. Auch hier stehen grundrechtlich geschützte Ansprüche auf dem Spiel, die mit einer solchen Regelung auf nicht nachvollziehbare Weise untergraben und missachtet werden.

Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind. Die AAKD müssten künftig gewisse Datenkategorien systematisch erheben, um dieser Pflicht nachzukommen. Art. 27 Abs. 2 BÜPF erklärt allerdings, dass AAKD «auf Verlangen die *ihnen zur Verfügung stehenden* Randdaten des Fernmeldeverkehrs der überwachten Person liefern» müssen. Bei einer dahingehenden Auslegung des Bestimmungen bedeutete dies einen weiteren Verstoss gegen das BÜPF.

Unter rechtsstaatlichen Gesichtspunkten gilt es ausserdem die geplante Schwächung der Institution des Zwangsmassnahmengerichts auf das Schärfste zu kritisieren. Mit der Schaffung der zwei neuen Auskunftstypen, die mittels einfacher Auskunftsanfrage automatisch abgerufen werden können, werden rechtliche Kontrollmechanismen wie das Zwangsmassnahmengericht umgangen und der Einflussbereich der Staatsanwaltschaft noch weiter ausgebaut. Art. 42a und 43a sind daher vollumfänglich zu streichen.

Antrag: Streichung der Artikel

Art. 50a

Art. 50a sieht vor, dass Anbieter:innen verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Auch diese Pflicht soll eine Vielzahl neuer Unternehmen erfassen: Betroffen sind nicht mehr nur FDA (Art. 26 BÜPF) und ausnahmsweise AAKD (Art. 27 BÜPF), sondern sämtliche Anbieter:innen mit mehr als 5'000 Nutzer:innen. Im Ergebnis wäre fast die gesamte Schweizer AAKD-Branche betroffen (kaum ein Produkt ist lebensfähig mit weniger als 5'000 Teilnehmer:innen).

Die Ausdehnung dieser Pflicht auf AAKD stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar: Es findet keine Einzelfallprüfung statt und die AAKD werden dieser Pflicht unterworfen, auch wenn sie keineswegs «Dienstleistungen von grosser

wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten», was jedoch gesetzliche Vorgabe ist (Art. 27 Abs. 3 BÜPF).

Problematisch ist zudem, dass aufgrund dieser Vorgabe Anbieter:innen ihrer Verschlüsselungen so konfigurieren müssen, dass sie von ihnen aufgehoben werden können – eine durch Anbieter:innen aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung allerdings in jedem Fall. Dies führt zu schwächeren Verschlüsselungen und der Abnahme der Sicherheit von Kommunikationsdiensten.

Daraus ergibt sich eine Grundrechtsproblematik von erheblicher Tragweite: Das Verhältnismässigkeitsgebot aus Art. 36 BV kann nicht eingehalten werden, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Die Interessenabwägung darf hier nicht zuungunsten der Grundrechtsträger:innen erfolgen, da es sich bei deren Interessen um solche von fundamentalem Gewicht – dem Zugang zu sicherer Kommunikation und damit direkt verbunden dem Recht auf freie Meinungsäusserung – handelt.

Wichtig ist, dass Verschlüsselungen, die auf dem Endgerät der Nutzer:innen erfolgen – also End-zu-End-Verschlüsselungen – nicht unter die Pflicht zur Aufhebung gemäss Art. 50a VE-VÜPF fallen dürfen. Diese Form der Verschlüsselung liegt ausschliesslich in der Sphäre der Nutzer:innen und es wäre untragbar, die Pflicht zur Aufhebung von Verschlüsselungen in dieser Sphäre zu verlangen. Die Anbieter:innen dürfen daher nicht dazu verpflichtet werden, diese Inhalte zu entschlüsseln und zugänglich zu machen. Im Gegensatz dazu betrifft die Transportverschlüsselung «lediglich» die Verbindung zwischen Client und Server und kann von Anbieter:innen kontrolliert werden. Es ist wichtig, dass diese technischen Unterscheidungen und unterschiedlichen Schutzwirkungen und -richtungen bei rechtlichen Umsetzungen beachtet werden. Wir begrüssen die Klarstellung im erläuternden Bericht, dass die End-zu-End-Verschlüsselung vom Anwendungsbereich ausgenommen ist. Es muss jedoch ebenso klar sein, dass das ganze Endgerät von Nutzer:innen aus dem Anwendungsbereich von Art. 50a VE-VÜPF ausgenommen ist.

Es braucht im Übrigen auch eine Klarstellung darüber, dass eine rückwirkende Möglichkeit zur Aufhebung klar ausgeschlossen ist. Eine solche würde de facto eine Vorratsdatenspeicherung verschlüsselter Inhalte und Keys darstellen, die mit dem Prinzip der Datenminimierung (Art. 6 Abs. 3 DSG) und dem Schutz der Privatsphäre (Art. 13 BV) unvereinbar ist.

Antrag: Streichung der «Anbieterin mit reduzierten Pflichten» aus dem Anwendungsbereich sowie eine Klarstellung darüber, dass die Aufhebung von Verschlüsselungen auf dem Endgerät der Nutzer:innen sowie eine rückwirkende Verpflichtung zur Aufhebung ausgeschlossen sind.

Bemerkungen zu einzelnen Artikeln der VD-ÜPF

Art. 14 Abs. 3 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und wirtschaftlich nicht tragbar, was das Einführen von Fristen obsolet werden lässt. Der Absatz ist daher ersatzlos zu streichen.

Antrag: Streichung

Art. 14 Abs. 4 VD-ÜPF

Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der Unterworfenen AAKD – da auch AAKD mit reduzierten Pflichten erfasst sind – massiv. Dies ist wie bereits ausgeführt weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.

Antrag: Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten»

Art. 20 Abs. 1 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen, ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.

Antrag: Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»

Schlussbemerkung

Trotz des Umfangs dieser Stellungnahme gilt: Das Ausbleiben einer expliziten Bemerkung zu einzelnen Bestimmungen bedeutet keine Zustimmung der Digitalen Gesellschaft. Die Ablehnung der Revision bleibt volumnäiglich bestehen.

Freundliche Grüsse

Erik Schönenberger
Geschäftsleiter

Von: A

Gesendet: Dienstag, 6. Mai 2025 18:33:45 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Vernehmlassungsantwort zu den geplanten Änderungen des Schweizer Überwachungsgesetz

Sehr geehrte Damen und Herren

Mit dieser E-Mail nehme ich Stellung zur vorgeschlagenen Änderung des Überwachungsgesetzes (BÜPF).

Ich lehne die geplanten Änderungen entschieden ab. Eine Ausweitung der Überwachungsmöglichkeiten gefährdet grundlegende Freiheitsrechte und das Vertrauen in rechtsstaatliche Prinzipien. Statt mehr staatlicher Überwachung braucht es klare Grenzen und wirksame Kontrollen zum Schutz der Privatsphäre.

Ich fordere Sie daher auf, von dieser Gesetzesänderung abzusehen.

Freundliche Grüsse

Alissa Rosskopf

Von: Daniel Guggisberg

Gesendet: Dienstag, 6. Mai 2025 18:40:08 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer

von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Größere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb zieht jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört**
Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/05/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung**
Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).

- Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch](#)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
- **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
 - **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
 - **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
 - **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
 - **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
 - **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit

des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und

wirkungslos Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse
Daniel Guggisberg

Von: Toivo Voll

Gesendet: Dienstag, 6. Mai 2025 18:50:03 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:
 1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
 2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote** Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten

sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartner** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](#)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung**
Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch](#)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
 - **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
 - **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
 - **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
 - **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
 - **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmäßige Anordnungen klagen können, ist der Reputations- und

Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Toivo Voll

Von: Shant Dakessian
Gesendet: Dienstag, 6. Mai 2025 18:54:23 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht

bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Größere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten compromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

4. **Erzwungene Metadaten-Log-Speicherung zerstört**

Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/03/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).

6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung**

Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

- Ausländische Dienste ohne solche Vorschriften nutzen.
- Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
- Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal

Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

- **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
- **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse,

Shant Dakessian

Von: Yangchi Stocker

Gesendet: Dienstag, 6. Mai 2025 19:15:05 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer

von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Größere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb zieht jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört**
Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/05/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung**
Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).

- Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch](#)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
- **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
 - **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
 - **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
 - **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
 - **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
 - **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit

des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

wirkungslos Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Leang-Yang-chi-Jan Stocker

Von: guggisberg@protonmail.ch
Gesendet: Dienstag, 6. Mai 2025 19:28:15 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

Es ist mir Schleierhaft, dass der Bundesrat eine solche Änderung durchwinkt wenn dieser verstehen würde die Konsequenzen hat. Bedenken Sie:

(V1) Informationstechnische Daten sind so omnipräsent, dass das Abrufen solcher informationsquellen mit physischer Direktüberwachung / Hausdurchsuchung / Abhörung korrespondiert.

(V2) Praktisch alles ist heute informationstechnische Daten: Jedes Mobiltelefon hat ein (Mikrofon, Kamera, GPS und Sensoren), Jedes Auto hat Kameras, praktische alles ist Videoüberwacht, die Post ist praktisch nur noch digital, Einkäufe sind Digital, Bilderbücher sind digital einfach alles

(V3) Jedes Unternehmen hat solche Daten und die meisten Betriebsgeheimnisse und Know How sind auch in diesen Daten zu finden.

(V4) Diese Änderung würde dazu führen dass böswilligen Akteuren das Scheunentor geöffnet wird auf diese Daten zuzugreifen.

Ich bitte um Stellungnahme bezüglich der Punkte V1-V4

Freundliche Grüsse

Joël Guggisberg

Vertiefung:

Die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

- 1. API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die

Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:
 1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
 2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
 3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote** Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles

Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](#)).

6. Kriminelle umgehen die Massnahmen – Kollaterale Überwachung

Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

- Ausländische Dienste ohne solche Vorschriften nutzen.
- Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
- Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch](#)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

- **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
- **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit,

Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Joël Guggisberg

Von: Adrian Nussbaum
Gesendet: Dienstag, 6. Mai 2025 19:52:04 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:
 1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
 2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote** Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartner** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal

Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. **Massenüberwachung durch Pattern Matching**, „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](#)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger Terroristen und Schwerkriminelle** werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch](#)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
 - **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
 - **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
 - **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
 - **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
 - **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmäßige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.
9. **Demokratische und rechtliche Missachtung**
 - Der Verordnungsweg umgeht das Referendumrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
 - Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung

dieses Ausmasses würde im Referendum voraussichtlich abgelehnt werden.

- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und

wirkungslos Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Adrian Nussbaum

Von: A E

Gesendet: Dienstag, 6. Mai 2025 19:55:56 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Teilrevision der VÜPF und VD-ÜPF – Ablehnung der vorgeschlagenen Änderungen

Sehr geehrte Damen und Herren

Mit dieser E-Mail nehme ich als Privatperson klar Stellung zur laufenden Vernehmlassung betreffend der Teilrevision der Verordnungen über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF).

Ich, André Emmenegger, spreche mich ausdrücklich gegen die vorgeschlagenen Änderungen aus. Die vorgesehene Ausweitung der Mitwirkungspflichten – insbesondere die detailliertere Kategorisierung der Anbieter und die Pflicht zur Entfernung von Verschlüsselungen (ausgenommen Ende-zu-Ende-Verschlüsselung) – stellt aus meiner Sicht einen gefährlichen Eingriff in die Privatsphäre der Nutzerinnen und Nutzer dar. Auch die Einführung neuer Überwachungstypen, insbesondere rückwirkender und partieller Inhaltsüberwachungen, führt zu einer besorgniserregenden Ausweitung der staatlichen Überwachung.

Ich erachte die vorgeschlagenen Anpassungen als unverhältnismässig, innovationsfeindlich und demokratisch höchst fragwürdig. Datenschutz, Kommunikationsfreiheit und der Schutz sensibler Nutzerdaten dürfen nicht weiter untergraben werden.

Ich fordere den Bundesrat auf, diese Teilrevision in der vorliegenden Form zurückzuziehen.

Mit freundlichen Grüßen

André Emmenegger

Von: luigi gimmi

Gesendet: Dienstag, 6. Mai 2025 20:11:11 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

API-basierte Echtzeit-Überwachung ohne Rechtsschutz Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ohne nationale eID. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).

Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.

In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

Massenüberwachung durch Pattern Matching „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. Keyword-Filter (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?

Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren (EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse).

Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

Ausländische Dienste ohne solche Vorschriften nutzen.

Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).

Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

Ökonomische Selbstzerstörung und Abwanderung «Diese Verordnung ist wirtschaftlicher Selbstdmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

Kostendruck durch technische Nachrüstung: Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

Abwanderung von Unternehmen: Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und

Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.

Investitionsstopp: Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.

Ausfall von Arbeitsplätzen: Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz: Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.

Rechtliche Risiken und Klagen: Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

Demokratische und rechtliche Missachtung

Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.

Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.

Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos
Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt.
Dieser Widerspruch erzeugt folgende Effekte:

Massive Verlagerung zu E2EE und Self-Hosting: Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.

Verschlüsselung der Metadaten: Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.

Weniger statt mehr Zugriff für Behörden: Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Luigi Gimmi

Von: Darius Doongaji
Gesendet: Dienstag, 6. Mai 2025 20:11:58 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zur Teilrevision der VÜPF und VD-ÜPF – Ablehnung der vorgeschlagenen Änderungen

Sehr geehrte Damen und Herren

Mit dieser E-Mail nehme ich als Privatperson klar Stellung zur laufenden Vernehmlassung betreffend der Teilrevision der Verordnungen über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF).

Ich, Darius Doongaji, spreche mich ausdrücklich gegen die vorgeschlagenen Änderungen aus. Die vorgesehene Ausweitung der Mitwirkungspflichten – insbesondere die detailliertere Kategorisierung der Anbieter und die Pflicht zur Entfernung von Verschlüsselungen (ausgenommen Ende-zu-Ende-Verschlüsselung) – stellt aus meiner Sicht einen gefährlichen Eingriff in die Privatsphäre der Nutzerinnen und Nutzer dar. Auch die Einführung neuer Überwachungstypen, insbesondere rückwirkender und partieller Inhaltsüberwachungen, führt zu einer besorgnisregenden Ausweitung der staatlichen Überwachung.

Ich erachte die vorgeschlagenen Anpassungen als unverhältnismässig, innovationsfeindlich und demokratisch höchst fragwürdig. Datenschutz, Kommunikationsfreiheit und der Schutz sensibler Nutzerdaten dürfen nicht weiter untergraben werden.

Ich fordere Sie auf, diese Teilrevision in der vorliegenden Form zurückzuziehen.

Mit freundlichen Grüßen

Darius Doongaji

Von: Kiki

Gesendet: Dienstag, 6. Mai 2025 20:15:12 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. ****API-basierte Echtzeit-Überwachung ohne Rechtsschutz**** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. ****KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich**** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ****ohne nationale eID****. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:
 1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
 2. Größere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) ([\[en.wikipedia.org\]\(https://en.wikipedia.org/wiki/2017_Equifax_data_breach?utm_source=chatgpt.com\)](https://en.wikipedia.org/wiki/2017_Equifax_data_breach?utm_source=chatgpt.com)) würde Nutzerdaten kompromittieren.
 3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele

jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

4. ****Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote****
Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur ****massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern**** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. ****Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. ****Keyword-Filter**** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.**

* Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?

* Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse]

(<https://www.eff.org/deeplinks/2022/08/googles-scans-private-photos-led-false-accusations-child-abuse>)).

6. ****Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger****
Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

* Ausländische Dienste ohne solche Vorschriften nutzen.

* Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).

* Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

8. ****Ökonomische Selbstzerstörung und Abwanderung**** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (<https://www.watson.ch/digital/wirtschaft/517198902-proton-schweiz-chef-andy-yen-zum-ausbau-der-staatlichen-ueberwachung>). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

* ****Kostendruck durch technische Nachrüstung:**** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

* ****Abwanderung von Unternehmen:**** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.

* ****Investitionsstopp:**** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.

* ****Ausfall von Arbeitsplätzen:**** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

* ****Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:**** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen,

KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.

* **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. **Demokratische und rechtliche Missachtung***

* Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.

* Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.

* Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. **Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos*** Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

* **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.

* **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.

* **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit* Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Lakisha Bruton

Von: Michael Glaus

Gesendet: Dienstag, 6. Mai 2025 20:30:06 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. API-basierte Echtzeit-Überwachung ohne Rechtsschutz

Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

2. KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich

Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene

Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.

3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
3. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote**
Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
4. **Massenüberwachung durch Pattern Matching**
„Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/07/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).
5. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger**
Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
6. **Ökonomische Selbstzerstörung und Abwanderung**
«Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
 - **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren

Compliance-Lasten zu migrieren.

- **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

7. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

8. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unaufgetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen

demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Michael Glaus

Von: David Lanz
Gesendet: Dienstag, 6. Mai 2025 20:40:28 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. API-basierte Echtzeit-Überwachung ohne Rechtsschutz Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

2. KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich
Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:
1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene

Datensätze) ([en.wikipedia.org](https://en.wikipedia.org/wiki/2017_Equifax_data_breach?utm_source=chatgpt.com)) würde Nutzerdaten kompromittieren.

3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

4. ****Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote****
Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur ****massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern**** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. Massenüberwachung durch Pattern Matching

„Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. Keyword-Filter (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen. Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt? Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse]

(<https://www.eff.org/deeplinks/2022/08/googles-scans-private-photos-led-false-accusations-child-abuse>)).

6. Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

Ausländische Dienste ohne solche Vorschriften nutzen.

Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).

Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

8. Ökonomische Selbstzerstörung und Abwanderung «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (<https://www.watson.ch/digital/wirtschaft/517198902-proton-schweiz-chef-andy-yen-zum-ausbau-der-staatlichen-ueberwachung>). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

Kostendruck durch technische Nachrüstung: Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

Abwanderung von Unternehmen: Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.

Investitionsstopp: Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.

Ausfall von Arbeitsplätzen: Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz: Ohne flächendeckende

eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.

Rechtliche Risiken und Klagen: Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.

Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.

Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

Massive Verlagerung zu E2EE und Self-Hosting: Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.

Verschlüsselung der Metadaten: Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.

Weniger statt mehr Zugriff für Behörden: Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit: Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

David Lanz

Von: mikeott@mikeott.ch

Gesendet: Dienstag, 6. Mai 2025 20:50:20 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Vernehmlassungsantwort zu den geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. API-basierte Echtzeit-Überwachung ohne Rechtsschutz

Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmäßigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmäßige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

2. KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich

Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung.

Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat?
Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und

Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Größere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten compromittieren.

In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

3. Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote

Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

4. Massenüberwachung durch Pattern Matching

„Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

- Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden?
- Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/03/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).

5. Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger

Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

- Ausländische Dienste ohne solche Vorschriften nutzen.
- Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
- Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

6. Ökonomische Selbstzerstörung und Abwanderung

«Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

- **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
- **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

7. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

8. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit

Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Mike Ott

Von: Fabrice Ulmann
Gesendet: Dienstag, 6. Mai 2025 21:10:22 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote**
Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/07/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung**
Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene

Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

- **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu

verhindern.

- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Fabrice Ulmann

Von: Dario Cotti
Gesendet: Dienstag, 6. Mai 2025 21:35:25 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:
 1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
 2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio.

betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.

3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote**
Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. **Massenüberwachung durch Pattern Matching**, „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/07/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung**
Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
 - **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
 - **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
 - **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Dario Cotti

Von: Kilian Lattion
Gesendet: Dienstag, 6. Mai 2025 21:55:30 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. API-basierte Echtzeit-Überwachung ohne Rechtsschutz Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

2. KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ohne nationale eID. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele

jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

4. Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur massenhaften Aufzeichnung von Standort, IP, Gerät-ID und Kontaktpartnern gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. Massenüberwachung durch Pattern Matching „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. Keyword-Filter (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

- Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
- Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren (EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse).

6. Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

- Ausländische Dienste ohne solche Vorschriften nutzen.
- Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
- Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

8. Ökonomische Selbstzerstörung und Abwanderung «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

- Kostendruck durch technische Nachrüstung: Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
- Abwanderung von Unternehmen: Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- Investitionsstopp: Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- Ausfall von Arbeitsplätzen: Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz: Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- Rechtliche Risiken und Klagen: Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse

vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- Massive Verlagerung zu E2EE und Self-Hosting: Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- Verschlüsselung der Metadaten: Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- Weniger statt mehr Zugriff für Behörden: Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse
Kilian Lattion

Von: juri.furer@pm.me
Gesendet: Dienstag, 6. Mai 2025 22:01:46 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote**
Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/07/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung**
Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene

Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

- **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu

verhindern.

- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse
Juri Furer

Von:]

Gesendet: Dienstag, 6. Mai 2025 22:10:44 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste

eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Größere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten compromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote**
Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/03/eef-google-s-scans-private-photos-led-false-accusations-child-abuse)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung**
Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

- **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
- **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen

zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.

- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Jan Eichelberger

Von: Benedict.Knecht@gmx.ch Im Auftrag von Bénédict Knecht
Gesendet: Dienstag, 6. Mai 2025 22:28:15 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote** Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/07/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung** **Unschuldiger** Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene

Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

- **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu

verhindern.

- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Bénédict Knecht

Eidgenössisches Justiz- und Polizeidepartement (EJPD)

Bundeshaus West

CH-3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

06.05.2025, Zürich

Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat Beat Jans,

Sehr geehrte Empfänger,

Ich möchte sie gerne darauf hinweisen, dass eine Aushebelung von TLS bedingen würde, das auf allen Endgeräten in der Schweiz ein valides Root-Zertifikat installiert sein müsste.

Dieses könnte jederzeit deinstalliert werden, und somit könnte nichts mehr entschlüsselt werden.

Zudem stellt es auch ein ernormes internationales Risiko dar, dass die RSA-Schlüssel in böswillige Hände fallen könnten. Wenn Internet-Anbieter in der Schweiz nämlich solche einsetzen müssten, was eine technische Voraussetzung wäre, damit Internet Geschwindigkeiten nicht massiv langsamer wären, würde das Risiko für einen erfolgreichen Hacking-Angriff und Diebstahl dieser Schlüssel sehr gross.

Mit diesem Risiko würde im Übrigen auch die Akzeptanz eines Schweizer Root-Zertifikat klein sein, womit es auf in der Regel auch nicht auf Endgeräten präsent sein würde.

Zuletzt hat es Russland mit gemischtem Erfolg versucht, die Bevölkerung zu zwingen ihr eigenes Zertifikat zu installieren. Sonst macht dies kein Land, ausser vielleicht noch Nordkorea.

Des weiteren möchte ich gerne auf die Stellungnahme der Digitalen Gesellschaft verweisen.

<https://www.digitale-gesellschaft.ch/uploads/2025/05/Stellungnahme-Digitale-Gesellschaft-VUePF-VD-UePF.pdf>

Freundliche Grüsse,

Njal Kuhn

Vernehmlassungsantwort zur Teilrevision VÜPF und VD-ÜPF

Betreff: Stellungnahme zur geplanten Ausweitung der Überwachungskompetenzen durch Verordnungsänderung

Sehr geehrter Herr Bundesrat Beat Jans

Sehr geehrte Damen und Herren

Hiermit äussere ich mich **kritisch** zur geplanten Teilrevision der VÜPF und VD-ÜPF. Ich lehne die vorgeschlagenen Änderungen aus den folgenden Gründen ab:

1. Demokratische Legitimation fehlt:

Die Anpassung erfolgt auf Verordnungsebene und entzieht sich damit einer demokratischen Abstimmung. Solch tiefgreifende Eingriffe in die Grundrechte der Bevölkerung gehören nicht in eine Verordnung, sondern müssten – wenn überhaupt – auf Gesetzesebene mit Referendumsmöglichkeit erfolgen.

2. Rechtliche Bedenken:

Die Digitale Gesellschaft hat in ihrer Vernehmlassungsantwort nachvollziehbar dargelegt, dass die vorgeschlagenen Änderungen gegen höherrangiges Recht verstossen, insbesondere gegen die Bundesverfassung und die EMRK. Ich schliesse mich diesen Einschätzungen an.

Quelle: <https://www.digitale-gesellschaft.ch/2025/05/02/bundesrat-will-ueberwachungsstaat-per-verordnung-massiv-ausbauen-stellungnahme-zur-teilrevision-vuepf-und-vd-uepf/>

3. Schädlich für den Innovationsstandort Schweiz:

Die Ausweitung der Überwachungspflichten gefährdet die Existenz von Schweizer IT- und Datenschutzunternehmen wie Proton, Threema oder Nym. Die Schweiz würde dadurch an digitaler Glaubwürdigkeit und internationalem Vertrauen verlieren.

Ich fordere den Bundesrat auf, die geplanten Änderungen zurückzuziehen und ein rechtsstaatlich und demokratisch legitimes Verfahren zu wählen, falls überhaupt ein Regulierungsbedarf besteht.

Mit freundlichen Grüßen

David Lopez Garcia



9000 St. Gallen

St. Gallen den 06.05.2025

Von: domweb@bluewin.ch

Gesendet: Dienstag, 6. Mai 2025 23:11:40 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren

Vorab möchte ich anmerken, dass obschon der nachfolgende Text als Vorlage kopiert wurde, ich ihn vollständig durchgelesen habe und hiermit bestätige, dass der Inhalt sich mit meinen persönlichen Ansichtungen und Überzeugungen deckt und ich den ursprünglichen Verfasser vollends unterstütze:

Stellungnahme:

Die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. API-basierte Echtzeit-Überwachung ohne Rechtsschutz

Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

2. KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich

Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene

Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

3. Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote

Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

4. Massenüberwachung durch Pattern Matching

„Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

- Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
- Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/07/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).

5. Kriminelle umgehen die Massnahmen – Kollaterale Überwachung

Unschuldiger

Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

- Ausländische Dienste ohne solche Vorschriften nutzen.
- Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
- Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

6. Ökonomische Selbstzerstörung und Abwanderung

«Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

- **Kostendruck durch technische Nachrüstung:**
Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
- **Abwanderung von Unternehmen:**
Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- **Investitionsstopp:**
Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- **Ausfall von Arbeitsplätzen:**
Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:**
Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:**
Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmäßige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

7. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

8. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:**
Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:**
Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:**
Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit:

Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse
Dominic Weber

Von: Jonas Weber

Gesendet: Dienstag, 6. Mai 2025 23:31:09 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1.

API-basierte Echtzeit-Überwachung ohne Rechtsschutz Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 2-einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab

Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – *ohne nationale eID*. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1.

Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).

2.

Größere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) ([en.wikipedia.org <https://en.wikipedia.org/wiki/2017_Equifax_data_breach?utm_source=chatgpt.com>](https://en.wikipedia.org/wiki/2017_Equifax_data_breach?utm_source=chatgpt.com)) würde Nutzerdaten kompromittieren.

3.

In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

4.

Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur *massenhaften Aufzeichnung von Standort, IP, Gerät-ID und Kontaktpartnern* gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeyholes für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5.

Massenüberwachung durch Pattern Matching „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. *Keyword-Filter* (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

*

Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?

*

Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren (EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse <<https://www.eff.org/deeplinks/2022/08/googles-scans-private-photos-led-false-accusations-child-abuse>>).

6.

*Kriminelle umgehen die Massnahmen – Kollaterale Überwachung
Unschuldiger* Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

*

Ausländische Dienste ohne solche Vorschriften nutzen.

*

Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).

*

Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

7.

Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

8.

Ökonomische Selbstzerstörung und Abwanderung «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch) <<https://www.watson.ch/digital/wirtschaft/517198902-proton-schweiz-chef-andy-yen-zum-ausbau-der-staatlichen-ueberwachung>>).

Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

*

Kostendruck durch technische Nachrüstung: Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

*

Abwanderung von Unternehmen: Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.

*

Investitionsstopp: Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.

*

***Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

*

***Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.

*

***Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9.

Demokratische und rechtliche Missachtung

*

Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.

*

Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.

*

Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10.

***Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos**: Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

*

***Massive Verlagerung zu E2EE und Self-Hosting**: Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um

Behördenzugriff zu verhindern.

*

Verschlüsselung der Metadaten: Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.

*

Weniger statt mehr Zugriff für Behörden: Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse
Jonas Weber

--

PGP public key: <https://drj.ch>

Von: Flurin Devonas

Gesendet: Dienstag, 6. Mai 2025 23:34:21 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. ****API-basierte Echtzeit-Überwachung ohne Rechtsschutz**** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

2. ****KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich**** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ****ohne nationale eID****. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene

Datensätze) ([en.wikipedia.org](https://en.wikipedia.org/wiki/2017_Equifax_data_breach?utm_source=chatgpt.com)) würde Nutzerdaten kompromittieren.

3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

4. ****Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote****

Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur ****massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern**** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. ****Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. ****Keyword-Filter**** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.**

* Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?

* Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse]

(<https://www.eff.org/deeplinks/2022/08/googles-scans-private-photos-led-false-accusations-child-abuse>)).

6. ****Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger**** Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

* Ausländische Dienste ohne solche Vorschriften nutzen.

* Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).

* Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

8. ****Ökonomische Selbstzerstörung und Abwanderung**** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch](<https://www.watson.ch/digital/wirtschaft/517198902-proton-schweiz-chef-andy-yen-zum-ausbau-der-staatlichen-ueberwachung>)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

* ****Kostendruck durch technische Nachrüstung:**** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

* ****Abwanderung von Unternehmen:**** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.

* ****Investitionsstopp:**** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.

* ****Ausfall von Arbeitsplätzen:**** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

* ****Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:**** Ohne

flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.

* ***Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. **Demokratische und rechtliche Missachtung**

* Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.

* Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.

* Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. **Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos** Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

* ***Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.

* ***Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.

* ***Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Flurin Devonas

Von: Kurz Aaron

Gesendet: Dienstag, 6. Mai 2025 23:36:26 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF; Biberstein Jean-Louis ISC-EJPD

Betreff: Stellungnahme zur geplanten Änderung des Schweizer Überwachungsgesetzes

Sehr geehrte Damen und Herren,

hiermit möchte ich meine Stellungnahme zur geplanten Änderung des Schweizer Überwachungsgesetzes einreichen. Die Frist zur Einreichung endet heute, am 6. Mai 2025.

Ich bin tief besorgt über die geplanten Änderungen, die durch den Dienst für die Überwachung des Post- und Fernmeldeverkehrs (PTSS) vorgeschlagen wurden. Diese Änderungen würden die Überwachungsbefugnisse des Staates erheblich erweitern und stellen einen massiven Eingriff in die Privatsphäre und die Grundrechte der Schweizer Bürger dar.

Das Bundesgericht hat bereits früher strengere Regeln abgelehnt, die durch ein Informationsblatt des PTSS eingeführt werden sollten. Nun versucht der Bundesrat, diese Maßnahmen auf höherer rechtlicher Ebene durch eine Verordnung durchzusetzen. Dies ist besonders problematisch, da Verordnungen nicht dem Referendum unterliegen und somit die Bevölkerung nicht darüber abstimmen kann.

Laut der Digitalen Gesellschaft verstossen die geplanten Änderungen gegen höherrangiges Recht, darunter die Bundesverfassung und die Europäische Menschenrechtskonvention (EMRK). Diese Argumente sind in ihrer ausführlichen Vernehmlassungsantwort detailliert dargelegt und sollten bei einem zukünftigen Gerichtsverfahren relevant sein.

Ich teile die Bedenken der Digitalen Gesellschaft und unterstütze ihre Stellungnahme voll und ganz. Die geplanten Änderungen würden nicht nur die Privatsphäre der Bürger gefährden, sondern auch die Wettbewerbsfähigkeit von Schweizer Unternehmen beeinträchtigen, die auf Datenschutz und Sicherheit setzen. Firmen wie Threema, Proton und NymVPN könnten unter diesen Bedingungen nicht mehr wie bisher operieren, was einen erheblichen wirtschaftlichen Schaden verursachen würde.

In einer Zeit, in der Europa digitale Souveränität anstrebt und sich von der Abhängigkeit von US-Tech-Konzernen lösen will, wären solche Massnahmen nicht nur falsch, sondern auch gefährlich. Sie würden das Vertrauen der Bürger in die Schweizer

Datenschutzstandards untergraben und die Position der Schweiz als sicheres und vertrauenswürdiges Land für digitale Dienste schwächen.

Ich fordere daher den Bundesrat auf, von diesen geplanten Änderungen Abstand zu nehmen und stattdessen Maßnahmen zu ergreifen, die die Privatsphäre und die Grundrechte der Bürger schützen und die Wettbewerbsfähigkeit der Schweizer Wirtschaft fördern.

Mit freundlichen Grüßen,

Aaron Kurz

Von: Wolfgang Schertler
Gesendet: Dienstag, 6. Mai 2025 23:50:11 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht

bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Größere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten compromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

4. **Erzwungene Metadaten-Log-Speicherung zerstört**

Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - o Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - o Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/03/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).

6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung**

Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

- o Ausländische Dienste ohne solche Vorschriften nutzen.
- o Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
- o Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal

Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

- **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
- **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Wolfgang Schertler

Von: brunner.pascal
Gesendet: Dienstag, 6. Mai 2025 23:59:25 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Ablehnung der geplanten Anpassung vom Nachrichtendienstgesetzes

Sehr geehrte Damen und Herren,

hiermit möchte ich meine nachdrückliche Ablehnung der geplanten massiven Ausweitung der Überwachungsbefugnissen des Staates, durch die Anpassung vom Nachrichtendienstgesetz [1] zum Ausdruck bringen.

Die vorgesehenen Massnahmen, insbesondere die weitreichenden Identifikations- und Überwachungspflichten sowie die Vorratsdatenspeicherung für praktisch alle Anbieter von Kommunikationsdiensten, stellen einen schwerwiegenden Angriff auf unsere Grundrechte, insbesondere das Recht auf **Privatsphäre** und die **informationelle Selbstbestimmung**, dar.

Es ist inakzeptabel, dass derart weitreichende Überwachungspflichten auf Verordnungsstufe eingeführt werden sollen. **Regelungen von dieser Tragweite gehören zwingend in ein Gesetz und müssen dem demokratischen Prozess unterworfen werden.**

Letztlich droht die geplante Regulierung auch Open-Source-Projekte, die eine freie und offene Gesellschaft fördern und für Innovation essentiell sind, unverhältnismässig zu benachteiligen oder gar zu behindern.

Ich teile die im Artikel der Digitalen Gesellschaft [2] geäußerten Bedenken vollumfänglich und sehe in dieser geplanten Verschärfung eine ernsthafte Bedrohung für eine freie und offene Gesellschaft.

Mit freundlichen Grüßen

Pascal Brunner

[1] <https://www.vbs.admin.ch/de/nachrichtendienstgesetz>

[2] <https://www.digitale-gesellschaft.ch/2025/05/02/bundesrat-will-ueberwachungsstaat-per-verordnung-massiv-ausbauen-stellungnahme-zur-teilrevision-vuepf-und-vd-uepf/>

Von: Gabor Tanz

Gesendet: Mittwoch, 7. Mai 2025 00:22:36 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

API-basierte Echtzeit-Überwachung ohne Rechtsschutz Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ohne nationale eID. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).

Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.

In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

Massenüberwachung durch Pattern Matching „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. Keyword-Filter (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?

Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren (EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse).

Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

Ausländische Dienste ohne solche Vorschriften nutzen.

Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).

Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

Ökonomische Selbstzerstörung und Abwanderung «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

Kostendruck durch technische Nachrüstung: Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

Abwanderung von Unternehmen: Privacy-Startups und etablierte Anbieter werden die

Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.

Investitionsstopp: Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.

Ausfall von Arbeitsplätzen: Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz: Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.

Rechtliche Risiken und Klagen: Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

Demokratische und rechtliche Missachtung

Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.

Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.

Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

Massive Verlagerung zu E2EE und Self-Hosting: Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.

Verschlüsselung der Metadaten: Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.

Weniger statt mehr Zugriff für Behörden: Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere

Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Gabor Tanz

Von: Matthieu Mayor <matthieu.mayor@gmail.com>
Gesendet: Dienstag, 6. Mai 2025 18:07
An: _ISC-EJPD-Aemterkonsultationen <aemterkonsultationen@isc-ejpd.admin.ch>
Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist:
6. Mai 2025

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. ****API-basierte Echtzeit-Überwachung ohne Rechtsschutz**** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

2. ****K -Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich**** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ****ohne nationale eID****. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (H -/Software, Support, Compliance).

2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: Mio. betroffene Datensätze)

([en.wikipedia.org][https://en.wikipedia.org/wiki/2017_Equifax_data_breach?utm_source=chatgpt.com]) würde Nutzerdaten kompromittieren.

3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigen heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

4. ****Erzwungene Metadat -Log-Speicherung zerstört Zero-Log-Angebote**** Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur ****massenhaften Aufzeichnung von Standort, IP, Gerät-ID und Kontaktpartnern**** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. ****Massenüberwachung durch Pattern Matching****, „Te -Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. ****Keyword-Filter**** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

* Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Disco -Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?

* Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse]
(<https://www.eff.org/deeplinks/2022/08/googles-scans-private-photos-led-false-accusations-child-abuse>)).

6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger**** Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
- * Ausländische Dienste ohne solche Vorschriften nutzen.
 - * Metadaten fälschen oder verschleieren (z. B. IP-Adressen, Standortdaten).
 - * Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung**** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch] (<https://www.watson.ch/digital/wirtschaft/517198902-proton-schweiz-chef-andy-yen-zum-ausbau-der-staatlichen-ueberwachung>)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
- * **Kostendruck durch technische Nachrüstung:**** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
 - * **Abwanderung von Unternehmen:**** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
 - * **Investitionsstopp:**** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
 - * **Ausfall von Arbeitsplätzen:**** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
 - * **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:**** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
 - * **Rechtliche Risiken und Klagen:**** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmäßige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.
9. **Demokratische und rechtliche Missachtung**
- * Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
 - * Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
 - * Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.
10. **Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos**** Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

* **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.

* **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.

* **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Matthieu Mayor
Sent from my iPhone

Von: patrick@patrickwirth.com

Gesendet: Mittwoch, 7. Mai 2025 10:50:56 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:
 1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).

2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote** Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/eff-google-scans-private-photos-led-false-accusations-child-abuse)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung**
Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

Abwanderung von Unternehmen: Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.

- **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmäßige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

1. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und

wirkungslos Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten

Massenüberwachungsmechanismen, zerstören heutige Privacy Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Patrick Wirth

Patrick Wirth

[REDACTED]

[REDACTED]

[REDACTED]
patrick@patrickwirth.com

Von: Vlacic Goran

Gesendet: Mittwoch, 7. Mai 2025 10:56:04 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

API-basierte Echtzeit-Überwachung ohne Rechtsschutz Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmäßigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmäßige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ohne nationale eID. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).

Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.

In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

Massenüberwachung durch Pattern Matching „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. Keyword-Filter (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?

Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren (EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse).

Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

Ausländische Dienste ohne solche Vorschriften nutzen.

Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).

Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

Ökonomische Selbstzerstörung und Abwanderung «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

Kostendruck durch technische Nachrüstung: Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

Abwanderung von Unternehmen: Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und

Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.

Investitionsstopp: Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.

Ausfall von Arbeitsplätzen: Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz: Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.

Rechtliche Risiken und Klagen: Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

Demokratische und rechtliche Missachtung

Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.

Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.

Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos
Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt.
Dieser Widerspruch erzeugt folgende Effekte:

Massive Verlagerung zu E2EE und Self-Hosting: Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.

Verschlüsselung der Metadaten: Selbst Kommunikationsmetadaten (Standort, IP, Geräte-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.

Weniger statt mehr Zugriff für Behörden: Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Goran Vlacic

Von: Olivier D'Ancona <olivier_dancona@hotmail.com>

Gesendet: Mittwoch, 7. Mai 2025 03:29

An: Biberstein Jean-Louis ISC-EJPD <jean-louis.biberstein@isc-ejpd.admin.ch>

Betreff: Surveillance des télécommunications

Monsieur/Madame,

Je tiens à exprimer ma vive inquiétude concernant l'ordonnance sur la surveillance des télécommunications que le Conseil fédéral propose actuellement. En tant que professionnel du secteur numérique et défenseur des droits à la vie privée, il me semble que cette initiative menace directement non seulement la sécurité des citoyens suisses, mais aussi l'ensemble du secteur technologique en Suisse, qui est encore en développement (Nym, Infomaniak, Proton, Threema).

Je vous pose soumet alors mes questions les plus brûlantes :

1. **N'est-il pas contradictoire de promouvoir la Suisse comme un bastion de la cybersécurité et de la confidentialité, tout en adoptant des lois favorisant la surveillance de masse ?** Comment concilier ces deux principes ? N'est-ce pas là une remise en question des bases mêmes de la cybersécurité et de la confidentialité que la Suisse se doit de défendre ?
2. **La politique de la Suisse en matière de cybersécurité ne devrait-elle pas s'aligner sur le principe fondamental du secret numérique et la souveraineté de notre espace cyber ?** Si nous compromettons ces valeurs, que reste-t-il de notre indépendance numérique ?
3. **N'est-il pas dangereux de permettre à des autorités de déchiffrer des communications privées, notamment celles via des services de messagerie et de VPN ?** Ne devrions-nous pas nous interroger sur le caractère antidémocratique et autoritaire de telles mesures ? À quel point cela menace-t-il la liberté individuelle et le respect des droits fondamentaux des citoyens ?

4. **Ces mesures de traçage risquent-elles de nuire à la liberté des citoyens ?** En permettant à un État de potentiellement contrôler les masses, ne risquons-nous pas d'aller à l'encontre des principes de liberté individuelle que nous chérissons ? Après tout, nous ne sommes ni la Chine ni les États-Unis, mais une nation fière de sa liberté.
5. **L'implémentation de telles lois pourrait-elle affaiblir la compétitivité de nos entreprises et accroître leur vulnérabilité ?** En introduisant des backdoors dans des services conçus pour être sécurisés, qui aura réellement le contrôle de ces systèmes ? Ne faudrait-il pas repenser ces mesures pour ne pas sacrifier la sécurité de nos infrastructures et données sensibles ?
6. **En quel nom souhaite-t-on surveiller les services de messagerie ?** Ces services contribuent à la neutralité de la Suisse, en offrant à la fois un respect des libertés individuelles et une communication sécurisée. Pourquoi alors limiter cette liberté au nom de la sécurité, en risquant d'endommager la réputation de la Suisse comme un bastion de neutralité ?

Je vous invite à considérer mes questions avant qu'une décision irréversibles ne soit prise. Ne devrions-nous pas, au contraire, encourager les entreprises suisses à innover dans le respect des libertés individuelles et dans un environnement sécurisé, plutôt que de leur imposer des contraintes qui risquent de ruiner ce secteur vital pour notre avenir numérique ? Nous devrions protéger les entreprises qui sont notre fleuron de souveraineté numérique et les défendre contre les états autoritaires tels que la Chine ou les États-Unis plutôt que de fragiliser notre écosystème en instaurant des backdoors.

Je vous remercie pour votre attention et vous encourage vivement à tenir compte des répercussions que cette ordonnance pourrait avoir non seulement sur la sécurité des citoyens, mais également sur l'indépendance et la réputation de notre pays en matière de cybersécurité.

Merci beaucoup,

Olivier D'Ancona

Von: Thomas Götz

Gesendet: Mittwoch, 7. Mai 2025 11:29:06 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrte Damen und Herren

Es ist schockierend!

Ganz offensichtlich ist dem Schweizerischen Bundesrat ein grundlegendes Verständniss von Informatik abzusprechen.

Es kann nicht sein, dass die Privatsphäre der überwiegenden Mehrheit der schweizer Bevölkerung derart negiert werden kann, respektive ein solches Vorgehen überhaupt in betracht gezogen wird, um eine kleinst-Minderheit an Deliquenten ausfindig zu machen. Dies obwohl diese Delinquenten auch auf anderem Wege wesentlich beweissicherer dingfest gemacht werden können.

Es kann nicht sein, dass ein Staat seine Finger derart in das Privatleben seiner Bürger steckt.

Alle Beispiele von ähnlichen Vorhaben in der Vergangenheit zeigen nur ein Bild: Daten welche vorhanden sind, werden früher oder später auch genutzt. Selbst das Büpf selbst dient hier als Beispiel. Als Kompromiss zwischen Privatsphäre und Sicherheit vom schweizer Souverän angenommen, wird es inzwischen ad absurdum geführt und versucht zu genau dem zu machen was es verhindern soll. Einer pseudo legitimierten Fichen affäre 2.0. Nur können diese Fichen dieses mal automatisiert ausgewertet werden.

Sie beschreiben einen Orwelschen feuchten Traum... Auf Rückschlüsse bezüglich der Motivation des Nachrichtendienstes, und weiterer von dieser Art der Überwachung profitierender Banden, möchte ich hier verzichten, mir wird so bereits genug übel.

Weiterhin erschüttert es mein Vertrauen in die Politik, dass so ein Vorhaben über den Verordnungsweg überhaupt nur zur Diskussion zugelassen wird.

Die Grundrechte der schweizer Bevölkerung, genaugenommen sogar weiterreichend als nur für schweizer Bürger, werden hier Diskutiert. Dies kann und darf nicht über eine Bundesrätliche Verordnung passieren, vor allem im Hinblick, dass die Grundkenntnisse der diskutierten Technologien schlicht und ergreifend nicht vorhanden sind. Ja sehr geehrte Bundesräte und Bundesrätinnen, ich spreche Ihnen diese Kompetenz ab! Sie haben Kompetenzen in sehr vielen Bereichen, daran kann es keine Zweifel geben. Wenn Sie allerdings dazu bereit sind über solch eine Verordnung ernsthaft zu diskutieren, zum wiederholten male möchte ich anfügen, lässt dies für mich keinen anderen Schluss zu. Ich bitte Sie hiermit mein Vertrauen in Ihren Menschenverstand wiederherzustellen, und diese Verordnung zu versenken.

Ebenfalls möchte ich meine Zeit sinnvoller verwenden als mit dem Politischen Kampf gegen einen Orwelschen Überwachungsstaat in unserer schönen Schweiz. Zum Beispiel für meine Tochter. Sie wissen schon, die Zukunft unseres Landes als lebenswertes Zuhause?

Ich bin sicher sie können nachvollziehen was ich meine.

Mit freundlichen Grüßen und in grosser Hoffnung auf Ihre Zurechnungsfähigkeit
Thomas Götz

Von: Robin Schlup
Gesendet: Mittwoch, 7. Mai 2025 19:40:43 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
An: _ISC-EJPD-Aemterkonsultationen ÜPF
Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,
die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. API-basierte Echtzeit-Überwachung ohne Rechtsschutz Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ohne nationale eID. Jeder Anbieter müsste eigene Identitätsserver

betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur massenhaften Aufzeichnung von Standort, IP, Gerät-ID und Kontaktpartnern gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. Massenüberwachung durch Pattern Matching „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. Keyword-Filter (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/03/scans-private-photos-led-false-accusations-child-abuse)).
6. Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).
 - Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. Ökonomische Selbstzerstörung und Abwanderung «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton (watson.ch). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
 - Kostendruck durch technische Nachrüstung: Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen

- im sechs- bis siebenstelligen Bereich pro Unternehmen.
- Abwanderung von Unternehmen: Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
- Investitionsstopp: Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
- Ausfall von Arbeitsplätzen: Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
- Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz: Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
- Rechtliche Risiken und Klagen: Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos

Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- Massive Verlagerung zu E2EE und Self-Hosting: Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- Verschlüsselung der Metadaten: Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- Weniger statt mehr Zugriff für Behörden: Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare

Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Robin Schlup

Von: Lorenzo Valentini

Gesendet: Donnerstag, 8. Mai 2025 00:08:45 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. **API-basierte Echtzeit-Überwachung ohne Rechtsschutz** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.
2. **KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer

von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – **ohne nationale eID**. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Größere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) (en.wikipedia.org) würde Nutzerdaten kompromittieren.
3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb zieht jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.
4. **Erzwungene Metadaten-Log-Speicherung zerstört**
Zero-Log-Angebote Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.
5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.
 - Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?
 - Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse](https://www.eff.org/deeplinks/2018/07/eff-google-s-scans-private-photos-led-false-accusations-child-abuse)).
6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung**
Unschuldiger Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:
 - Ausländische Dienste ohne solche Vorschriften nutzen.
 - Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).

- Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.
7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.
8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch](#)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:
- **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.
 - **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.
 - **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.
 - **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.
 - **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.
 - **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit

des Landes beeinträchtigt.

9. Demokratische und rechtliche Missachtung

- Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.
- Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.
- Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und

wirkungslos Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

- **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.
- **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.
- **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Lorenzo Valentini

Von: Patrick Fehr

Gesendet: Donnerstag, 8. Mai 2025 06:39:31 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Stellungnahme zur Vernehmlassung über die geplanten Änderungen des Überwachungsgesetzes (Frist: 6. Mai 2025)

Sehr geehrte Damen und Herren,

die geplanten Änderungen der VÜPF (SR 780.11) und der VD-ÜPF (SR 780.117) gefährden sowohl die Grundrechte der Bevölkerung als auch den Wirtschaftsstandort Schweiz. Im Folgenden führe ich die zentralen Kritikpunkte anhand konkreter Beispiele und Quellen auf:

1. ****API-basierte Echtzeit-Überwachung ohne Rechtsschutz**** Die Einführung einer Lawful-Intercept-API erlaubt es Behörden, per Knopfdruck Live-Streams von Voice, Chat oder VPN-Sessions abzurufen – automatisiert und ohne unabhängige Verifikation. Anbieter müssen Daten unverzüglich liefern, noch bevor die Rechtmässigkeit geprüft oder die Echtheit des Dokuments verifiziert ist. Was passiert, wenn ein leeres oder unvollständiges Gerichtsdokument eingereicht wird? Gewährt die API in solchen Fällen trotzdem Zugang? Wer kontrolliert, dass jede Anfrage wirklich auf einem gültigen Beschluss basiert? Und wie sollen Unternehmen gegen unrechtmässige, automatisierte Abrufe vorgehen, wenn ihnen die Daten bereits übermittelt wurden? Da der Zugriff automatisch erfolgt, gibt es keine wirksamen Prüfmechanismen – die Behörde erhält die Daten sofort und kann sie verwenden, selbst wenn ein späterer Rechtsstreit die Anordnung für ungültig erklärt. Anbieter können den Schaden nicht rückgängig machen, wenn die Daten schon weg sind. Nutzerinnen und Nutzer erfahren nie, dass sie überwacht werden – es gibt keinerlei Benachrichtigung oder Transparenz, sodass jegliche Überwachung im Verborgenen stattfindet. Im Gegensatz dazu ist eine physische Durchsuchung eines Hauses für alle Betroffenen sichtbar und nachvollziehbar: Man stellt den Durchsuchungsbefehl vor, bei Verweigerung muss die Polizei die Tür gewaltsam öffnen, und Betroffene können den Umfang und Zeitpunkt des Zugriffs unmittelbar erkennen und, wenn nötig, juristisch anfechten.

2. ****KYC-Pflicht ab 5 000 Nutzern ist willkürlich und gefährlich**** Unklar bleibt, ob die Schwelle sich auf Registrierungen, Downloads oder aktive Nutzer bezieht. Zählt ein Account, der vor zehn Jahren einmalig erstellt wurde, ebenso wie ein aktiver Nutzer von heute? Ohne genaue Definition droht Willkür bei der Anwendung. Gilt die Pflicht bereits bei 5 000 kumulierten Anmeldungen, bei 5 000 einmaligen Downloads oder bei 5 000 aktiven Nutzern pro Monat? Ab Erreichen dieser Schwelle müssen Firmen Ausweiskopien, Adressnachweise und Zahlungsinformationen sammeln – ****ohne nationale eID****. Jeder Anbieter müsste eigene Identitätsserver betreiben, was bedeutet:

1. Hohe Initial- und Betriebskosten (Hard-/Software, Support, Compliance).
2. Grössere Angriffsfläche: Jedes Leck (vgl. Equifax-Datenleck: 147 Mio. betroffene Datensätze) ([\[en.wikipedia.org\]](https://en.wikipedia.org/wiki/2017_Equifax_data_breach?utm_source=chatgpt.com)(https://en.wikipedia.org/wiki/2017_Equifax_data_breach?utm_source=chatgpt.com)) würde Nutzerdaten kompromittieren.

3. In der Schweiz existiert bislang keine flächendeckende eID-Infrastruktur; deshalb fiele jede Firma auf eigene, heterogene Lösungen zurück, die potenziell fehleranfällig und teuer sind.

4. **Erzwungene Metadaten-Log-Speicherung zerstört Zero-Log-Angebote**

Zero-Log-VPNs und Privacy-Apps, die heute keine Nutzerdaten sammeln, würden zur **massenhaften Aufzeichnung von Standort, IP, Geräte-ID und Kontaktpartnern** gezwungen. Dies hebt Geschäftsmodelle auf, schafft neue Honeypots für Hacker und zerstört das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen: Datenschutz und Privatsphäre.

5. **Massenüberwachung durch Pattern Matching** „Teil-Content-Capture“ ist faktisch eine flächendeckende Inhaltsanalyse aller Kommunikation. **Keyword-Filter** (z. B. Erkennung von „Bomb“) ohne semantische Kontextprüfung führen zwangsläufig zu Fehlalarmen und massenhaften Abfragen.

* Wie soll ein Algorithmus unterscheiden, ob „bomb“ in einem Discord-Chat von Gamern eine Spielstrategie oder eine echte Bedrohung darstellt, wenn der Kontext fehlt?

* Welche Mechanismen verhindern, dass hunderttausende Nutzer aufgrund harmloser Begriffe überwacht werden? Ein eklatantes Beispiel: Googles Algorithmen stufen harmlose medizinische Kinderfotos als Missbrauchsmaterial ein und melden sie automatisch den Behörden, ohne die Betroffenen zu informieren ([EFF: Google's Scans of Private Photos Led to False Accusations of Child Abuse] (<https://www.eff.org/deeplinks/2022/08/googles-scans-private-photos-led-false-accusations-child-abuse>)).

6. **Kriminelle umgehen die Massnahmen – Kollaterale Überwachung Unschuldiger*** Terroristen und Schwerkriminelle werden Schweizer Anbieter mit Protokoll- und API-Hintertürpflichten umgehen, indem sie:

* Ausländische Dienste ohne solche Vorschriften nutzen.

* Metadaten fälschen oder verschleiern (z. B. IP-Adressen, Standortdaten).

* Selbstgehostete oder dezentrale E2EE-Lösungen verwenden.

7. Während sich Kriminelle anderen Lösungen zuwenden, führt diese Regelung zu einer flächendeckenden Überwachung normaler Nutzer ohne zusätzlichen Nutzen für die Strafverfolgung. Höchst erfahrene Täter lassen sich nicht durch Log-Pflichten abschrecken, sodass nur Unschuldige betroffen sind.

8. **Ökonomische Selbstzerstörung und Abwanderung** «Diese Verordnung ist wirtschaftlicher Selbstmord für die Schweiz», warnt Andy Yen, CEO von Proton ([watson.ch] (<https://www.watson.ch/digital/wirtschaft/517198902-proton-schweiz-chef-andy-yen-zum-ausbau-der-staatlichen-ueberwachung>)). Die Vorschläge gefährden das zentrale Alleinstellungsmerkmal Schweizer Tech-Unternehmen – Datenschutz und Privatsphäre – und haben weitreichende ökonomische Folgen:

* **Kostendruck durch technische Nachrüstung:** Anbieter müssen eigene Lawful-Intercept-Server, Authentifizierungsinfrastruktur und Metadaten-Datenbanken aufbauen und betreiben – täglich, rund um die Uhr. Die initialen Investitionen und laufenden Betriebskosten liegen im sechs- bis siebenstelligen Bereich pro Unternehmen.

* **Abwanderung von Unternehmen:** Privacy-Startups und etablierte Anbieter werden die Schweiz verlassen, um ihr zentrales Alleinstellungsmerkmal – Datenschutz und Privatsphäre – nicht zu gefährden und in Länder mit geringeren Compliance-Lasten zu migrieren.

* **Investitionsstopp:** Risikokapitalgeber und Business Angels ziehen sich zurück, wenn die Schweiz als Standort kein verlässliches Datenschutz-Regime bietet.

* **Ausfall von Arbeitsplätzen:** Tausende hochqualifizierter IT-Fachkräfte verlieren Perspektiven in der Schweiz, wenn Tech-Firmen abwandern oder keine neuen Projekte starten.

* **Mangelnde eID-Infrastruktur verschärft Kosten – greift zu kurz:** Ohne flächendeckende eID müssen Unternehmen eigene Identitätssysteme entwickeln, was zusätzlich Zeit und Ressourcen bindet. Selbst bei einer zentralen eID bliebe das

fundamentale Problem bestehen, dass Betreiber automatisierter API-Schnittstellen, KYC-Verpflichtungen und Metadaten-Loggings weiterhin unkontrolliert auf Nutzerdaten zugreifen können. Eine eID-Lösung behebt nicht die fehlende Prüf-, Transparenz- und Widerspruchsmechanismen im Überwachungsprozess.

* **Rechtliche Risiken und Klagen:** Anbieter verlieren die Möglichkeit, Gerichtsbeschlüsse vor Auslieferung zu prüfen. Selbst wenn sie später erfolglos gegen unrechtmässige Anordnungen klagen können, ist der Reputations- und Datenverlust nicht rückgängig zu machen. Insgesamt droht eine Abwanderung des gesamten Privacy-Ökosystems aus der Schweiz – ein Szenario, das langfristig die digitale Souveränität und Wettbewerbsfähigkeit des Landes beeinträchtigt.

9. **Demokratische und rechtliche Missachtung**

* Der Verordnungsweg umgeht das Referendumsrecht: Die Bevölkerung verliert ihr Recht auf direkte Mitsprache und Abschaffung oder Verschärfung von Grundrechtseingriffen zu verhindern.

* Diese Umgehung ist offensichtlich demokratisch illegitim, denn eine Gesetzesänderung dieses Ausmaßes würde im Referendum voraussichtlich abgelehnt werden.

* Als Privatperson behalte ich mir vor, im Fall einer Verabschiedung Klage beim Europäischen Gerichtshof für Menschenrechte einzureichen.

10. **Serverseitige Verschlüsselung und Schlüsselübergabe – kontraproduktiv und wirkungslos**: Der Entwurf zwingt serverseitig verschlüsselte Dienste zur Herausgabe von Schlüsseln oder Klartext, während echte Ende-zu-Ende-Verschlüsselung (E2EE) unangetastet bleibt. Dieser Widerspruch erzeugt folgende Effekte:

* **Massive Verlagerung zu E2EE und Self-Hosting:** Anbieter und Nutzer weichen zu dezentralen, selbst gehosteten oder E2EE-Lösungen aus, um Behördenzugriff zu verhindern.

* **Verschlüsselung der Metadaten:** Selbst Kommunikationsmetadaten (Standort, IP, Gerät-ID, Kontaktpartner) können Ende-zu-Ende verschlüsselt werden, wodurch die Pflicht zur Herausgabe praktisch wirkungslos wird.

* **Weniger statt mehr Zugriff für Behörden:** Trotz gesetzlicher Schlüsselübergabe erhalten Strafverfolger faktisch weniger verwertbare Daten, weil relevante Akteure auf andere Dienste ausweichen.

Fazit: Die vorgeschlagenen Änderungen führen zu automatisierten, intransparenten Massenüberwachungsmechanismen, zerstören heutige Privacy-Geschäftsmodelle, umgehen demokratische Kontrolle und beschädigen die Rechtsstaatlichkeit. Ich fordere Sie eindringlich auf, die Verordnungsänderungen zurückzuziehen und den Innovations- sowie Datenschutz-Standort Schweiz nicht zu gefährden.

Freundliche Grüsse

Patrick Fehr

Von: Samuel Progin <samuel@prog.in>
Gesendet: Montag, 12. Mai 2025 16:09
An: Biberstein Jean-Louis ISC-EJPD <jean-louis.biberstein@isc-ejpd.admin.ch>
Betreff: Consultation sur la révision des ordonnances OSCPT et OME-SCPT

Cher Monsieur,

On dit souvent qu'il ne faut pas attribuer à la malveillance ce qui peut s'expliquer par l'incompétence. À la lecture du projet de modification des deux ordonnances d'exécution de la surveillance de la correspondance par poste et télécommunication (OSCPT et OME-SCPT), je ne sais plus à quel saint me vouer. Ces deux textes se vautrent allègrement dans l'atteinte à la vie privée et l'ignorance technique crasse. Il est difficile de comprendre comment, dans un pays généralement réputé pour son intelligence pragmatique et sa modération, un tel projet a pu ne serait-ce qu'atteindre le stade de la consultation.

Certes, nous ne sommes pas à notre coup d'essai. On se souvient encore de l'ancien conseiller national Dominique de Buman qui voulait... taxer les e-mails. Plus récemment, nous avons inscrit dans la loi une absurdité consistant à imposer le blocage DNS des sites de jeux d'argent non autorisés. L'implémentation de référence fournie par Switch [1] ne fonctionne plus depuis au moins un an. Littéralement personne ne s'en sert. Mais cette fois, on franchit un cap.

Alors même que la LPD timidement revue, ou l'adoption plus ou moins volontaire du RGPD, vont dans le sens d'une meilleure protection de la vie privée, vous proposez ici une mécanique inversée : stocker massivement des données qui, dans la grande majorité des cas, ne seront ni utiles ni utilisées — sauf peut-être lorsqu'elles fuiront dans la nature. Ce qui arrivera.

Au moment où l'on parle (souvent hypocritement, certes) de sobriété numérique, ces ordonnances imposent un gaspillage massif de ressources — tant en stockage qu'en bande passante. Avez-vous ne serait-ce que tenté une estimation, même grossière, des volumes de données générés et des coûts techniques associés ?

Quel besoin réel cette mise à jour cherche-t-elle à satisfaire ? Une meilleure surveillance ? Mais de qui ? Pour quoi faire ? Et selon quelle logique de retour sur investissement ? Aucune étude d'impact sérieuse n'est présentée. On devine donc que c'est, comme souvent, la peur floue qui dicte la plume.

Ces ordonnances instaurent un régime de présomption de culpabilité généralisée, où chaque citoyen devra prouver qu'il n'a rien à cacher, fournir ses identifiants à l'avance, et accepter que ses activités soient enregistrées de manière indiscriminée. Dieu reconnaîtra les siens. On aurait pu croire que le scandale des fiches ait servi de leçon. Mais il semble qu'il soit plus confortable d'oublier les erreurs du passé que de s'en inspirer.

Sur le plan technique, ces mécanismes ne toucheront que les naïfs et les honnêtes gens. Quiconque souhaite réellement protéger ses données ou métadonnées (pour de bonnes ou de mauvaises raisons, d'ailleurs) dispose déjà d'outils comme les VPN, TOR, les relais, les résolveurs DNS non censurés ou chiffrés. Des générateurs automatiques de trafic vont probablement se multiplier, produisant des torrents (pun intended) de données inutiles, noyant les dispositifs de journalisation dans des flux dénués de valeur.

Le brouhaha sur le chiffrement, sa suppression s'il est mis en place par un FST ou non, montre le degré de non professionnalisme dans le domaine.

Sérieusement, avez-vous travaillé avec des experts en cybersécurité digne de ce nom? S'il s'agit d'un ou plusieurs consultants externes, je serai ravi d'avoir leur référence, j'ai un dîner mercredi soir.

Et pendant cette mascarade réglementaire, ce sont les entreprises suisses du numérique, les acteurs de l'hébergement et de la cybersécurité, qui vont payer la facture en compétitivité.
L'environnement aussi, soit dit en passant. Quant aux personnes vraiment intéressantes à surveiller, elles seront non seulement invisibles, mais encore plus difficiles à localiser. Regardez ce qu'il s'est passé lorsque Tumblr a été censuré...

J'ose espérer, Monsieur, que vous serez bientôt noyé sous un torrent (re-pun intended) de lettres de citoyens consternés, indignés et inquiets par ce projet désastreux.

Malgré mon retard, recevez, Monsieur, mes salutations les plus modérément (re-re-pun intended) respectueuses,

[1] <https://www.switch.ch/fr/switch-public-dns>

--
Samuel Progin

1033 Cheseaux-sur-Lausanne
Switzerland

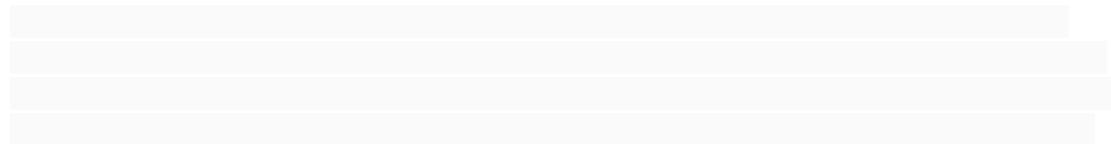
Von: 93.bravura-neat@icloud.com

Gesendet: Montag, 5. Mai 2025 20:52:08 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff:

Cette révision va à l'encontre du contrat social suisse qui prévoit une liberté et une responsabilité individuelle des citoyens. Elle a déjà été annoncée comme illégale et le processus de révision de l'ordonnance est anti-démocratique et honteux, en plus d'être inutile car des outils supplémentaires ne sont pas nécessaires dans le contexte actuel.



Von: hinkucker

Gesendet: Dienstag, 6. Mai 2025 18:14:30 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: _ISC-EJPD-Aemterkonsultationen ÜPF

Betreff: Beschwerde ÜPF Vernehmlassung

Sehr geehrte Damen und Herren bitte entnehmen Sie die Beschwerde aus der Pdf Datei die angehängt ist.

Sehr geehrte Damen und Herren

Die geplante Ausweitung der Möglichkeiten des ÜPF wird von mir in seinem Umfang kategorisch abgelehnt.

Begründung

1. Die Erweiterung fügt der Bevölkerung mehr Schaden als Nutzen zu. Dies auf Grund der persönlichen Freiheiten und der Wirtschaftlichen Betätigungsfeldern von Technologieunternehmen.
2. Die digitalen Behörden der Schweiz haben es bisher versäumt unter Beweis zu stellen, dass sie mit sensiblen Daten gebührend umzugehen verstehen.
3. Ein Eingreifen der behördlichen Gewalt auf Informationssysteme in diesem Umfang bedingt einer gesellschaftlichen Debatte, welche aber mit der „Erweiterung“ einer Verordnung umgangen wird. Dies stellt m.A. bereits in sich ein verfassungsrechtliches Problem dar und muss daher auch vor dem Volk begründet und abgestimmt werden.

Mit freundlichem Gruss

Eure Schweizer BürgerInnen

Von: [Philipp B](#)
An: [ISC-EJPD-Aemterkonsultationen ÜPF](#)
Betreff: Fernmeldeüberwachung und mitwirkungspflichtige Unternehmen: Vernehmlassung eröffnet
Datum: Dienstag, 6. Mai 2025 11:37:24

Guten Tag

Ich habe erst kürzlich von dieser geplanten Änderung des Gesetzes gehört. Ich bin überrascht und schockiert, dass die Schweiz nach dem Ende des Bankengeheimnisses nun auch die Privatsphäre der eigenen Bürger aufgeben will. Das ist zutiefst unschweizerisch und ich lehne dieses neue Gesetz ab.

Bitte überdenken Sie die neu geplante Regelung nochmal und die Konsequenzen für die einzelnen Bürger und das beschädigte Vertrauen in die Institutionen. Und schlussendlich bedenken Sie auch Nachteile für die Schweizer Firmen und schlussendlich die schweizer Wirtschaft. Ein strenges Datenschutzgesetz könnte eine Chance sein statt ein Standortnacheil.

Freundliche Grüsse
Philipp B