



Eidgenössisches Justiz- und Polizeidepartement
3003 Bern

6. Juli 2022 (RRB Nr. 983/2022)

**Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur
Bekämpfung von terroristischen und anderen schweren Straftaten
(Vernehmlassung)**

Sehr geehrte Frau Bundesrätin

Wir danken Ihnen für die Gelegenheit zur Stellungnahme zum Vorentwurf für ein Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG) und äussern uns wie folgt:

Die Einführung und Stossrichtung des neuen Gesetzes begrüessen wir. Es besteht jedoch folgender Anpassungsbedarf:

Zu Art. 1 Bst. b:

In dieser Bestimmung sind die Luftverkehrsunternehmen definiert. Gemäss Erläuterndem Bericht (S. 20) sollen Privatflüge nicht darunterfallen. Gerade bei Flügen mit Privatjets ist die Gefahr aber besonders gross, dass Personen und/oder Gegenstände befördert werden, die einen Bezug zu schweren Straftaten haben. Die Privatfliegerei sollte daher vom FPG zwingend auch erfasst werden.

Zu Art. 5:

Die hier genannte Informationspflicht erscheint insoweit überflüssig, als sich aus dem Gesetz ergibt, dass entsprechende Informationen gesammelt und bearbeitet werden. Die Flugpassagiere noch zusätzlich zu informieren, erscheint unnötig. Dies wird bei anderen Datenbearbeitungen im Bereich der Strafverfolgung auch nicht anders gehandhabt.

Zu den PNR-Deliktskategorien (Art. 6 in Verbindung mit Anhang 2):

Art. 6 in Verbindung mit Anhang 2 regelt, welche Straftaten vorliegen müssen, damit eine Datenbearbeitung zulässig ist.

Gemäss Art. 6 Abs. 2 gelten als terroristische Straftaten solche, die in Anhang 1 Ziff. 22 des Schengen-Informationsaustausch-Gesetzes vom 12. Juni 2009 (SR 362.2) enthalten sind. Ziff. 22 enthält jedoch nur den Straftatbestand der Finanzierung des Terrorismus

(Art. 260^{quinquies} StGB). Gemäss Erläuterndem Bericht gelten auch die Tatbestände nach Art. 1–4 des Rahmenbeschlusses des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (Rahmenbeschluss 2002/475/JI) als terroristische Straftaten. Diese decken sich mit Anhang 1a der Verordnung über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro (N-SIS-Verordnung, SR 362.0). Entsprechend muss für die Definition der terroristischen Straftaten auf Anhang 1a der N-SIS-Verordnung verwiesen werden.

Die Bestimmung von Art. 6 Abs. 3 Bst. a ist zu eng gefasst. Bei Betäubungsmitteldelikten beispielsweise kann nicht zum Voraus gesagt werden, ob der Tatvorwurf im Ermittlungsverfahren auf ein Vergehen oder ein Verbrechen lautet. Die damit verbundene Unklarheit führt unter Umständen dazu, dass sich die Bearbeitung von PNR-Daten im Nachhinein als unzulässig erweist. Die Kriminalität im Bereich von Betäubungsmitteldelikten zeichnet sich aber durch eine hochgradige Organisation aus. So werden in den allermeisten Fällen nicht die Haupttäterinnen und -täter auf den Flügen verhaftet, sondern Betäubungsmittelkuriere als Mittäterinnen und Mittäter. Deren Verhaftung ist in der Bekämpfung der organisierten Kriminalität im Betäubungsmittelbereich zentral. Insbesondere dadurch lassen sich Netzwerke und Organisationen aufdecken und letztlich auch bekämpfen. Die Bearbeitung von Flugpassagierdaten gibt den Ermittlerinnen und Ermittlern ein wirksames Mittel zur Erkennung der Abläufe in die Hand. Ähnlich verhält es sich bei anderen Themenfeldern der organisierten Kriminalität, wie beispielsweise dem Menschenschmuggel. Diesem Umstand trägt der Deliktskatalog zu wenig Rechnung. Entsprechend ist für die Definition der anderen schweren Straftaten auf den Deliktskatalog von Anhang 1b der N-SIS-Verordnung zu verweisen.

Mit Art. 6 Abs. 3 Bst. b werden Straftaten, die durch das Bundesamt für Zoll und Grenzsicherheit (BAZG) verfolgt werden, in den Deliktskatalog aufgenommen. Das BAZG ist aber keine Strafverfolgungsbehörde im eigentlichen Sinn. Strafverfolgungskompetenzen des BAZG ergeben sich ausschliesslich aus dem Sachzusammenhang «Zoll» und sind rein verwaltungsstrafrechtliche Verfahren. Diese verwaltungsstrafrechtlichen Tatbestände der Bekämpfung von Terrorismus und Schwerstkriminalität gleichzustellen, ist grundsätzlich nicht angebracht. Gemäss Art. 6 Abs. 4 soll zudem erst auf Verordnungsstufe festgelegt werden, bei welchen Delikten in der Verfolgungskompetenz des BAZG Flugpassagierdaten bearbeitet werden dürfen, obschon der Erläuternde Bericht (S. 56 ff.) bereits einen eindeutigen Katalog mit Straftaten enthält. Wir beantragen, Art. 6 Abs. 3 Bst. b und Art. 6 Abs. 4 wegzulassen. Sollte daran festgehalten werden, wären die Deliktskategorien auf Gesetzesstufe zu regeln.

Zur Übermittlung von biometrischen Daten (Art. 6 Abs. 6, Art. 8, Anhang 1):

Im Anhang 1 werden die Flugpassagierdaten definiert. Die biometrischen Daten einer Person fallen nicht darunter. Die PIU kann im Rahmen von Art. 6 Abs. 6 aber biometrische Daten bearbeiten. Wenn der Abgleich der Flugpassagierdaten mit den Daten aus polizeilichen Informationssystemen eine Übereinstimmung ergeben hat, übermittelt die PIU die Daten an die Strafverfolgungsbehörden oder den Nachrichtendienst des Bundes (NDB). Dabei müssen zur Erleichterung der weiteren Strafverfolgung auch biometrische Daten übermittelt werden können. Der Klarheit halber muss dies in Art. 8 ausdrücklich festgehalten werden.

Zu Art. 11:

In Art. 11 ist vorgesehen, dass auf begründeten Antrag hin im Einzelfall Flugpassagierdaten an Strafverfolgungsbehörden des Bundes und der Kantone, dem NDB oder dem Europäischen Polizeiamt übermittelt werden können. Gemäss dem Erläuternden Bericht (S. 32) sind generische Abfragen nicht zulässig. Allerdings verhindert dies auch Abfragen, die auf grössere Datensätze wie beispielsweise ganze Flüge abzielen. Es wird den Ermittlerinnen und Ermittlern damit verunmöglicht, Hinweise auf neue Verhaltensmuster zu verifizieren, nachdem sie Täterinnen und Täter aufgrund anderer Ermittlungsmethoden überführt haben. Da Verhaltensmuster rasch ändern, ist eine regelmässige Überprüfung im Rahmen von grösseren Datensätzen für die Ermittlungsarbeit zentral. Zudem ist die Formulierung im Erläuternden Bericht sehr unspezifisch und kaum praktikabel. Es muss jedenfalls möglich sein, beispielsweise alle Passagiere eines bestimmten Fluges abzufragen. Wir beantragen deshalb, Abfragen von grösseren Datensätzen im Rahmen der Überprüfung von Verhaltensmustern ausdrücklich zu erlauben und dies in der Botschaft entsprechend zu berücksichtigen.

Zu Art. 12:

Der in dieser Bestimmung verwendete Begriff «konkreter Verdacht» in Abs. 1 kommt im Strafrecht nicht vor und sollte deshalb nicht verwendet werden (hingegen: Anfangsverdacht, hinreichender Tatverdacht, dringender Tatverdacht). Zudem ist die Schwelle zu hoch, um für eine solche Meldung überhaupt einen Verdacht zu verlangen. Es muss genügen, wenn «Hinweise» oder «Anhaltspunkte» für eine entsprechende Straftat vorliegen. Ein Verdacht wird im Übrigen für eine Abfrage durch eine Strafverfolgungsbehörde gemäss Art. 11 FPG auch nicht verlangt. Es ist deshalb nicht nachvollziehbar, einen solchen für eine Spontanmitteilung durch die PIU zu verlangen. Gemäss Erläuterndem Bericht ist ein Verdacht «konkret», wenn er sich auf eine bestimmte Person bezieht (S. 32). Ein (konkreter) Verdacht kann sich aber auch auf eine unbekannte Person oder Personengruppe beziehen. Die Bestimmung sind entsprechend anzupassen.

Zu Art. 19 f.:

Für eine wirksame Nutzung von Flugpassagierdaten im Kampf gegen Terrorismus und Schwerstkriminalität ist der Faktor Zeit zentral. Eine zeitlich unmittelbare Weitergabe der Daten durch die PIU ist deshalb entscheidend, insbesondere bei Fahndungen. Die PIU muss deshalb rund um die Uhr tätig sein.

Zu Art. 20:

Wichtig ist, dass sich alle Kantone angemessen an den Kosten für ihre Mitarbeitenden der PIU beteiligen, da alle vom Sicherheitsgewinn profitieren.



Zu Art. 22 Abs. 3:

An eine ausländische PIU sollen keine Daten übermittelt werden können, wenn gegen die betreffende Person kein «begründeter Verdacht» vorliegt. Es ergibt wenig Sinn, einen Verdacht im strafrechtlichen Sinne vorauszusetzen, um die Daten übermitteln zu dürfen, siehe dazu die Bemerkungen zu Art. 12. Entsprechend ist der Begriff «begründeter Verdacht» durch «Anhaltspunkte» zu ersetzen.

Genehmigen Sie, sehr geehrte Frau Bundesrätin,
die Versicherung unserer ausgezeichneten Hochachtung.

Im Namen des Regierungsrates

Der Präsident:

Die Staatsschreiberin:

Ernst Stocker

Dr. Kathrin Arioli





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

RRB Nr.: 795/2022
Direktion: Sicherheitsdirektion
Klassifizierung: Nicht klassifiziert

17. August 2022

**Vernehmlassung des Bundes: Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten
Stellungnahme des Kantons Bern**

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Der Regierungsrat des Kantons Bern bedankt sich für die Möglichkeit, zu oben genannter Vernehmlassung Stellung nehmen zu können.

Aufgrund eines internen Fehlers des Bundesamts für Polizei fedpol wurden die Kantone nicht wie üblich über die Eröffnung des Vernehmlassungsverfahrens informiert. Nach Rückfrage der Staatskanzlei des Kantons Bern hat das fedpol dem Kanton Bern eine Fristverlängerung bis zum 17. August eingeräumt.

1. Grundsätzliches

Der Kanton Bern begrüsst die vorgesehene Einführung der systematischen Bearbeitung von Flugpassagierdaten zur Unterstützung der Verhinderung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten sehr. Ebenfalls möchten wir unsere Bereitschaft zur personellen Beteiligung an der bei fedpol angesiedelten Stelle «Passenger Information Unit (PIU)» sowie zur Ausarbeitung einer entsprechenden Vereinbarung bestätigen, auch wenn der tatsächliche operative Aufwand für den Kanton Bern noch nicht beziffert werden kann. Sodann geht der Regierungsrat davon aus, dass der Bundesrat – wie von fedpol angekündigt – das Urteil des Europäischen Gerichtshofs vom 21. Juni 2022 angemessen berücksichtigen wird.

Gerne erlauben wir uns, folgende Anträge zu stellen:

2. Anträge

2.1 Antrag zu Artikel 6 Absatz 2 FPG

Aus Sicht des Kantons Bern sind mindestens folgende Straftaten zusätzlich in Artikel 6 Absatz 2 aufzunehmen:

- Artikel 260^{sexies} Strafgesetzbuch (StGB; SR 311.0): Anwerbung, Ausbildung und Reisen im Hinblick auf eine terroristische Straftat;
- Artikel 2 des Bundesgesetzes über das Verbot der Gruppierungen «Al-Qaïda» und «Islamischer Staat» sowie verwandter Organisationen (SR 122).

Der Abruf von Flugpassagierdaten fokussiert vor allem auf die Bekämpfung des Terrorismus. In Anbetracht dessen ist es notwendig, dass alle Straftaten mit terroristischem Bezug vom Anwendungsbereich des FPG erfasst sind. Gemäss dem Wortlaut von Artikel 6 Absatz 2 FPG gelten als terroristische Straftaten solche, welche in Anhang 1 Ziffer 22 des Schengen-Informationsaustausch-Gesetzes vom 12. Juni 2009 (SIaG, SR 362.2) enthalten sind. Ziffer 22 enthält jedoch nur den Straftatbestand der Finanzierung des Terrorismus (Art. 260^{quinquies} StGB). Dies steht im Widerspruch zur Aufzählung der terroristischen Straftaten in Anhang 1 des Erläuternden Berichts (vgl. S. 22 und 52). Demgemäss gelten auch die Tatbestände nach Artikel 1 bis 4 des Rahmenbeschlusses des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung (2002/475/JI) als terroristische Straftaten. Der Geltungsbereich ist zwingend zu überprüfen. Insgesamt ist er möglichst extensiv zu halten, damit terroristische Gefährdungen effektiv verhindert und bekämpft werden können. Der Regierungsrat würde entsprechend eine Angleichung an Anhang 1a der N-SIS-Verordnung vom 8. März 2013 (SR 362.0) begrüssen.

2.2 Art. 6 Abs. 3 Bst. a und b FPG

Die Unterscheidung zwischen Straftaten mit einer Strafandrohung von einer Freiheitsstrafe «von mehr als drei Jahren» (Bst. a) und solchen von einer «maximalen Freiheitsstrafe von mindestens drei Jahren» (Bst. b) ist nicht nachvollziehbar. Damit in beiden Fällen Verbrechen und Vergehen erfasst sind, beantragt der Regierungsrat, sowohl für Bst. a als auch für Bst. b eine maximale Freiheitsstrafe von mindestens 3 Jahren vorzusehen.

Artikel 6 Absatz 3 Buchstabe a ist zu eng gefasst, weil zum Beispiel bei Betäubungsmitteldelikten zu Beginn der Ermittlungen oft nicht klar ist, ob der Tatvorwurf auf ein Verbrechen oder «nur» ein Vergehen lautet. Dies könnte dazu führen, dass sich die Bearbeitung von PNR-Daten im Nachhinein als unzulässig erweist. Die Kriminalität im Bereich von Betäubungsmitteldelikten ist jedoch hochgradig organisiert: So werden auf den allermeisten Flügen nicht die Haupttäter verhaftet, sondern Betäubungsmittelkuriere als Gehilfen. Deren Verhaftung ist in der Bekämpfung der organisierten Kriminalität im Betäubungsmittelbereich zentral: Insbesondere dadurch können die Strafverfolgungsbehörden Netzwerke und Organisationen aufdecken und letztlich auch bekämpfen. Die Bearbeitung von Flugpassagierdaten gibt den Ermittlern ein effektives Mittel zur Erkennung der Abläufe in die Hand. Ähnlich verhält es sich in anderen Bereichen der organisierten Kriminalität, zum Beispiel beim Menschenmuggel. Diesem Umstand trägt der Deliktskatalog nach Artikel 6 Absatz 3 Buchstabe a i.V.m. Anhang 2 FPG zu wenig Rechnung. Entsprechend sollte für die Definition der anderen schweren Straftaten auf den Deliktskatalog von Anhang 1b N-SIS-Verordnung zu verwiesen werden.

2.3 Antrag zu Artikel 6 Absatz 6 Buchstabe b FPG

Im erläuternden Bericht hat eine Klarstellung betreffend polizeiliche Sanktionen zu erfolgen.

In der Regel beschlagen terroristische Gefährder auf kantonaler Ebene das polizeiliche Bedrohungsmanagement, aus welchem Massnahmen zum Schutz einzelner Personen und zur Sicherheit der Bevölkerung abgeleitet werden. Diese Massnahmen werden nicht zwingend im Rahmen eines verwaltungsrechtlichen Verfahrens erlassen. Sie können als polizeiliche Reakte angeordnet werden. Sicherheits- oder Schutzmassnahmen können für die Beurteilung der PIU sehr dienlich sein, weshalb für die Datenübermittlung solcher Informationen Klarheit bestehen sollte.

2.4 Artikel 7 FPG (Datenabgleich mit Informationssystemen)

Im erläuternden Bericht ist zu Artikel 7 klärend festzuhalten, dass der vom Kanton entsandte PIU-Mitarbeitende einen Datenabgleich mit den Informationssystemen seines Kantons vornehmen kann. Sollten die gesetzlichen Grundlagen dafür nicht ausreichen, sind solche mit dem FPG zu schaffen. Nur so kann dem angestrebten Ziel gemäss Artikel 1 Absatz 1 FPG hinreichend nachgekommen werden.

Der Bund und die Kantone verfügen mit dem nationalen Polizeiindex über ähnliche Angaben auf nationaler Ebene. Die kantonalen Informationssysteme, welche die Grundlage der präventiven bzw. sicherheitspolizeilichen Arbeit der kantonalen Polizeibehörden darstellen, enthalten aber weitergehende zweckmässige Informationen zur Gefahrenabwehr. Diese Informationen müssen zur Gewährleistung der Sicherheit und der Abwehr terroristischer Gefahren direkt durch die von den Kantonen entsandten PIU-Mitarbeitenden in Abgleich gebracht werden können. Der entsendende Kanton wird den Zugriff seiner Mitarbeitenden auf die Informationssysteme des Kantons nicht einschränken wollen. Entsprechend muss ein Abgleich mit den PIU-Daten ermöglicht werden. Ohne diesen Direktabgleich würden die Wirkung des FPG und damit die sicherheitspolitischen Interessen der Schweiz massgebend geschwächt.

2.5 Antrag zu Artikel 8 Absatz 2 Buchstabe a, Artikel 11 Buchstabe a und Artikel 12 Absatz 1 FPG

Die zuständigen Behörden sind in Artikel 8, 11 und 12 wie folgt zu bezeichnen:

«a. die Polizei- und Strafverfolgungsbehörden des Bundes und der Kantone»

Der Begriff der Strafverfolgungsbehörden der Kantone ist zu eng gefasst. Die Polizeibehörden können bereits präventiv zur Verhinderung von Straftaten Ausschreibungen im RIPOL/SIS erfassen, nicht erst im Strafverfahren. Demnach machen es die sicherheitspolizeilichen Aufgaben notwendig, dass die Polizeibehörden auch als zuständige Behörden bezeichnet werden (analog Art. 10 Abs. 4 Bst. c des Bundesgesetzes über die polizeilichen Informationssysteme des Bundes; BPI, SR 361). Vermutlich ist auch Artikel 8 Absatz 1 FPG mit «das Vorliegen einer Straftat» zu eng formuliert. Ob eine Straftat tatsächlich vorliegt, entscheidet letztlich das Strafgericht. In aller Regel dürfte es sich im Anwendungsbereich des FPG um einen «Verdacht auf das Vorliegen einer Straftat» handeln. Der Regierungsrat ersucht Sie, die Formulierung zu überprüfen und gegebenenfalls anzupassen.

2.6 Antrag zu Artikel 12 und 22

Überprüfung der Formulierungen «konkret» und «begründet» in Bezug auf die erwähnten Verdachtsmomente.

Es stellt sich die Frage, warum in den beiden Normen eine unterschiedliche Formulierung gewählt worden ist und ob die Formulierung angeglichen werden sollte. Weder bei einem begründeten noch bei einem konkreten Verdacht handelt es sich im Übrigen um strafprozessuale Fachbegriffe.

2.7 Anträge zum erläuternden Bericht

- a. Der erläuternde Bericht sollte sich vertiefter mit dem Thema Datensicherheit auseinandersetzen.

Gemäss Artikel 7 Absatz 1 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1) müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Die Pseudonymisierung wird im erläuternden Bericht zu Recht als eine der Datensicherheit zuträgliche Massnahme beschrieben. Der Bundesrat wird auf Verordnungsstufe weitere Massnahmen zu ergreifen haben. Der Regierungsrat erachtet es angesichts der erheblichen Datenmenge und des damit verbundenen Missbrauchspotenzials für angezeigt, bereits im erläuternden Bericht entsprechende Hinweise zu anzubringen.

- b. Der Erläuternde Bericht schränkt die Möglichkeit der Abfragen ein und verbietet «Generische Abfragen, die nicht spezifiziert sind und zu einer Vielzahl von unterschiedlichsten Suchergebnissen führen können» (S. 31 f.). Diese Einschränkung findet im Gesetzeswortlaut aber keinerlei Grundlage. Nur schon deshalb ist sie aus dem Erläuternden Bericht zu entfernen. Zudem ist die Formulierung im Erläuternden Bericht selbst sehr unspezifisch und kaum praktikabel. Nach Ansicht des Regierungsrates muss es – bei hinreichender Begründung – möglich sein, beispielsweise alle Passagiere eines bestimmten Fluges abzufragen.

Der Regierungsrat dankt Ihnen für die Berücksichtigung seiner Anliegen.

Freundliche Grüsse

Im Namen des Regierungsrates

Christine Häslar
Regierungspräsidentin

Christoph Auer
Staatsschreiber

Verteiler:

- Sicherheitsdirektion
- Kantonspolizei Bern
- Justizleitung des Kantons Bern
- Kantonale Datenschutzaufsicht

Justiz- und Sicherheitsdepartement

Bahnhofstrasse 15
Postfach 3768
6002 Luzern
Telefon 041 228 59 17
justiz@lu.ch
www.lu.ch

Eidg. Justiz- und Polizeidepartement
Bundesamt für Polizei

per Mail
kd-rechtsabteilung@fedpol.admin.ch

Luzern, 5. Juli 2022

Protokoll-Nr.: 882

Polizeiwesen: Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG); Vernehmlassung

Sehr geehrte Damen und Herren

Im Namen und Auftrag des Regierungsrates teile ich Ihnen mit, dass der Kanton Luzern das neue Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten unterstützt. Mit dem Flugpassagierdatengesetz wird eine Lücke geschlossen und die gesetzliche Grundlage dafür geschaffen, dass diese Daten – wie dies in über 60 anderen Staaten der Welt bereits heute der Fall ist – auch in der Schweiz bearbeitet werden können. Es sind keine Gründe ersichtlich, weshalb die Schweiz auf die damit verbundenen Möglichkeiten verzichten sollte. Mit den fraglichen Informationen kann ein Mehrwert geschaffen werden, indem diese Daten für die Aufklärung und Verhinderung von terroristischen Straftaten und anderen schweren Delikten herangezogen werden können.

Bemerkungen zu einzelnen Bestimmungen:

zu Artikel 7 Datenabgleich mit Informationssystemen

Dank Art. 7 FPG werden die Strafverfolgungsbehörden in Zukunft über die Ein- oder Ausreise von ihnen national oder international ausgeschriebenen Personen informiert. Dies ist insbesondere bei Flugbewegungen innerhalb des Schengenraums, bei denen keine Grenzkontrollen durchgeführt werden, eine deutliche Verbesserung zum heutigen Zustand. Einen grossen Einfluss auf den Nutzen dieser neuen Möglichkeit hat jedoch die Frist, innert der mit einer solchen Meldung gerechnet werden kann. Gemäss Art. 2 Abs. 2 FPG müssen die Luftverkehrsunternehmen die PNR-Daten 48 bis 24 Stunden vor dem planmässigen Abflug und dann nochmals nach Abschluss des Boardings der PIU übermitteln. Wie lange die PIU dann Zeit hat, diese Daten mit den Systemen (z.B. Ripol) abzugleichen und eine Meldung den betroffenen Behörden zu tätigen, ist dem Gesetz bzw. dem erläuternden Bericht nicht zu entnehmen.

Zwar wird in Art. 7 Abs. 2 FPG festgehalten, dass der automatische Abgleich "unmittelbar nach Erhalt der Daten" erfolgen müsse. Jedoch müssen automatisch erzielte Treffer anschliessend noch manuell von einem Mitarbeiter überprüft werden, bevor sie den Behörden übermittelt werden (Art. 7 Abs. 3 FPG). Gemäss Bericht ist zudem noch unklar, ob ein 24/7-Betrieb gewährleistet werden soll. Dabei gilt es auch zu bedenken, dass nach einer entsprechenden Meldung auch der Zugriff (also die Verhaftung der ausgeschriebenen Person unmittelbar nach der Landung am Zielflughafen) noch organisiert werden muss. Weniger zeitkritisch wäre es, wenn die betroffenen Flughafenpolizeien von der PIU direkt über die Ein-/Ausreise einer (im Ripol) ausgeschriebenen Person informiert würden und deren Festnahme selbständig durchgeführt würde. Der Nutzen der Meldungen hängt in der Praxis somit wesentlich davon ab, dass diese rechtzeitig bei den Strafverfolgungsbehörden eintreffen.

zu Artikel 9 Datenabgleich mit Risikoprofilen und Beobachtungslisten

Auch die in Art. 9 FPG vorgesehene Möglichkeit Risikoprofile und Beobachtungslisten erstellen und diese laufend mit den gelieferten Passagierdaten abgleichen zu lassen, dürfte für die Strafverfolgungsbehörden gerade bei Ermittlungen im Bereich von organisierter Kriminalität grundsätzlich sehr nützlich sein. Gemäss Art. 9 Abs. 1 FPG kann die PIU auch auf Antrag der Behörden solche Risikoprofile und Beobachtungslisten erstellen. Es handelt sich dabei also um eine Kann-Vorschrift, weshalb der Nutzen dieses Instrumentes für die Strafverfolgungsbehörden stark von der Praxis der PIU abhängt. Im Bericht wird zudem auch nicht ausgeführt, in welcher Form dieser Antrag sowie der Entscheid der PIU zu erfolgen hat (schriftlich, mündlich, begründet), wer bei der PIU über einen solchen Antrag entscheidet und welche Möglichkeiten man gegen einen ablehnenden Entscheid hat. Diese Aspekte gilt es beim Erstellen der entsprechenden Verordnung zu berücksichtigen.

Gemäss dem vorgeschlagenen Absatz 5 werden Risikoprofile und Beobachtungslisten regelmässig auf ihre Begründetheit und Wirksamkeit hin überprüft, was zu begrüssen ist. Es sollte auch verhindert werden, dass die Risikoprofile und Beobachtungsliste zu Diskriminierung führt. Deswegen sollten Risikoprofile und Beobachtungsliste auch auf ihre Nichtdiskriminierung bzw. Gleichbehandlung der betroffenen Personen überprüft werden.

zu Artikel 11 Übermittlung von Flugpassagierdaten auf Antrag

Ähnlich wie bei Art. 9 verhält es sich auch mit der in Art. 11 FPG vorgesehenen Möglichkeit, dass Strafverfolgungsbehörden bei der PIU im Rahmen von Ermittlungen in einem Strafverfahren Passagierdaten herausverlangen können. Auch diese Möglichkeit kann bei der Aufklärung von Straftaten von sehr grossem Nutzen sein. Doch auch hier handelt es sich um eine Kann-Vorschrift und es wird weder im Gesetz selbst noch im Bericht erwähnt, wer bei der PIU über solche Anträge entscheidet und ob es dagegen ein Rechtsmittel gibt. Auch hier dürfte der Nutzen also wiederum stark von der Handhabung solcher Anfragen durch die PIU abhängen. Wir regen an, auch diesen Aspekt beim Erstellen der entsprechenden Verordnung zu berücksichtigen.

zu Artikel 15 Aufhebung der Pseudonymisierung

Bezüglich Art. 15 FPG dürfte aufgrund der zu erwartenden grossen Relevanz solcher Passagierdaten und dem breit gefassten Deliktskatalog nur schon von Seiten der Strafverfolgungsbehörden mit einer erheblichen Anzahl von Anträgen auf Aufhebung der Pseudonymisierung zu rechnen sein (in Ermittlungen dürften denn auch vielfach Daten, die älter als 6 Monate sind, relevant sein). Dem ist bezüglich der nötigen Kapazitäten beim Bundesverwaltungsgericht Rechnung zu tragen.

Zu Artikel 17 Aufsicht

Gemäss dieser Bestimmung überwacht die Datenschutzstelle von fedpol die Einhaltung der Datenschutzvorschriften. Um diese Aufgabe effektiv zu erfüllen, sollte sichergestellt werden, dass die Datenschutzstelle von fedpol Zugang zu sämtlichen verarbeiteten Daten erhält (vgl. Art. 6(7) Richtlinie (EU) 2016/681).

Zu Artikel 18 Auskunftsrecht

Gemäss Art. 18 Abs. 2 sind die pseudonymisierten Daten vom Auskunftsrecht ausgenommen. Pseudonymisierte Daten gelten als Personendaten und sollten nicht kategorisch vom Auskunftsrecht ausgenommen werden. Gemäss dem erläuternden Bericht versteht es sich mit Blick auf den Zweck der Datenbearbeitung, dass die Auskunft nicht immer oder nicht immer vollständig erteilt werden kann; zum Beispiel, wenn die Verweigerung der Auskunftserteilung im überwiegenden öffentlichen Interesse, insbesondere der inneren oder der äusseren Sicherheit der Schweiz, erfolgt. Grundsätzlich sollte das Auskunftsrecht der Betroffenen auf alle Daten, einschliesslich pseudonymisierte Daten, ausgedehnt und nur ausnahmsweise beschränkt werden.

zu Artikel 22 Amtshilfe

Inhaltlich kann diese Bestimmung zu ungewollten Fragestellungen führen. So kann die Definition insbesondere von schweren Straftaten je nach Land unterschiedlich sein und es gilt zu vermeiden, dass die Schweiz Daten von Personen weiterleiten muss, die in einem Land gegen schwere Straftaten verstossen, deren Definition mit dem schweizerischen Deliktskatalog der schweren Straftaten und der schweizerischen Rechtsauffassung unvereinbar sind. Wir empfehlen daher, die doppelte Strafbarkeit, wie sie in Art. 64 des Bundesgesetzes über internationale Rechtshilfe in Strafsachen ausgeführt ist, im Flugpassagierdatengesetz sinngemäss zu verankern, sodass diese Regelung auch für die Übermittlung von Flugpassagierdaten zur Anwendung kommt.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse



Paul Winiker
Regierungsrat



Landammann und Regierungsrat des Kantons Uri

Bundesamt für Polizei fedpol
Nussbaumstrasse 29
3003 Bern

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten; Vernehmlassung

Sehr geehrte Frau Direktorin
Sehr geehrte Damen und Herren

Am 20. Juni 2022 hat das Eidgenössische Justiz- und Polizeidepartement EJPD den Regierungsrat im Rahmen eines Vernehmlassungsverfahrens eingeladen, zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten bis zum 31. Juli 2022 Stellung zu nehmen.

Aufgrund der geringen Betroffenheit des Kantons Uri verzichten wir auf die Einreichung einer Stellungnahme. Zudem bitten wir Sie, in Zukunft die ordentlichen Vernehmlassungsfristen einzuhalten.

Sehr geehrte Frau Direktorin, sehr geehrte Damen und Herren, wir danken Ihnen für die Gelegenheit zur Stellungnahme und grüssen Sie freundlich.

Altdorf, 8. Juli 2022

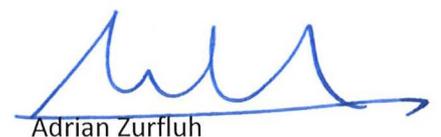


Im Namen des Regierungsrats

Der Landammann

Der Kanzleidirektor-Stv.


Urs Janett


Adrian Zurfluh



6431 Schwyz, Postfach 1260

per E-Mail

Eidgenössisches Justiz- und Polizeidepartement
3003 Bern

kd-rechtsabteilung@fedpol.admin.ch

Schwyz, 5. Juli 2022

Flugpassagierdatengesetz

Vernehmlassung des Kantons Schwyz

Sehr geehrte Frau Bundesrätin

Am 13. April 2022 haben Sie die Kantonsregierungen eingeladen, zur oben erwähnten Vernehmlassungsvorlage bis 31. Juli 2022 Stellung zu nehmen.

Bei der Buchung eines Flugtickets werden von den Passagieren verschiedene Daten erhoben, die von den Luftverkehrsunternehmen für die Reservation und Abfertigung des Fluges benötigt werden. Dieser Flugpassagierdatensatz, international bekannt als Passenger Name Record (PNR), enthält beispielsweise den Namen und die Anschrift eines Flugpassagiers oder einer Flugpassagierin, aber auch andere Informationen wie Angaben zum mitgeführten Gepäck oder zu den Zahlungsmodalitäten. Mehr als 60 Staaten haben das Potenzial von PNR erkannt und nutzen die Daten seit Jahren als Instrument zur Bekämpfung von Terrorismus und anderer schwerer Kriminalität. Mit der Bearbeitung von Flugpassagierdaten und spezifischen Datenanalysen können nicht nur Personen ermittelt werden, die den Strafverfolgungsbehörden bereits bekannt sind. Vielmehr lassen sich über neue Ermittlungsansätze auch Personen identifizieren, die den Strafverfolgungsbehörden bislang nicht bekannt waren, aber mit Terrorismus und anderer schwerer Kriminalität in Zusammenhang stehen könnten.

Die Nutzung von PNR wird derzeit global vorangetrieben. Drei für die Schweiz bindende Resolutionen des UNO-Sicherheitsrats weisen die internationale Gemeinschaft an, Flugpassagierdaten zur Verhinderung von Terrorismus zu verwenden. Die Schweiz ist als Mitglied der Internationalen Zivilluftfahrtorganisation (ICAO) verpflichtet, deren PNR-Standards anzuwenden. Die Europäische Union (EU) hat ihre Mitgliedstaaten mit der Richtlinie (EU) 2016/681 verpflichtet, nationale PNR-Systeme aufzubauen. Die Richtlinie ist keine Weiterentwicklung des Schengen-Besitzstandes. Dennoch ist die Schweiz von deren Umsetzung betroffen, denn alle Luftverkehrsunternehmen mit Flügen aus der Schweiz in die EU und umgekehrt sind zur Datenübermittlung verpflichtet.

Heute werden zwar PNR-Daten von Flügen aus der Schweiz namentlich in EU-Mitgliedstaaten, ins Vereinigte Königreich, in die USA oder nach Kanada übermittelt, die Schweiz selber kann aber PNR-Daten nicht systematisch bearbeiten, solange sie über keine gesetzliche Grundlage und ein nationales PNR-System verfügt. Ohne PNR-System stehen der Schweiz (im Vergleich zu anderen Schengen-Staaten) weniger Daten für die Einreisekontrollen zur Verfügung. Damit riskiert sie, dass Personen, die eine Gefahr für die öffentliche Sicherheit darstellen, über die Schweiz unerkannt in den Schengen-Raum gelangen. Die PNR-Nutzung ist schliesslich auch eine Bedingung der USA zum Verbleib der Schweiz im Visa Waiver Program. Dieses erlaubt es schweizerischen Staatsangehörigen, zu geschäftlichen oder touristischen Zwecken für bis zu 90 Tage ohne Visum in die USA zu reisen.

Das internationale Recht verpflichtet somit die Schweiz, die PNR-Standards anzuwenden. Zuständig für die Bearbeitung der Daten soll eine neu zu schaffende, beim Bundesamt für Polizei (fedpol) angesiedelte Stelle (Passenger Information Unit [PIU]) werden. Durch die Abgleichung von Flugpassagierdaten mit polizeilichen Informationssystemen lassen sich im Vorfeld eines Fluges Personen erkennen, die eine Gefahr darstellen könnten. Diese Treffer werden vom PIU den zuständigen Behörden von Bund und Kantonen bekannt gegeben, sodass diese rechtzeitig die notwendigen Massnahmen in die Wege leiten können. Die Flugpassagierdaten werden nach Ablauf von sechs Monaten pseudonymisiert und nach fünf Jahren gelöscht. Die Hälfte der Mitarbeitenden, die bei der PIU tätig sind, soll von den Kantonen entsendet und von diesen finanziert werden.

Der Kanton Schwyz stimmt der Vorlage im Wesentlichen zu. Die systematische Überprüfung respektive Bearbeitung von Flugpassagierdaten unterstützt die Verhinderung, Ermittlung und Verfolgung von terroristisch motivierten und anderen gesetzlich erwähnten schweren Straftaten wesentlich. Die geplante zentrale und organisatorische Ansiedelung der PIU beim fedpol ist zu begrüssen. Das Vorgehen erscheint auf den ersten Blick pragmatisch, im Detail ergeben sich jedoch aus Sicht des Kantons Schwyz eine Vielzahl organisatorischer und prozessualer Fragen. In dieser Hinsicht wäre die Organisation über ein Konkordat mit strukturierten und adäquaten Verrechnungsmechanismen zu prüfen. Zentral ist, dass die Kantone bei den weiteren Planungsarbeiten und insbesondere bei der Erarbeitung der konkreten Organisationsstruktur von Beginn weg miteinbezogen werden. Dabei ist zudem der, trotz Automatisierung erstaunlich hohe, Personalansatz kritisch zu prüfen. Datenschutzrechtlich ist und bleibt die Vorlage heikel. Hier ist unbedingt darauf zu achten, dass auch die in diesem Bereich international ergangene Gerichtsentscheide miteinbezogen werden. So hat beispielsweise der Europäische Gerichtshof (Grosse Kammer) am 21. Juni 2022 bezüglich des belgischen Rechts festgehalten, dass Passagierdaten von EU-Flügen nur bei einer echten terroristischen Bedrohung gespeichert werden dürfen oder auf sogenannten «Verbrecherrouten». Die Speicherung ist auf das «absolut Notwendige» zu beschränken. Der erwähnte Entscheid betrifft zwar nur die belgische Gesetzgebung, deutet aber grundsätzlich auf einen Korrekturbedarf in der Speicherung von Passagierdaten hin.

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

Im Namen des Regierungsrates:



André Rügsegger
Landammann



Dr. Mathias E. Brun
Staatsschreiber



CH-6060 Sarnen, Enetriederstrasse 1, SSD

Bundesamt für Polizei
Eidgenössisches
Justiz- und Polizeidepartement EJPD
3003 Bern

per Mail an:
kd-rechtsabteilung@fedpol.admin.ch

Referenz/Aktenzeichen: OWSTK.4408
Unser Zeichen: fu

Sarnen, 26. August 2022

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten; Stellungnahme

Sehr geehrte Frau Bundesrätin, *geschätzte Karin*
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Einladung zur Vernehmlassung betreffend Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten.

Wir haben die Unterlagen geprüft und begrüssen die vorgesehene Einführung der systematischen Bearbeitung von Flugpassagierdaten zur Verhinderung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten. Ebenso unterstützen wir das Vorgehen, die Materie in einem neuen Gesetz zu erfassen. Die Vorlage enthält eine technologieneutrale Formulierung, was auch die Reaktion bei zukünftigen technologischen Entwicklungen ohne Gesetzesanpassungen zulässt und deshalb sehr wichtig ist. Ebenso erscheint es sachgerecht, fedpol die technischen Einzelheiten der Übermittlung festlegen zu lassen. Dabei sind auch die datenschutzrechtlichen Vorgaben entsprechend zu berücksichtigen.

Die zentrale, organisatorische Ansiedlung der PIU (Passenger Information Unit) beim Bund wird sehr begrüsst. Es ist auch nachvollziehbar, die PIU hälftig aus Mitarbeitenden des Bundes und der Kantone zu besetzen. So ist der Kompetenztransfer sichergestellt, was der Erstellung von Risikoprofilen und Beobachtungslisten förderlich ist.

Zu erwähnen ist, dass die Vorlage zu einem personellen Mehraufwand für die Kantone führt, der noch nicht abschliessend beziffert werden kann. Ebenso ist ein künftiger Verteiler dieser Aufwendungen

unter den Kantonen noch nicht vorhanden. Daher ist es wichtig die Vorlage so auszugestalten, dass eine effiziente und effektive Arbeitsweise der PIU ermöglicht wird.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse



Christoph Amstad
Regierungsrat

Kopie an:

- Kantonale Mitglieder der Bundesversammlung
- Kantonspolizei
- Staatskanzlei (Kommunikation)



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

PER E-MAIL

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter
Bundeshaus West
3003 Bern

Telefon 041 618 79 02
staatskanzlei@nw.ch
Stans, 5. Juli 2022

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten. Stellungnahme

Sehr geehrte Frau Bundesrätin

Mit undatiertem Schreiben eröffnete das Eidgenössische Justiz- und Polizeidepartement (EJPD) unter anderem bei den Kantonen das Vernehmlassungsverfahren zum Entwurf des Bundesgesetzes über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten. Für die Möglichkeit zur Stellungnahme bedanken wir uns herzlich.

Mit dieser Gesetzesvorlage soll auch die Schweiz systematisch Flugpassagierdaten bearbeiten können, um Behörden des Bundes und der Kantone bei der Verhinderung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten zu unterstützen.

Der Kanton Nidwalden begrüsst, dass die Bearbeitung der Flugpassagierdaten in einem Gesetz einheitlich geregelt wird. Somit müssen die Regelungen nicht in mehreren bestehenden Bundesgesetzen eingefügt werden. Zum rechtlichen Inhalt des Flugpassagierdatengesetzes werden keine Ergänzungen oder Anpassungen gefordert. Insbesondere wird die technologie-neutrale Formulierung des Gesetzes begrüsst. Hiermit wird sichergestellt, dass im Falle zukünftiger technologischer Entwicklungen keine Notwendigkeit einer Gesetzesrevision besteht. Diesbezüglich wird die in Art. 2 Abs. 4 festgelegte Zuordnung der Festlegung der technischen Einzelheiten der Übermittlung an das Bundesamt für Polizei (fedpol) begrüsst.

Mit der Einführung des Flugpassagierdatengesetzes wird beim Bundesamt für Polizei (fedpol) eine neue Stelle geschaffen und angesiedelt. Die Stelle (international als Passenger Information Unit, kurz PIU, bezeichnet) erhält die Daten von den Luftverkehrsunternehmen 24 bis 48 Stunden vor Abflug eines Flugzeuges aus der oder in die Schweiz. Die PIU gleicht die erhaltenen Daten mit polizeilichen Informationssystemen ab und gibt diese bei "Treffern" an die zuständigen Behörden von Bund und Kantonen weiter.

Der Kanton Nidwalden begrüsst die in der Vernehmlassungsvorlage vorgesehene organisatorische Ansiedlung der PIU beim Bund. Wir unterstützen auch das vorgesehene Entsendemodell, wonach die Hälfte der Mitarbeitenden, die bei der PIU tätig sind, von den Kantonen entsendet und auch von diesen finanziert werden. Das Entsendemodell erlaubt einen

Kompetenztransfer von der PIU in die Kantone, welcher insbesondere für das Konzipieren von Risikoprofilen und Beobachtungslisten nützlich sein kann. Derzeit wird von einem personellen Aufwand nach dem vollen Ausbau der PIU von 30 Vollzeitäquivalenten (FTE) ausgegangen. Dies würde sich auf die Kantone mit 15 FTE auswirken.

Wie die Beteiligung der Kantone geregelt werden soll, ist derzeit noch offen. Gemäss Vernehmlassungsentwurf ist vorgesehen, diese in einer noch zu erstellenden Vereinbarung zwischen Bund und Kantonen zu regeln. Um hier eine von allen betroffenen Kantonen getragene Lösung zu erreichen, müssen die Kantone zwingend von Anfang an in die Erarbeitung dieser Vereinbarung einbezogen werden.

Der Regierungsrat Nidwalden bedankt sich für die Möglichkeit zur Stellungnahme. Er unterstützt den Entwurf des Bundesgesetzes über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten.

Freundliche Grüsse
NAMENS DES REGIERUNGSRATES



Joe Christen
Landammann



lic. iur. Armin Eberli
Landschreiber

Geht an:
- kd-rechtsabteilung@fedpol.admin.ch

Regierungsrat
Rathaus
8750 Glarus

Eidgenössisches Justiz- und Poli-
zeidepartement
3003 Bern

Glarus, 16. August 2022
Unsere Ref: 2022-143

Vernehmlassung i. S. Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten

Hochgeachtete Frau Bundesrätin
Sehr geehrte Damen und Herren

Das Eidgenössische Justiz- und Polizeidepartement gab uns in eingangs genannter Angelegenheit die Möglichkeit zur Stellungnahme. Dafür danken wir und können Ihnen mitteilen, dass wir mit der Vorlage einverstanden sind und diese im Grundsatz begrüßen. Insbesondere wird von uns auch die organisatorische Ansiedlung der Aufgabe beim Bund befürwortet. Wie die Beteiligung der Kantone genau geregelt sein soll, ist derzeit aber noch offen. Gemäss Vernehmlassungsentwurf ist vorgesehen, diese in einer noch zu erstellenden Vereinbarung zwischen Bund und Kantonen festzulegen. In deren Ausarbeitung sind die Kantone unbedingt von Anfang an einzubeziehen.

Genehmigen Sie, hochgeachtete Frau Bundesrätin, sehr geehrte Damen und Herren, den Ausdruck unserer vorzüglichen Hochachtung.

Freundliche Grüsse

Für den Regierungsrat



Benjamin Mühlemann
Landammann



Hansjörg Dürst
Ratsschreiber

E-Mail an (PDF- und Word-Version):
- kd-rechtsabteilung@fedpol.admin.ch

Regierungsrat, Postfach, 6301 Zug

Nur per E-Mail

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Zug, 23. August 2022 rv

**Vernehmlassung zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur
Bekämpfung von terroristischen und anderen schweren Straftaten
Stellungnahme des Kantons Zug**

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit undatiertem Schreiben haben Sie die Kantonsregierungen eingeladen, sich bis am 31. Juli 2022 bzw. mit Fristverlängerung bis 31. August 2022 zur obgenannten Vorlage vernehmen zu lassen. Wir danken Ihnen für die Möglichkeit zur Stellungnahme und nehmen diese gerne wahr.

Grundsätzlich begrüssen wir die Einführung und Stossrichtung der Gesetzesvorlage, welche der Schweiz die systematische Bearbeitung von Flugpassagierdaten zur Verhinderung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten ermöglicht. Ebenso wird die zentrale, organisatorische Ansiedlung der PIU (Passenger Information Unit) beim Bund als sehr sinnvoll erachtet. Allerdings wird der Entwurf mit Blick auf das Urteil C-817/19 des Europäischen Gerichtshofes vom 21. Juni 2022 in verschiedener Hinsicht und insbesondere hinsichtlich der Aufbewahrungsfrist zu überdenken sein. In Bezug auf die Inkraftsetzung des Gesetzes ist zu berücksichtigen, dass den Kantonen genügend Zeit für die Budgetierung der entsprechenden Stellen zur Verfügung gestellt werden muss.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse
Regierungsrat des Kantons Zug



Martin Pfister
Landammann



Tobias Moser
Landschreiber

Versand per E-Mail an:

- EJPD (kd-rechtsabteilung@fedpol.admin.ch; als PDF- und Word-Version)
- Sicherheitsdirektion (info.sd@zg.ch)
- Zuger Polizei (kommandooffice.polizei@zg.ch)
- Obergericht des Kantons Zug (marc.siegwart@zg.ch)
- Datenschutzstelle des Kantons Zug (datenschutz.zug@zg.ch)
- Zuger Mitglieder der Bundesversammlung
- Staatskanzlei (info.staatskanzlei@zg.ch zur Aufschaltung der Vernehmlassungsantwort im Internet)



ETAT DE FRIBOURG
STAAT FREIBURG

Conseil d'Etat CE
Staatsrat SR

Rue des Chanoines 17, 1701 Fribourg

T +41 26 305 10 40, F +41 26 305 10 48
www.fr.ch/ce

Conseil d'Etat
Rue des Chanoines 17, 1701 Fribourg

PAR COURRIEL

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

Courriel : kd-rechtsabteilung@fedpol.admin.ch

Fribourg, le 28 juin 2022

2022-746

Loi fédérale sur le traitement des données relatives aux passagers aériens pour la lutte contre les infractions terroristes et les autres infractions pénales graves

Madame la Conseillère fédérale,

Par courrier du 13 avril dernier, vous nous avez consultés sur le projet cité en titre, et nous vous en remercions.

Sur le fond, nous approuvons ce projet, qui renforcera la sécurité de notre pays dans le domaine de la lutte contre le terrorisme et d'autres infractions pénales graves.

Si nous pouvons admettre le principe d'une participation des cantons en termes de mise à disposition de personnel policier au sein de l'Unité d'information passagers (UIP), nous regrettons que le projet n'évoque aucune clé de répartition ni la prise en compte dans cette clé de la présence ou non d'un aéroport international sur sol cantonal. Cela nous laisse dans l'incertitude sur notre engagement futur dans la mise en œuvre de l'UIP, sachant que notre Police cantonale ne dispose a priori pas, dans son plan de développement à moyen terme, de personnel pour y contribuer.

Avec cette réserve, nous vous réitérons notre appui de principe à ce projet et vous prions de croire, Madame la Conseillère fédérale, à l'assurance de nos sentiments les meilleurs.

Au nom du Conseil d'Etat :

Olivier Curty, Président



Danielle Gagnaux-Morel, Chancelière d'Etat

Copie

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

Regierungsrat

Rathaus / Barfüssergasse 24
4509 Solothurn
www.so.ch

Bundesamt für Polizei fedpol
Rechtsabteilung
Guisanplatz 1A
3003 Bern

16. August 2022

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG) – Vernehmlassung

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Für die Gelegenheit zur Stellungnahme danken wir. Gerne äussern wir uns wie folgt:

Wir begrüssen, das mit dem Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG) die gesetzliche Grundlage für die zielgerichtete und angemessene Nutzung bestimmter Personendaten (PNR) zwecks Bekämpfung schwerer Straftaten geschaffen wird. In anderen Staaten gehört die Bearbeitung von PNR bereits seit längerem zum staatlichen Massnahmenpaket zur Abwehr schwerer Straftaten und Gewährleistung der inneren Sicherheit. Zudem würde ein fortdauerndes Abseitsstehen das Risiko bergen, dass zur Umgehung der Datenbearbeitung durch andere Staaten bewusst die Schweiz zur Ein- beziehungsweise Ausreise benutzt wird.

Die vorgeschlagene Zusammenarbeit zwischen den Luftverkehrsunternehmen und der bei fedpol angegliederten Passenger Information Unit (PIU) erachten wir als sachgerecht. Auch die weiteren Regelungen (gesetzliche Meldepflicht der Luftverkehrsunternehmen und Definition der Übermittlungszeitpunkte (Art. 2 E-FPG), Sanktionen bei Verletzung der Meldepflicht (Art. 23 E-FPG), Vorgaben für die Datenübermittlung an ausländische Behörden (Art. 3 und 21 E-FPG)) begrüssen wir. Zustimmend nehmen wir den definierten Umfang der zu übermittelnden Flugpassagierdaten (Anhang 1) zur Kenntnis, zumal besonders schützenswerte Personendaten ausdrücklich davon ausgenommen sind (Art. 2 Abs. 3 E-FPG). Ausdrücklich einverstanden sind wir ausserdem mit den vorgeschlagenen Deliktskategorien (Art. 6 E-FPG i.V.m. Anhang 2).

Als Single Point of Contact (SPOC) wird die PIU für die Luftverkehrsunternehmen und ausländische Behörden allenfalls 24/7 betrieben werden. Das Personal der PIU soll je hälftig aus Mitarbeitenden des Bundes und der Kantone bestehen (Art. 20 E-PFG), wobei die Kantone die Kosten für ihre Mitarbeitenden zu tragen haben (Abs. 4). Vorgesehen ist eine befristete Entsendung von Mitarbeitenden der Kantone, analog zu bereits bestehenden besonderen Zusammenarbeitsmodellen zwischen dem Bund und den Kantonen (bspw. bei den Polizei- und Kooperationszentren in Genf und Chiasso sowie bei der ausserprozessualen Zeugenschutzstelle). Aufgrund der föderal ausgestalteten Strafverfolgung der Schweiz ist auch für die personelle

Ausstattung der PIU ein solches Modell angezeigt. Die Zuständigkeit für die Strafverfolgung der Delikte gemäss Anhang 2 liegt weitgehend bei den Kantonen. Dementsprechend hat die Umsetzung der Vorlage erhebliche Auswirkungen auf die Kantone. Die von den Kantonen zu entsendenden Polizeiangehörigen fehlen während der Dienstausbildung bei der PIU im kantonalen Polizeikorps. Ausserdem sind die Polizeikorps gehalten, die Bearbeitung von PNR-Daten zu integrieren. Sie haben entsprechende Spezialisten auszubilden, um die wirkungsvolle Zusammenarbeit mit der PIU im Einzelfall zu gewährleisten. Ergibt sich Erkenntnis, hat die kantonal zuständige Strafverfolgungsbehörde überdies die erforderlichen Massnahmen zu ergreifen. Der sich aus der Umsetzung der Vorlage ergebende Zusatzaufwand für die Kantone lässt sich vorab nicht konkret einschätzen.

Die bereits heute bekannte Entsendungsverpflichtung sowie die Implementierung der Datenbearbeitung in die kantonale Polizeitätigkeit sind im Rahmen der anstehenden Bestandsplanung zu berücksichtigen. Diesem Zusatzaufwand ist der Nutzen gegenüberzustellen. Diesbezüglich teilen wir vollumfänglich die auf Seite 17 der Erläuterungen dargelegte Ansicht: Schwere Kriminalität verursacht immense Schäden. Der Rechtsstaat hat derartige Straftaten aus volkswirtschaftlichen Gründen entschieden zu bekämpfen und er ist zum Schutz seiner Bevölkerung dazu verpflichtet.

IM NAMEN DES REGIERUNGSRATES

sig.
Dr. Remo Ankli
Landammann

sig.
Andreas Eng
Staatsschreiber



Rathaus, Marktplatz 9
CH-4001 Basel

Tel: +41 61 267 85 62
Fax: +41 61 267 85 72
E-Mail: staatskanzlei@bs.ch
www.regierungsrat.bs.ch

Bundesamt für Polizei (fedpol)

Per E-Mail an:
kd-rechtsabteiluna@fedpol.admin.ch

Basel, 5. Juli 2022

Präsidentialnummer: P220836

Regierungsratsbeschluss vom 5. Juli 2022

Vernehmlassung zur Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG); Stellungnahme des Kantons Basel-Stadt

Sehr geehrte Damen und Herren

Mit Schreiben vom 13. April 2022, bei uns erst im Juni 2022 eingegangen, haben Sie uns die Vernehmlassungsunterlagen zur Revision des neuen oben genannten Gesetzes zukommen lassen. Wir danken Ihnen für die Gelegenheit zur Stellungnahme und lassen Ihnen nachstehend Bemerkungen zukommen.

Der Regierungsrat des Kantons Basel-Stadt begrüsst die vorgesehene Einführung der systematischen Bearbeitung von Flugpassagierdaten zur Unterstützung der Verhinderung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten. Mit dieser setzt die Schweiz ein Zeichen für mehr Sicherheit und entspricht internationalen Verpflichtungen.

Richtig erscheint uns, die organisatorische Ansiedlung der PIU beim Bund und ein Entsendemodell, nachdem sich die PIU aus Mitarbeitenden des Bundes und der Kantone zusammensetzt und die entsendende Behörde dafür die Kosten trägt. Dies erlaubt – wie in der Vernehmlassungsvorlage erwähnt – den Kompetenztransfer von der PIU in die Kantone, der insbesondere für das Konzipieren von Risikoprofilen und Beobachtungslisten nützlich sein kann. Eine hälftige personelle Beteiligung der Kantone an der PIU lehnen wir allerdings ab. Der Kanton Basel-Stadt kann und möchte höchstens einen Mitarbeitenden an die PIU entsenden

Schliesslich sei darauf hingewiesen, dass der Datenschutzbeauftragte des Kantons Basel-Stadt – aus eingangs erwähnten Gründen der verzögerten Zusendung – die datenschutzrechtlichen Aspekte der Vorlage noch nicht vollständig abklären konnte. Allfällige datenschutzrechtliche Bedenken würden wir Ihnen sobald als möglich nachreichen.

Regierungsrat des Kantons Basel-Stadt

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Im Namen des Regierungsrates des Kantons Basel-Stadt



Beat Jans
Regierungspräsident



Barbara Schüpbach-Guggenbühl
Staatsschreiberin

Kopie

Datenschutzbeauftragter des Kantons Basel-Stadt

Regierungsrat BL, Rathausstrasse 2, 4410 Liestal
Eidgenössisches Justiz- und
Polizeidepartement
kd-rechtsabteilung@fedpol.admin.ch

Liestal, 30. August 2022

Vernehmlassung
zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung
von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz)

Sehr geehrte Frau Bundesrätin

Besten Dank für die Möglichkeit zur Meinungsäusserung, zum erwähnten Gesetzesentwurf teilen wir Folgendes mit:

A. Allgemeine Bemerkungen

Grundsätzlich begrüssen wir die Einführung und Zielsetzung des neuen Gesetzes. Damit können namentlich Polizei- und Strafverfolgungsbehörden Informationen über die Anreise oder Abreise von Personen bearbeiten, die im Verdacht terroristischer oder anderer schwerer Straftaten stehen. Heute ist es für diese Behörden äusserst aufwändig zu eruieren, ob jemand mit einem bestimmten Flug eingereist oder ausgereist ist. Teils braucht es dafür ein Rechtshilfeersuchen in das Ausland, das leider nicht selten unbeantwortet bleibt. Diese für unsere Sicherheitslage elementaren Abklärungen werden durch die Einführung eines PNR¹-Systems massgeblich verbessert.

Den entworfenen Gesetzesregelungen können wir grundsätzlich zustimmen, dies gilt auch für die Einrichtung einer zentralen Bundesstelle für die Bearbeitung der Passagierdaten («Passenger Information Unit PIU») beim Bundesamt für Polizei fedpol. Entsprechend der organisatorischen Eingliederung der PIU in die Bundesverwaltung ist diese neue Einrichtung auch mehrheitlich durch den Bund zu ressourcieren. Eine hälftige personelle Beteiligung der Kantone an der neuen Bundesstelle lehnen wir ab. Zumal der erläuternde Bericht (Seite 46) bloss rudimentäre Hinweise zu den finanziellen Auswirkungen auf die Kantone enthält. Aufgrund der jetzigen Angaben kann der einzelne Kanton kaum abschätzen, welche Kosten auf ihn zukommen werden. Die Angaben zu den finanziellen Konsequenzen für die Kantone müssen entsprechend ergänzt und konkretisiert werden.

¹ Passenger Name Record (Flugpassagierdatensatz)

B. Bemerkungen zu einzelnen Bestimmungen des Gesetzesentwurfs

Artikel 4 verpflichtet die Luftverkehrsunternehmen lediglich, die rechtzeitige Übermittlung der Flugpassagierdaten zu gewährleisten und den Eintrag unplausibler Namen zu verunmöglichen². Nach wie vor ist es aber möglich, einen Flug mit falschen Namensangaben zu buchen. Wir sind der Meinung, die Flugverkehrsunternehmen müssten mindestens gewährleisten können, dass beim Boarding – wo ohnehin eine Ausweiskontrolle stattfindet – der bei der Buchung angegebene Name zu überprüfen ist. Andernfalls bringt der Datenabgleich mit Fahndungssystemen gemäss Artikel 7 nichts.

Artikel 6: Die «Strafverfolgungsbehörden», also auch die kantonalen Polizeikorps, können nach Artikel 11 Anfragen zu Flugpassagierdaten an die PIU richten, die in der Vergangenheit liegen. Mit Blick auf den Grundsatz von Absatz 1 erscheint wichtig sicherzustellen, dass diese Daten auch zur Zielfahndung nach verurteilten Straftätern benutzt werden dürfen. Also etwa dazu, eine Fluchroute nachzuverfolgen, um später ein Auslieferungersuchen an den Aufenthaltsstaat richten zu können.

Absatz 3 Buchstaben a und b: Es ist nicht nachvollziehbar, weshalb «schwere Straftaten» unterschiedlich eingestuft werden, je nachdem, ob sie von den regulären Strafuntersuchungsbehörden oder vom Bundesamt für Zoll und Grenzsicherheit verfolgt werden. Eine Gleichsetzung der «schweren Straftat» mit Vergehen oder Verbrechen wäre praktikabler und zielführender, gegebenenfalls wie nach Absatz 3 Buchstabe b beschränkt auf Straftaten mit einer maximalen Freiheitsstrafe von drei Jahren. Die qualifizierenden Merkmale einer Straftat – namentlich beim Betäubungsmittelhandel, beim Menschenschmuggel oder beim Waffenhandel – sind insbesondere zu Beginn einer Strafuntersuchung schwer nachzuweisen. Anders als etwa im Bereich der aktiven geheimen Überwachungsmassnahmen (etwa einer Telefonüberwachung nach Artikel 269 StPO) handelt es sich bei der Übermittlung von Passagierdaten nach Artikel 11 des Gesetzesentwurfs letztlich um eine Registerabfrage mit weitaus geringerer Eingriffswirkung als bei einer aktiven Überwachung. Eine solche Registerabfrage lässt sich mit einer rückwirkenden Erhebung von Telekommunikationsdaten vergleichen, die auch bei Drittpersonen möglich ist (Artikel 273 StPO). Für diese Datenerhebung genügt der Verdacht auf ein Vergehen.

Artikel 8 Absatz 1 setzt «das bestätigte Vorliegen einer Straftat» nach Artikel 6 Absatz 2 und 3 voraus, damit Daten von der PIU an die Strafverfolgungsbehörden übermittelt werden können. Aus unserer Sicht wird damit die Übermittlung zur Verhinderung oder Aufdeckung einer Straftat (wie es in Artikel 1 Absatz 1 neben der Verfolgung auch als Zweck des Flugpassagierdatengesetzes angeführt wird) nicht abgedeckt. Es sollte hier statt «soweit die Überprüfung das Vorliegen einer Straftat nach ... bestätigt hat» heissen: «soweit die Überprüfung bestätigt hat, dass die Daten der Verhinderung oder Verfolgung einer Straftat nach ... dienen».

Artikel 11: Für uns ist unverständlich, dass die Erläuterungen zu dieser Bestimmung «generische Abfragen» als nicht zulässig erklären³. Diese Bemerkung widerspricht auch den Erläuterungen zu Artikel 15, wo zur Aufhebung der Pseudonymisierung festgehalten wird, diese sei u.a. zulässig, wenn sich die Anfrage auf einen bestimmten Flug beziehe⁴. Aus unserer Sicht sollte auf den erwähnten Passus in den Erläuterungen zu Artikel 11 verzichtet werden, zumal sich diese Einschränkung nicht auf den entworfenen Gesetzeswortlaut abstützen lässt. Tatsächlich richtet sich

² Erläuternder Bericht, Seiten 21 f.

³ Erläuternder Bericht, Seite 32, erste Zeile.

⁴ Erläuternder Bericht, Seite 35, erster Aufzählungspunkt.

ein Anfangsverdacht zunächst oft gegen eine unbekannte Täterschaft. So kann sich etwa aus einer Aussage eines Informanten ergeben, dass eine tatverdächtige Person mit einem bestimmten Flug in die Schweiz eingereist sei. In diesen Fällen wird es zur Eingrenzung und zur weiteren Ermittlung der Täterschaft unumgänglich sein, Einsicht in die Passagierliste eines ganzen Flugs zu beantragen. Dasselbe kann notwendig sein, wenn etwa im Fall von Menschenhandel (Artikel 182 StGB) nur bekannt ist, dass das Opfer mit einem bestimmten Flug ausser Landes gebracht worden sein soll.

Artikel 23 Absatz 1 sieht eine Sanktionierung bei Verletzung der Pflichten vor, die in den Artikeln 2, 4 oder 5 geregelt sind. Somit wäre keine Sanktionierung möglich, wenn das Luftverkehrsunternehmen seine Pflicht missachtet, die Daten ausländischen Behörden zu melden (Artikel 3). Hingegen soll eine Verletzung der Sorgfaltspflicht im Sinn von Artikel 4 sanktionierbar sein, was an sich nicht sinnvoll ist. Die Verletzung der «Lieferpflicht» muss sanktioniert werden, nicht die Verletzung einer Sorgfaltspflicht bei der Vorbereitung der Lieferung, wenn anschliessend trotzdem geliefert wird. Eventuell handelt es sich um ein Versehen bei der Redaktion des Gesetzesentwurfs. Daher unser Vorschlag: Sanktionierung von Verletzungen des Artikels 3 anstelle des Artikels 4.

Zur Wahrung der Rechtssicherheit sollte im Gesetzeswortlaut selbst (und nicht bloss in den Erläuterungen) definiert werden, was ein schwerer Fall ist, der mit der dreifachen Summe sanktioniert werden kann. Nach den Erläuterungen fällt darunter insbesondere die wiederholte Verletzung der gesetzlichen Pflichten oder die Nichtmeldung eines gesamten Datensatzes eines Flugs oder wenn die Mehrzahl der Daten falsch geliefert wird.

C. Bemerkungen aus der Sicht des Datenschutzes

Die Aufsichtsstelle Datenschutz des Kantons Basel-Landschaft merkt zum Gesetzesentwurf Folgendes an:

1. Grundsätzliches

Am 21. Juni 2022 fällte der Europäische Gerichtshof (EuGH)⁵ ein Urteil zur Vereinbarkeit gewisser Bestimmungen der «EU-Richtlinie über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (PHN-Richtlinie)»⁶ mit dem Unionsrecht, insbesondere mit den Artikeln 7, 8 und 52 der EU-Charta der Grundrechte. Nach dem EuGH kann die PHN-Richtlinie prinzipiell grundrechtskonform ausgelegt werden und ist nicht direkt ungültig zu erklären. Allerdings erachtet der EuGH die Daten-Aufbewahrungsdauer von 5 Jahren⁷ als unverhältnismässig lang.

Im Flugpassagierdatengesetz soll nach dem erläuternden Bericht⁸ die Erhebung und Nutzung der PNR-Daten so geregelt werden, dass sie dem Datenschutz und der Datenbearbeitung der PNR-Richtlinie entspricht. Das ist zu begrüessen. Folglich müssen nun die einschlägigen Bestimmungen des Gesetzesentwurfs an das EuGH-Urteil angepasst werden. Handlungsbedarf besteht namentlich bei der Zweckbindung, der Aufbewahrungsdauer, der hinreichend präzisen Bezeichnung der Daten, der klaren Bezeichnung der Datenbanken, mit denen die Daten abzugleichen sind, so-

⁵ Rechtssache C-817/19

⁶ Nr. 2016/681

⁷ Artikel 12 Absatz 1 PNR-Richtlinie

⁸ Seite 8

wie beim Gebot der diskriminierungsfreien Datenauswertung mit Hilfe von Algorithmen. Den Medien war zu entnehmen, dass der Bundesrat den Handlungsbedarf anerkennt und eine weitere Vernehmlassung zum angepassten Gesetzesentwurf plant. Aus diesem Grund äussern wir uns nachfolgend lediglich zu Bestimmungen des Gesetzesentwurfs, die keinen Konnex zum EuGH-Urteil haben.

2. Anmerkungen zu einzelnen / fehlenden Bestimmungen des Gesetzesentwurfs

Artikel 9: Während der Abgleich mit Daten aus polizeilichen Informationssystemen unmittelbar nach Erhalt der Daten von den Luftverkehrsunternehmen erfolgen muss (Artikel 7 Absatz 2) und automatisch erzielte Übereinstimmungen vor ihrer Übermittlung an die zuständige Behörde manuell auf ihre Plausibilität hin zu überprüfen sind (Artikel 7 Absatz 3), fehlen entsprechende Vorgaben für den Datenabgleich mit den von der «Passenger Information Unit PIU» erstellten Risikoprofilen und Beobachtungslisten. Auch dieser Abgleich müsste unmittelbar nach Erhalt der Daten erfolgen und kann nicht nach Belieben der PIU wiederholt werden, solange die Daten nicht pseudonymisiert wurden. Zudem sind auch hier Treffer zu plausibilisieren, bevor die Daten an andere Behörden übermittelt werden, damit Betroffene nicht zu Unrecht in Verdacht geraten. Diese Schranken sind im Gesetz zu statuieren und nicht an den Bundesrat zur Regelung auf Verordnungsstufe zu delegieren.

Artikel 13 regelt hinsichtlich der technischen und organisatorischen Massnahmen zum Schutz der Flugpassagierdaten lediglich – aber immerhin – die Zugriffsrechte auf die Daten im Informationssystem Passenger-Name-Record (PNR-System). Zudem ist vorgeschrieben, dass die Daten nach sechs Monaten automatisch pseudonymisiert werden. Mit Blick auf die Datenmenge und das Missbrauchspotenzial muss der Bundesrat weitere Anforderungen an die Datensicherheit festlegen.

Artikel 18 Absatz 2: Es ist nicht ganz nachvollziehbar, warum die pseudonymisierten Daten vom Auskunftsrecht bzw. vom Recht auf Zugang zu den eigenen Personendaten ausgeschlossen sein sollen. Die Daten sind de-pseudonymisierbar und in aller Regel dürften keine Gründe vorliegen, die für eine Einschränkung des Rechts z.B. aufgrund überwiegender öffentlicher Interessen (bspw. Gefährdung einer Ermittlung) sprechen könnten. Zumal es sich um die Daten von Personen handelt, bei denen kein Verdacht auf terroristische Tätigkeiten oder Beteiligung an einer schweren Straftat besteht.

Nach **Artikel 20 Absatz 3** darf das Personal der «Passenger Information Unit PIU» beim Einsatz erhobene Informationen nur zur Erfüllung der PIU-Aufgaben verwenden; laut dem erläuternden Bericht⁹ wird damit die Pflicht zur Verschwiegenheit statuiert. Allerdings betont der Gesetzeswortlaut eher den datenschutzrechtlichen Grundsatz der Zweckbindung und keine Geheimhaltungspflicht. Gerade wenn die Verschwiegenheitspflicht auch gegenüber dem vertraglichen Arbeitgeber der PIU-Mitarbeitenden gelten soll, wäre es sinnvoll, dies unmissverständlich im Gesetz festzuhalten.

Artikel 22 Absatz 3 regelt die Ausnahme von der Pflicht zu Amtshilfe gemäss Absatz 2. Da aber nach Absatz 2 ein begründeter Antrag vorliegen muss, und die anfragende ausländische Stelle mit den gleichen Aufgaben betraut sein muss wie die PIU, liefe diese Bestimmung auf eine materielle Überprüfung des «begründeten Verdachts» hinaus. Dies sollte nach unserem Verständnis die Aufgabe der ersuchenden Stelle sein.

⁹ Seite 39

Abschliessend bedanken wir uns nochmals für die Möglichkeit zur Meinungsäusserung sowie für eine wohlwollende Prüfung unserer Anliegen.

Hochachtungsvoll



Kathrin Schweizer
Regierungspräsidentin



Elisabeth Heer Dietrich
Landschreiberin

Kanton Schaffhausen
Regierungsrat
Beckenstube 7
CH-8200 Schaffhausen
www.sh.ch

T +41 52 632 71 11
F +41 52 632 72 00
staatskanzlei@sh.ch



Regierungsrat

Eidg. Justiz- und
Polizeidepartement EJPD

per E-Mail: kd-rechtsabtei-
lung@fedpol.admin.ch

Schaffhausen, 5. Juli 2022

Vernehmlassung EJPD betreffend Entwurf eines Bundesgesetzes über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten; Stellungnahme

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Am 13. April 2022 hat das Eidgenössische Justiz- und Polizeidepartement EJPD die Kantone eingeladen, zu einem Entwurf betreffend Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten Stellung zu nehmen. Wir danken Ihnen für diese Gelegenheit.

Der Kanton Schaffhausen begrüsst den Entwurf des Bundesgesetzes über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten. Insbesondere der automatisierte Abgleich der Flugpassagierdaten mit den Daten aus polizeilichen Informationssystemen gemäss Art. 8 FPG erachten wir als erfolgsversprechend.

Das vorgesehene Entsendemodell, wonach sich die PIU je hälftig aus Mitarbeitenden des Bundes und der Kantone zusammensetzen sollen, unterstützen wir gerne, die Kosten sollen jedoch vollumfänglich vom Bund übernommen werden.

Aus datenschutzrechtlicher Sicht stellt sich die Frage der Zuständigkeit für die datenschutzrechtliche Aufsicht (EDÖB oder kantonaler DSB), welche soweit ersichtlich weder in der Vorlage noch in den Erläuterungen geregelt bzw. erwähnt wird. Zu begrüßen ist, aber nicht als ausreichend erachten wir sodann die rein interne Aufsicht durch die Datenschutzstelle von FedPol, da FedPol

selbst polizeiliche Ermittlungen durchführt. Ergänzend regen wir daher an zu prüfen, ob eine unabhängige Aufsicht über die Tätigkeit der PIU vorgesehen werden könnte. Gesetzlich geregelt werden sollte sodann die weitere Verwendung der einmal gestützt auf Art. 8 FPG bekannt gegebenen Personendaten. Sodann stellt sich die Frage, ob die in Art. 15 FPG vorgesehene Pseudonymisierung sachdienlich ist. Stattdessen sollten die Lösungsfristen besser so kurz wie möglich gehalten und formell gesetzlich verankert werden. Schliesslich regen wir an ergänzend festzuhalten, dass die PIU-Daten lediglich an Staaten bekannt geben können sollen, welche ein angemessenes Datenschutzniveau gemäss Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten gewährleisten.

Wir danken Ihnen für die Kenntnisnahme und Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

Im Namen des Regierungsrates



Die Präsidentin:

A handwritten signature in blue ink, reading "C. Stamm Hurter".

Dr. Cornelia Stamm Hurter

Der Staatsschreiber:

A handwritten signature in blue ink, reading "Bilger".

Dr. Stefan Bilger



Regierungsrat, 9102 Herisau

Eidg. Justiz- und Polizeidepartement EJPD

per E-Mail: kd-rechtsabteilung@fedpol.admin.ch

[PDF- und Wordversion]

Herisau, 1. Juli 2022

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

Eidg. Vernehmlassung; Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG); Stellungnahme des Regierungsrates von Appenzel Ausserrhoden

Sehr geehrte Damen und Herren

Mit Schreiben vom 13. April 2022 wurden die Kantonsregierungen vom Eidgenössischen Justiz- und Polizeidepartement (EJPD) eingeladen, zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten bis zum 31. Juli 2022 Stellung zu nehmen.

Der Regierungsrat von Appenzel Ausserrhoden nimmt dazu wie folgt Stellung:

Er begrüsst die vorgesehene Einführung der systematischen Bearbeitung von Flugpassagierdaten zur Unterstützung der Verhinderung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten. Es ist aus Sicht des Regierungsrates richtig, hierzu ein neues Gesetz zu schaffen. Des Weiteren wird die Gesetzesvorlage in Bezug auf die technologieneutrale Formulierung befürwortet, womit auf künftige technologische Entwicklungen ohne Gesetzesrevision reagiert werden kann. Der Regierungsrat begrüsst die vorgesehene organisatorische Ansiedlung der "Passenger Information Unit" (PIU) beim Bund (Bundesamt für Polizei, fedpol). Hierbei wird das vorgesehene Entsendemodell, wonach sich die PIU je hälftig aus Mitarbeitenden des Bundes und der Kantone zusammensetzt, grundsätzlich unterstützt. Es erlaubt einen Kompetenztransfer von der PIU in die Kantone, welcher insbesondere für das Konzipieren von Risikoprofilen und Beobachtungslisten nützlich sein kann. Der Regierungsrat spricht sich jedoch dafür aus, dass die Kosten für die Mitarbeitenden vollumfänglich vom Bund übernommen werden, analog den Zentren für Polizei- und Zollzusammenarbeit (CCPD) in Genf und Chiasso. Nur so ist es insbesondere den kleineren Kantonen bzw. der Polizei möglich, Personal für diese Bundesaufgaben entsenden zu können. Art. 20 Abs. 4 FPG ist entsprechend anzupassen.



Wir danken Ihnen für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse

Im Auftrag des Regierungsrates

Dr. iur. Roger Nobs, Ratschreiber



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
kd-rechtsabteilung@fedpol.admin.ch

Appenzell, 18. August 2022

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten Stellungnahme Kanton Appenzell I.Rh.

Sehr geehrte Damen und Herren

Wir danken Ihnen für Ihr Schreiben, mit welchem Sie uns die Vernehmlassungsunterlagen zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten zukommen liessen.

Die Standeskommission hat die Unterlagen geprüft. Sie ist mit der Vorlage grundsätzlich einverstanden.

Sie macht darauf aufmerksam, dass der Bundesrat im Rahmen der Festlegung der weiteren Rahmenbedingungen für eine Vereinbarung mit den Kantonen über die Entsendung von Mitarbeitenden und deren Einsatz bei der PIU nach Art. 20 Abs. 5 nFPG zu berücksichtigen hat, dass der Kanton Appenzell I.Rh. aufgrund der Grösse der Kantonspolizei Appenzell I.Rh. kein Personal entsenden kann. Die Standeskommission geht weiter davon aus, dass das Urteil vom 22. Juni 2022 des Europäischen Gerichtshofs in der Rechtssache C-817/19 im Rahmen der Vernehmlassung berücksichtigt wird.

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

Im Auftrage von Landammann und Standeskommission

Der Ratschreiber:



Markus Dörig

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)



Eidgenössisches Justiz- und
Polizeidepartement
Bundeshaus West
3003 Bern

Regierung des Kantons St.Gallen
Regierungsgebäude
9001 St.Gallen
T +41 58 229 74 44
info.sk@sg.ch

St.Gallen, 1. September 2022

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten; Vernehmlassungsantwort

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 20. Juni 2022 laden Sie uns zur Vernehmlassung zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (abgekürzt FPG) ein. Wir danken für die Verlängerung der Vernehmlassungsfrist bis am 1. September 2022.

Wir danken für diese Gelegenheit und teilen Ihnen mit, dass wir die Vorlage begrüssen und grundsätzlich mit dieser einverstanden sind.

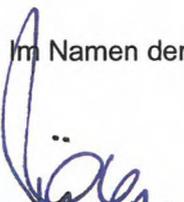
Im Hinblick auf den Datenabgleich mit Risikoprofilen und Beobachtungslisten (Art. 9 FPG) regen wir an, zu überprüfen, ob auch dort eine Plausibilitätsprüfung wie in Art. 7 Abs. 3 FPG durchgeführt werden könnte, bevor die entsprechenden Daten an die zuständigen Behörden übermittelt werden.

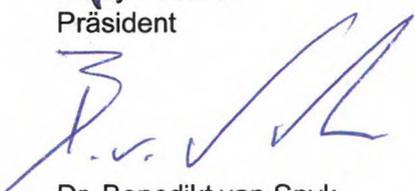
Betreffend die Aufbewahrungsfrist der gesammelten Flugpassagierdaten von sechs Monaten (Art. 14 FPG) bzw. fünf Jahren für pseudonymisierte Flugpassagierdaten (Art. 16 FPG) erlauben wir uns zudem den Hinweis auf das Urteil der grossen Kammer des Europäischen Gerichtshofes C-817/19 vom 21. Juni 2022, wonach die Flugpassagierdaten nicht generell fünf Jahre, sondern lediglich sechs Monate gespeichert werden dürfen, sofern keine Hinweise auf Terrorismus oder Schwerstkriminalität vorliegen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.



Im Namen der Regierung


Fredy Fässler
Präsident


Dr. Benedikt van Spyk
Staatssekretär



Zusätzlich per E-Mail (in PDF- und Word-Format) an:
kd-rechtsabteilung@fedpol.admin.ch



Sitzung vom

21. Juni 2022

Mitgeteilt den

23. Juni 2022

Protokoll Nr.

547/2022

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundeshaus West
3003 Bern

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

kd-rechtsabteilung@fedpol.admin.ch

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 13. April 2022 erhalten die Kantone Gelegenheit, sich zum erwähnten Geschäft zu äussern. Dafür danken wir Ihnen bestens. Wir erlauben uns jedoch den Hinweis, dass das Schreiben bei der Standeskanzlei des Kantons Graubünden nicht angekommen ist.

Die uns zugesandte Dokumentation haben wir geprüft. Die Regierung begrüsst grundsätzlich die Vorlage zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG) und die Regelung in einem eigenen Gesetz. Bezüglich Ausgestaltung derselben befürworten wir insbesondere die in der Vorlage gewählte technologieneutrale Formulierung. Mit dieser kann bei künftigen technologischen Entwicklungen auch ohne die Notwendigkeit einer Gesetzesrevision rasch reagiert werden. Die in Art. 2 Abs. 4 FPG festgelegte Zuordnung der Festlegung der

technischen Einzelheiten der Übermittlung an das Bundesamt für Polizei (fedpol) ist richtig.

Die in der Vorlage vorgesehene organisatorische Ansiedlung der Passenger Information Unit (PIU) beim Bund erachten wir als sachgerecht. Grundsätzlich sind wir auch mit dem Entsendemodell einverstanden, wonach sich die PIU je hälftig aus Mitarbeitenden des Bundes und der Kantone zusammensetzt. Die Kosten sind jedoch vollumfänglich vom Bund zu übernehmen, da es sich um eine Aufgabe in nationalem Interesse gestützt auf Bundesgesetzgebung handelt. Art. 20 Abs. 4 FPG ist entsprechend anzupassen.

Als Kontaktperson für Rückfragen steht Ihnen Herr Rechtsanwalt lic. iur. Gianni Scandella, juristischer Mitarbeiter, Departement für Justiz, Sicherheit und Gesundheit, zur Verfügung (081 257 25 15; gianni.scandella@djsq.gr.ch).

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



Namens der Regierung

Der Präsident:

Marcus Caduff

Der Kanzleidirektor:

Daniel Spadin

REGIERUNGSRAT

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

A-Post Plus
Bundesamt für Polizei
Guisanplatz 1A
3003 Bern

10. August 2022

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten; Vernehmlassung

Sehr geehrte Damen und Herren

Mit Schreiben vom 20. Juni 2022 haben Sie die Kantonsregierungen zur Vernehmlassung des oben genannten Geschäfts eingeladen. Wir bedanken uns für diese Gelegenheit und äussern uns wie folgt:

1. Grundsätzliches

Die Möglichkeit, Flugpassagierdaten im Zusammenhang mit terroristischen und anderen schweren Straftaten bearbeiten und analysieren zu können, ist ein wichtiges Mittel für die Bekämpfung solcher Straftaten. Es ist angezeigt, hier die entsprechenden gesetzlichen Grundlagen zu schaffen. Die Wirksamkeit der Nutzung von Flugpassagierdaten ist dann gegeben, wenn die Verarbeitung angesichts der Datenmenge und der Zeitverhältnisse automatisiert erfolgen kann, was der Fall ist, wenn die inländischen und ausländischen Daten standardisiert sind. Der Vorentwurf des Bundesgesetzes über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG) folgt der international üblichen Standardisierung. Der Regierungsrat begrüsst den vorliegenden Entwurf.

2. Kommentare zu einzelnen Paragraphen

2.1 Art. 1 lit. a und Art. 6 Abs. 1 E-FPG

Passagierdaten dürfen gemäss Wortlaut von Art. 1 lit. a und Art. 6 Abs. 1 E-FPG zur Verhinderung, Aufdeckung, Ermittlung und Verfolgung von Terrorismus und schweren Straftaten gemäss Delikt-katalog bearbeitet werden. Passagierdaten müssen aber für die Fahndung nach rechtskräftig verurteilten, flüchtigen Personen auch ausserhalb von Strafverfahren bearbeitet werden können. Die Bearbeitung von Daten von rechtskräftig verurteilten, flüchtigen Personen soll explizit im Gesetzestext genannt werden.

2.2 Anhang 1 E-FPG

Gemäss Art. 1 lit. a E-FPG sind im Anhang 1 E-FPG die Flugpassagierdaten, welche bearbeitet und analysiert werden dürfen, abschliessend aufgelistet. Biometrische Daten sind im Anhang 1 E-FPG nicht erwähnt. Gerade biometrische Daten, sofern erfasst und vorhanden, können bei der Verhinderung, Aufdeckung, Ermittlung und Verfolgung von Terrorismus und schweren Straftaten gemäss Deliktecatalog von grosser Relevanz sein. Die biometrischen Daten sollten demnach in die Liste im Anhang 1 E-FPG aufgenommen werden.

2.3 Art. 6 Abs. 3 lit. b E-FPG

Die vorliegende Formulierung "*maximale Freiheitsstrafe von mindestens drei Jahren*" ist interpretationsbedürftig. Es wird vermutet, dass damit Strafbestimmungen gemeint sind, deren oberer Strafrahmen gleich oder grösser drei Jahre beträgt. Die Formulierung wie auch die Erläuterungen sollten präzisiert werden.

2.4 Art. 20 Abs. 1 E-FPG

Der E-FPG sieht vor, dass das Personal der Passenger Information Unit (PIU) je hälftig aus Mitarbeitenden des Bundes und Mitarbeitenden der Kantone bestehen wird. Wir begrüssen diesen Ansatz sehr, da somit ein Wissenstransfer in die Kantone gewährleistet wird.

3. Operabilität PIU

Im Bereich der Bekämpfung von Terrorismus und schweren Straftaten gemäss Deliktecatalog ist der zeitlich unmittelbare Informationsaustausch zwingend. Informationen müssen zwingend 24/7 ausgetauscht, bearbeitet und analysiert werden können. Die ständige Operabilität der PIU ist deshalb 24/7 sicherzustellen.

Wir danken Ihnen für die Berücksichtigung unserer Vernehmlassung.

Freundliche Grüsse

Im Namen des Regierungsrats

Alex Hürzeler
Landammann

Joana Filippi
Staatsschreiberin

Kopie
kd-rechtsabteilung@fedpol.admin.ch

Staatskanzlei, Regierungsgebäude, 8510 Frauenfeld

Eidgenössisches
Justiz- und Polizeidepartement (EJPD)
Frau Karin Keller-Sutter
Bundesrätin
Bundeshaus West
3003 Bern

Frauenfeld, 5. Juli 2022

415

Entwurf für ein Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten

Vernehmlassung

Sehr geehrte Frau Bundesrätin

Wir danken Ihnen für die Möglichkeit zur Stellungnahme zum Entwurf für ein Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG) und teilen Ihnen mit, dass wir mit der Vorlage grundsätzlich einverstanden sind. Wir befürworten auch die im Entwurf vorgesehene organisatorische Ansiedlung der Passenger Information Unit (PIU) beim Bund und unterstützen das vorgesehene Entsendemodell, wonach sich die PIU je hälftig aus Mitarbeitenden des Bundes und der Kantone zusammensetzt. Entsprechend der Regelung von Art. 11 der Vereinbarung über den nationalen Betrieb gemeinsamer Polizei- und Zollkooperationszentren (CCPD) in Genf und Chiasso (SR 360.4) sind die Kosten jedoch vollumfänglich vom Bund zu übernehmen. Nur dies ermöglicht es den Kantonen, Personal für diese Bundesaufgabe abgeben zu können. Art. 20 Abs. 4 FPG ist in diesem Sinne anzupassen.

Mit freundlichen Grüssen

Die Präsidentin des Regierungsrates



Der Staatsschreiber



Il Consiglio di Stato

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

*Invio per posta elettronica (word e pdf):
kd-rechtsabteilung@fedpol.admin.ch*

Procedura di consultazione concernente la Legge federale sul trattamento dei dati dei passeggeri aerei per la lotta ai reati terroristici e ad altri reati gravi

Gentili signore,
egregi signori,

abbiamo ricevuto la vostra lettera in merito alla summenzionata procedura di consultazione. Le modifiche di legge, unitamente al relativo rapporto esplicativo sull'introduzione della nuova Legge federale sul trattamento dei dati dei passeggeri aerei per la lotta ai reati terroristici e ad altri reati gravi, sono stati da noi esaminati in collaborazione con il Ministero pubblico e i servizi di polizia interessati.

Ringraziando per l'opportunità che ci viene offerta di esprimere il nostro giudizio formuliamo le seguenti osservazioni.

In generale, come Esecutivo cantonale accogliamo favorevolmente la proposta di novella legislativa in oggetto, inerente all'adozione della nuova legge federale sul trattamento dei dati dei passeggeri aerei per la lotta ai reati terroristici e ad altri reati gravi, che permetterà alla Svizzera di utilizzare il set di dati conosciuto come Passenger Name Record (PNR). In effetti, con le nuove basi legali a disposizione all'interno del diritto federale, la Confederazione sarà autorizzata a trattare in modo sistematico i dati dei passeggeri aerei, consentendole così di sostenere le autorità federali e cantonali nella prevenzione, nell'investigazione e nel perseguimento dei reati terroristici e di altri reati gravi.

Anche per le Autorità di polizia il progetto legislativo rappresenta senz'altro un mezzo importante per contrastare le attività criminali, ritenuto come lo stesso permetterà di prevenire in maniera ancora più efficiente la criminalità e il terrorismo, combattendoli con maggior efficacia. Mettendo a disposizione dei Cantoni il sistema informativo PNR, la Confederazione fornisce infatti gli strumenti necessari per consentire alle autorità giudiziarie cantonali di accedere più facilmente e più rapidamente alle informazioni che semplificano la prevenzione e la lotta contro i reati gravi.

RG n. 3426 del 6 luglio 2022

Particolarmente apprezzata, inoltre, la formulazione del progetto di legge neutrale dal punto di vista tecnologico, la quale permetterà di reagire tempestivamente agli sviluppi tecnologici futuri senza dover procedere ogni volta con la revisione della relativa legge. A questo proposito, si approva quanto stabilito dall'art. 2 cpv. 4 del progetto di Legge, secondo cui spetta a fedpol definire le modalità tecniche relative alla trasmissione dei dati.

Premesso ciò, le Autorità di polizia nutrono tuttavia delle perplessità in merito ad alcuni aspetti legati al personale previsto per l'UIP: l'art. 20 del progetto di Legge prevede infatti che i Cantoni debbano contribuire ai costi dell'UIP, distaccando alcuni dei propri collaboratori e assumendosi altresì i costi di questo distacco. Stando a quanto indicato dalla Confederazione, si prevede inizialmente per l'UIP l'assunzione di 20 collaboratori a tempo pieno, passando successivamente a un totale di 30 unità. Metà di questi collaboratori saranno retribuiti dalla Confederazione, mentre l'altra metà dai singoli Cantoni. La chiave di ripartizione scelta dalla Confederazione appare discutibile, poiché comporta un onere eccessivo per i Cantoni. Infatti, il Canton Ticino dovrà prevedere il distacco dapprima di 1 unità e poi di 1.5, assegnati all'UIP. Ciò costituisce un carico finanziario non indifferente per il Cantone, ritenuto come il personale distaccato sarà principalmente destinato a svolgere i compiti previsti dall'UIP e non a rispondere alle necessità cantonali, gravando così sul servizio che metterà le unità a disposizione.

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

PER IL CONSIGLIO DI STATO

Il Presidente

Claudio Zali

Il Cancelliere

Arnaldo Coduri

Copia a:

- Consiglio di Stato (decs-dir@ti.ch; dfe-dir@ti.ch; di-dir@ti.ch; dss-dir@ti.ch; dt-dir@ti.ch; can-sc@ti.ch)
- Segreteria generale del Dipartimento delle istituzioni (di-sg.ap@ti.ch)
- Comando della Polizia cantonale (polizia-segr@polca.ti.ch)
- Divisione della giustizia (di-dg.portali@ti.ch)
- Deputazione ticinese alle Camere federali (can-relazioniesterne@ti.ch)
- Pubblicazione in Internet

Madame la Conseillère fédérale
Karine Keller-Sutter
Cheffe du Département fédéral de justice
et police
Palais fédéral ouest
3003 Berne

Réf. : 22_GOV_402

Lausanne, le 29 juin 2022

Consultation fédérale - Loi fédérale sur le traitement des données relatives aux passagers aériens pour la lutte contre les infractions terroristes et les autres infractions pénales graves

Madame la Conseillère fédérale,

Le Conseil d'Etat vaudois vous remercie de l'avoir associé à la consultation citée en titre, à laquelle il répond par la présente.

En introduction, il est constaté que le projet de loi susmentionné a pour but de régir l'ensemble du traitement des données relatives aux passagers aériens pour lutter contre les infractions terroristes et les autres infractions pénales graves ; offrant ainsi un maximum de transparence et de cohérence à cette démarche. Ce projet de loi est salué étant donné qu'il définit, pour la Suisse, une interface unique pour la mise en place du système regroupant l'ensemble des données sur les passagers, nécessaire à la réservation et à l'enregistrement d'un vol (PNR). Cette loi renforce dès lors la collaboration entre la Confédération et les pays étrangers, ainsi qu'entre les autorités de la Confédération et des cantons, ce que le Canton de Vaud soutient.

Concernant les coûts se rapportant à l'introduction du PNR en Suisse, la Confédération a déterminé que l'effectif nécessaire au fonctionnement du système s'élevait au départ à 20 équivalents plein temps (ETP) puis à 30 ETP. Cela étant, vos services estiment que les données PNR permettront également aux autorités cantonales de poursuite pénale de recevoir des informations sur des personnes recherchées au niveau national ou international qui arrivent en Suisse ou qui viennent de quitter le pays par voie aérienne. La Confédération envisage dès lors la prise en charge des coûts par moitié par la Confédération et par moitié par les cantons. Ainsi, la contribution des cantons devrait s'effectuer par le détachement au sein du nouveau service de collaborateurs dont les coûts relatifs à l'engagement sera pris en charge par les cantons. Cette clé de répartition choisie par la Confédération est très discutable et fait peser des coûts importants sur les cantons, ce qui n'est pas équitable en raison du fait que les infractions concernées relèvent de la compétence de la Confédération. En effet, après estimation, le Canton de Vaud serait dans l'obligation d'engager 1 puis 1,5 ETP afin de répondre à cette exigence fédérale. Cette charge financière est lourde pour le Canton de Vaud, le rôle des collaborateurs détachés devant également être clarifié quant à leur mission principale qui doit être de répondre aux sollicitations cantonales et non d'être principalement affectés à

remplir les missions de compétence fédérale. Il s'ensuit que la clé de répartition doit être revue afin que les cantons aient à supporter moins que la moitié des frais.

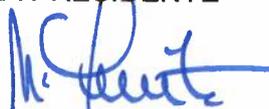
Pour le surplus, il convient de relever que les articles 8 et 11 P-LDPa mentionnent les autorités de poursuite pénale de la Confédération ou des cantons ou du Service de renseignement de la Confédération (SRC) mais ne citent pas les services de renseignement cantonaux (SRCa). Or, selon la loi fédérale sur le renseignement du 25 septembre 2015, si le SRC peut recevoir les informations de Passenger Information Unit (UIP), les SRCa devraient également pouvoir en bénéficier. Le Conseil d'Etat souhaite donc que les art. 8 al. 2 let. b) et 11 al. 1 let. b) P-LDPa soient complétés de manière à ce que les services de renseignement des cantons soient ajoutés en sus du Service de renseignement de la Confédération. En effet, si cet ajout n'est pas inséré dans la loi, les SRCa seront dans l'obligation de faire des demandes auprès du SRC produisant ainsi des lenteurs et des complications de procédure pour les autorités cantonales.

En définitive, le Conseil d'Etat est favorable au projet de loi établi par la Confédération, qui permettra aux autorités de la Confédération et des cantons d'être encore plus efficaces dans la lutte contre les infractions terroristes et les autres infractions pénales graves.

Nous vous prions de croire, Madame la Conseillère fédérale, à l'expression de notre très haute considération.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE



Nuria Gorrite

LE CHANCELIER



Aurélien Buffat

Copies

- OAE
- Police cantonale vaudoise



CONSEIL D'ETAT
DU CANTON
DE VAUD

1014 Lausanne

01.07.22

CH - 1300
Affr. Poste
2090058
30001733

1.10



A
STANDARD
LA POSTE

Eidg. Justiz- und
Polizeidepartement.

- 4. Juli 2022

No. fedpol

Madame la Conseillère fédérale
Karine Keller-Sutter
Cheffe du Département fédéral de justice et
police
Palais fédéral ouest
3003 Berne





2022.03300

P.P. CH-1951
Sion

A-PRIORITY Poste CH SA

Département fédéral de justice et police
Madame Karin Keller-Sutter
Conseillère fédérale
Bundesplatz 3
3003 Berne



Notre réf. *60
Votre réf. /

Date 10 AOUT 2022

Loi fédérale sur le traitement des données relatives aux passagers aériens pour la lutte contre les infractions terroristes et les autres infractions pénales graves : ouverture de la procédure de consultation

Madame la Conseillère fédérale,

Le Conseil d'Etat du canton du Valais fait suite à votre correspondance du 13 avril 2022 et vous remercie de l'avoir associé à la consultation précitée.

Sur le plan sécuritaire, nous saluons ce projet de loi qui permettra de traiter les données collectées lors de la réservation et de l'enregistrement des vols dans le but de lutter contre les infractions terroristes et autres infractions pénales graves.

Toutefois, les données seront traitées par l'Unité d'information passagers (UIP), rattachée à Fedpol, qui emploiera 30 EPT. La moitié des collaborateurs seront détachés par les cantons. A ce sujet, nous nous permettons de soulever les problématiques financières liées aux coûts générés pour notre canton par le détachement d'un collaborateur et la prise en charge de son indemnisation. De plus, l'intégration des données Passenger Name Record (PNR) à notre Corps de police impliquera également l'augmentation des ressources internes. Pour le surplus, nous n'avons pas d'observations particulières à faire valoir.

Nous vous prions d'agréer, Madame la Conseillère fédérale, l'assurance de notre considération distinguée.

Au nom du Conseil d'Etat

Le président


Roberto Schmidt



Le chancelier


Philipp Spörri

Copie à M. Christian Varone, Commandant de la Police cantonale
kd-rechtsabteilung@fedpol.admin.ch



LE CONSEIL D'ÉTAT

DE LA RÉPUBLIQUE ET
CANTON DE NEUCHÂTEL

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

Consultation portant sur la loi fédérale sur le traitement des données relatives aux passagers aériens pour la lutte contre les infractions terroristes et autres infractions graves (Loi sur les données relatives aux passagers aériens, LDPa)

Madame la conseillère fédérale,

Avec l'importante réserve mentionnée ci-après, le Canton de Neuchâtel salue le présent projet qui permettra à la Suisse de traiter les données relatives aux passagers aériens (PNR) afin que les autorités fédérales et cantonales puissent plus aisément prévenir les infractions terroristes et les autres infractions pénales graves.

Ceci étant dit, nous avons néanmoins quelques remarques s'agissant de l'organisation de l'Unité d'informations passagers (UIP).

D'abord, il est prévu le détachement de collaborateurs et collaboratrices venant de la Confédération et des cantons pour une durée déterminée, à l'image de ce qui se fait déjà actuellement pour le Centre de coopération policière et douanière de Genève et Chiasso (CCPD). Or, ce procédé aura des incidences en personnel pour les cantons qui ne peuvent être évaluées à ce jour. En effet, ces éléments seront traités à futur dans l'ordonnance de la loi et la convention passée entre la Confédération et les cantons. Aussi, nous espérons que cette répartition prendra en considération l'utilisation réelle de l'UIP par les autorités cantonales. Certains cantons, comme Neuchâtel, mènent peu souvent des affaires à caractère international en comparaison à d'autres. Aussi, il serait souhaitable que la répartition entre les cantons puisse tenir compte de l'utilisation concrète de ce nouvel outil.

Ensuite, s'agissant de la durée temporaire du détachement, il conviendrait qu'elle soit suffisamment longue pour permettre au personnel d'acquérir l'expérience requise de spécialistes. Il nous semble, en effet, qu'un détachement limité à seulement une année, comme c'est le cas pour les CCPD, soit peu judicieux si l'on considère le temps nécessaire pour développer les connaissances et les sensibilités propres aux analyses des profils de risque, par exemple.

NE

Finalement, s'agissant de la composition de l'UIP, il nous apparaît particulièrement important qu'elle représente toutes les entités utilisatrices concernées : Service de renseignement, Office fédéral de la douane et de la sécurité aux frontières, fedpol et polices cantonales.

À toutes fins utiles, et comme demandé, la cheffe du secteur juridique de la police neuchâteloise se tient à votre entière disposition : Mme Marika Raimondo, 032/ 889 90 50, marika.raimondo@ne.ch.

Tout en vous remerciant de nous avoir associés à la présente procédure de consultation, nous vous prions de croire, Madame la conseillère fédérale, à l'assurance de notre haute considération.

Neuchâtel, le 17 août 2022



Au nom du Conseil d'État :

Le président,
L. KURTH

La chancelière,
S. DESPLAND



DSPS
Case postale 3952
1211 Genève 3

Département fédéral de justice et police
Madame Karin Keller-Sutter
Conseillère fédérale

Envoyé par courriel :
Hanspeter.Dolder@fedpol.admin.ch

2947-2022

Genève, le 16 septembre 2022

Concerne : Consultation sur l'avant-projet de loi fédérale sur le traitement des données relatives aux passagers aériens pour la lutte contre les infractions terroristes et les autres infractions pénales graves

Madame la Conseillère fédérale,

Le Conseil d'Etat m'a transmis pour raison de compétence votre correspondance relative à l'objet susmentionné et vous remercie également pour le délai de réponse accordé par l'office fédéral de la police (fedpol).

Après un examen attentif de l'avant-projet de loi susmentionné, je vous informe que le canton de Genève le soutient pleinement dans la mesure où il renforcera la lutte contre le terrorisme et les autres infractions pénales graves.

Une attention particulière doit être portée, à mon sens, à la mise en place pratique des dispositifs prévus par la loi, notamment en ce qui concerne l'emplacement de l'Unité d'information passagers (ci-après : UIP), soit un nouveau service rattaché à fedpol, et aux répercussions directes sur l'activité de la police genevoise lors de l'appui dans des cas relevant d'autres cantons.

S'il ressort du rapport explicatif que la Confédération prendra en charge les coûts d'investissement et d'exploitation et que les cantons participeront pour moitié aux coûts en personnel dédié à une UIP, il n'est pas clairement défini, d'un point de vue organisationnel, s'il y aura une seule UIP centralisée (qui est prévue) ou des UIP décentralisées dans les principaux aéroports suisses.

En ce qui concerne les tâches qui pourraient être exécutées pour le compte d'autres cantons, celles-ci sont quantitativement difficiles à évaluer. Une analyse rétrospective après une année de fonctionnement ou une comparaison avec un pays qui a le même nombre de passagers aériens permettrait sans doute de déterminer le coût de fonctionnement de l'UIP, qui est fonction notamment du nombre de collaborateurs qu'elle emploiera.

L'article 6 alinéa 1 LDPa mentionne que les données PNR peuvent être traitées uniquement à des fins de prévention, de détection, d'enquête et de poursuite en matière d'infractions terroristes ou d'autres infractions pénales graves. L'ajout du domaine du renseignement

prohibé, dans ses diverses déclinaisons pénales, nous semble nécessaire dans la mesure où il s'agit également d'une tâche du Service de renseignement de la Confédération (SRC).

L'article 6 alinéa 2 LDPa comporte un renvoi à la loi sur l'échange d'informations Schengen (LEIS – RS 362. 2) pour définir les infractions terroristes n'est pas approprié, la disposition visée ne concernant que le financement du terrorisme. Un renvoi à l'annexe 1 à de l'ordonnance N – SIS (RS 362. 0) serait plus judicieux.

De plus, à la lecture de l'annexe 2 de la LDPa, il apparaît que l'espionnage politique (272 CP) et l'espionnage militaire (274 CP) ne sont pas pris en compte. Partant du principe que le chiffre 26 (espionnage industriel) mentionné dans l'annexe 2 de la LDPa couvre l'infraction d'espionnage économique (273 CP), cela représente une lacune en matière de prévention et détection du renseignement prohibé en ne couvrant qu'une partie des infractions visées dans ce cadre par le code pénal.

S'agissant de l'article 6 alinéa 3, il ne semble pas adéquat de définir les infractions graves en prévoyant qu'elles doivent être punissables d'une peine privative de liberté de plus de 3 ans (let. a) alors que les infractions douanières doivent être punissables d'au moins 3 ans (let. b). Il est proposé de l'harmoniser à 3 ans et plus de manière à englober toutes les infractions punies de 3 ans de peine privative de liberté.

Vous remerciant d'avoir consulté le canton de Genève, je vous prie de croire, Madame la Conseillère fédérale, à l'expression de ma haute considération distinguée.

Mauro Poggia



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

Département fédéral de justice et police DFJP
Madame la Conseillère fédérale
Karin Keller-Sutter
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 : kd-rechtabteilung@fedpol.admin.ch

Delémont, le 16 août 2022

Loi fédérale sur le traitement des données relatives aux passages aériens pour la lutte contre les infractions terroristes et les autres infractions pénales graves

Madame la Conseillère fédérale,
Madame, Monsieur,

Le Gouvernement de la République et Canton du Jura vous remercie de l'avoir consulté sur le projet de loi noté en titre.

Il approuve la mise en place d'un outil national permettant d'utiliser en Suisse les données PNR (Passenger Name Records) et la création d'un office central UIP (unité d'information passagers), à l'instar de ce qui se pratique déjà dans de nombreux autres pays.

Par contre, le Gouvernement conteste la clé de répartition qui prévoit que la moitié du personnel de l'UIP sera fourni par les cantons et l'autre par la Confédération. Il relève que ce projet a principalement pour but de lutter contre le terrorisme et la grande criminalité qui sont de la compétence principale des autorités de poursuite pénale fédérales, de Fedpol et du SRC. Il demande à ce qu'une répartition d'1/3 à la charge des cantons et 2/3 à la charge de la Confédération soit appliquée.

Le Gouvernement de la République et Canton du Jura vous remercie de prendre en compte le présent avis et vous présente, Madame la Conseillère fédérale, Madame, Monsieur, ses salutations les plus respectueuses.

AU NOM DU GOUVERNEMENT DE LA
RÉPUBLIQUE ET CANTON DU JURA

David Eray
Président



Jean-Baptiste Maître
Chancelier d'État

Per Mail: kd-rechtsabteilung@fedpol.admin.ch

Bern, 4. Juli 2022

Vernehmlassung: Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG)

Sehr geehrte Damen und Herren

Sie haben uns eingeladen, zur obengenannten Vernehmlassungsvorlage Stellung zu nehmen. Für diese Gelegenheit zur Meinungsäusserung danken wir Ihnen bestens.

Allgemeine Bemerkungen

Weltweit nutzen mehr als 60 Staaten das Potenzial von Flugpassagierdaten (Passenger Name Record, PNR) als Instrument zur Bekämpfung von Terrorismus und anderer Schwerstkriminalität. Dies wird auch vom UNO-Sicherheitsrat mittels dreier bindenden Resolutionen verlangt. Heute übermittelt die Schweiz schon PNR-Daten an EU-Mitgliedsstaaten, die USA, Kanada und das Vereinigte Königreich. Selber kann sie aber PNR-Daten nicht bearbeiten. Diese fehlende gesetzliche Grundlage soll mit dieser Vorlage geschaffen werden.

Die Mitte begrüsst, dass mit dem Flugpassagierdatengesetz diese Lücke geschlossen werden soll. Die Schweiz zeigt sich damit gegenüber dem restlichen Europa solidarisch, da sie keine Sicherheitslücken im Schengensystem zulassen will. Zudem ermöglicht das Flugpassagierdatengesetz den nationalen Strafverfolgungsbehörden PNR-Daten zur Bekämpfung von Terrorismus und Schwerstkriminalität im Inland zu nutzen.

Aufbau des PNR-Systems

Die Mitte favorisiert, wie das EJPD, die Nutzung des UNO PNR-Systems «goTravel» (Option 1). Es ist schon in verschiedenen Ländern im Einsatz und kann ohne grössere Anpassungen übernommen werden. Im Gegensatz zu einer Eigenentwicklung oder einem Kauf eines anderen Systems (Option 2) ist die Option «goTravel» auch deutlich günstiger.

Datenschutz

Flugpassagierdaten bestehen hauptsächlich aus Personendaten. Es ist deshalb begrüssenswert, dass die Vorlage sich schon am neuen Datenschutzgesetz orientiert, welches voraussichtlich 2023 in Kraft treten wird. Die Bearbeitung der Daten ist nur zum gesetzlichen Zweck erlaubt und bei Übereinstimmungen nach dem automatischen Abgleich ist eine manuelle Überprüfung und Plausibilisierung Pflicht. Aus Sicht der Mitte ist dadurch der Datenschutz der Reisenden ausreichend gewährleistet.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und verbleiben mit freundlichen Grüssen.

Die Mitte

Sig. Gerhard Pfister
Präsident Die Mitte Schweiz

Sig. Gianna Luzio
Generalsekretärin Die Mitte Schweiz

Eidgenössisches Justiz- und Polizeidepartement
EJPD

Bern, 15. August 2022

VL Flugpassagierdaten / MZ

Per Mail an:
kd-rechtsabteilung@fedpol.admin.ch

**Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG)
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.

FDP.Die Liberalen anerkennt die Notwendigkeit des vom Bundesrat vorgeschlagenen Flugpassagiergesetzes, welches die vorhandene Gesetzeslücke in Bezug auf die systematische Erhebung und Nutzung der heute schon gesammelten Flusspassagierdaten (Passenger Name Record - PNR) schliessen soll. Mittels des neuen Flugpassagierdatengesetz wird den Strafverfolgungsbehörden die Anwendung des international bewährten Instruments der Bearbeitung von PNR-Daten zur Bekämpfung von terroristischen und anderen schweren Straftaten, ermöglicht.

Die Gewährleistung von Sicherheit mittels einer effizienten Strafverfolgung ist für die FDP aus sicherheitspolitischer Betrachtungsweise zentral. Es braucht aber zugleich eine sorgfältige Abwägung mit Hinblick auf die persönliche Freiheit, namentlich den Datenschutz. In diesem Sinne begrüsst es die FDP ausdrücklich, dass die Vorlage gemäss Stellungnahme von Fedpol an das kürzlich ergangene Urteil des EuGHs betreffend Datensammlung und Datenspeicherung angepasst werden soll, womit der Datenschutz zusätzlich erhöht wird.

Internationaler Rechtsraum

Um im Vergleich mit den internationalen Strafverfolgungsbehörden mithalten zu können ist die Errichtung einer national legitimieren Behörde für die Bearbeitung von PNR-Daten unabdingbar, denn 62 Ländern im anglosächsischen wie aber auch europäischen Raum haben ein solches seit geraumer Zeit eingeführt und fordern punktuell bereits PNR-Daten von der Schweiz. Wohingegen die Schweiz aufgrund des Fehlens eines gesetzlich legitimierten PNR-Systems, die Daten, welche aufgrund internationaler Verpflichtungen ohnehin schon erhoben werden, nicht selbst systematisch bearbeiten darf.

Hinzu kommt die Forderung des UNO-Sicherheitsrates an ihre Mitgliedstaaten für die Errichtung einer solchen Behörde. Die europäischen Richtlinien stellen keine Weiterentwicklung des Schengen-Besitzstandes dar, aber die Flüge nach oder aus den betroffenen Ländern unterliegen schon der Pflicht zur Datenerfassung und -übermittlung. Die FDP begrüsst eine Harmonisierung der Instrumente in Anbetracht der Tatsache, dass die Schweizer Strafverfolgungsbehörden auf die Amtshilfe des Auslandes angewiesen sind.

Schlussendlich wird ein funktionierendes PNR-System für den Verbleib der Schweiz im «Visa Waiver Program» von den USA vorausgesetzt. Ein Wegfall dieser Visafreiheit für geschäftlichen wie auch touristischen Zweck würde für die Schweiz und deren Wirtschaftsstandort unhaltbare Nachteile mit sich bringen.

Schweizer Rechtsraum

Die Sammlungs- und Bearbeitungsmodalitäten auf Stufe Verordnung sollen in enger Abstimmung mit den betroffenen Flugbranchen ausgestaltet werden. Flugverkehrsunternehmen müssen infolge der neuen Gesetzgebung zeitnahe Datenübermittlungspflichten nachkommen und zeitgleich um einen reibungslosen und sicheren Flughafenbetrieb bemüht sein. Die FDP befürchtet, dass die Branchen übermässigen Bürokratieaufwand unterliegen werden, kein Mehrwert für die Sicherheit generiert wird und so der Flugalltag gestört wird. Dank dem Knowhow der Flugbranche soll aber eine technisch effiziente sowie privatsphären- und unternehmensfreundliche Form der Implementierung der Datenerfassung und -auswertung ermöglicht werden. Die zuständigen Behörden werden angehalten für die Erfüllung der gesetzlichen Pflichten kein Swiss-Finish vorzunehmen, sondern die bereits bestehenden PNR-Systeme für die Datenübermittlung zu brauchen und allenfalls auszuweiten.

Meldungsmodalitäten

Art. 12 Abs. 1 DSG schreibt der zuständigen nationalen Stelle, auch genannt Passenger Information Unit (PIU), vor, bei «konkretem» Verdacht auf eine terroristische oder andere schwere Straftat der Strafverfolgungsbehörden Meldung zu erstatten. Die FDP äussert in diesem Zusammenhang ihr Bedenken, dass die Hürde der Meldung zu hoch angesetzt wird für eine effektive präventive Strafverfolgung. Denn der FDP ist es ein wichtiges Anliegen, gezielt und schnell den Kampf gegen Terrorismus und Schwerstkriminalität voranzutreiben und die nötigen Massnahmen rechtzeitig einzuleiten. Folglich wird die Forderung gestellt, dass diese Meldung schon bei «Verdacht» vorzunehmen ist und dem Begriff «Verdacht» keine weiteren Anforderungen gestellt werden.

Zudem sind für die Verpflichtungen der PIU keine zeitlichen Angaben oder Fristen zu finden. Der Bundesrat wird angehalten in der vollziehenden Verordnung zu definieren innerhalb welcher Frist die erhobenen Daten abzugleichen und allenfalls der Strafverfolgungsbehörden die Meldung bei Verdachtsfällen zu erstatten sind. Aufgrund der zeitlichen Dringlichkeit bei Strafverfolgung insbesondere über die Landesgrenzen hinweg erweist sich ein schnelles Verfahren und eine proaktive Behörde als erforderlich. Deshalb ist der offene Begriff der Unmittelbarkeit nach Art. 7 Abs. 2 FPG nicht zufriedenstellend.

Datenschutz

Die FDP begrüsst die Informationspflicht der Luftverkehrsunternehmen gemäss Art. 5 FPG, die die Passagiere über die Sammlung und Bearbeitung ihrer PNR-Daten aufklären muss, was wesentlich zum Schutz der Persönlichkeitsrechte beiträgt. Dessen ungeachtet muss sich das PIU und die Strafverfolgungsbehörden trotzdem zwingend an das Datenschutzprinzip der Minimierung der Datensammlung und -speicherung orientieren.

Ebenfalls ist es – gerade aufgrund der grossen Mengen von PNR-Daten die primär aus Personendaten bestehen – zwingend, dass ein nachweisbarer Nutzen im Sicherheitsbereich entsteht. Weswegen nur Daten im Zusammenhang mit Terror oder Schwerstkriminalität erhoben werden dürfen, die gesetzlich auch verankert sind. Jegliche weiterführende Sammlung von persönlichen Daten, die in casu nicht weiterhelfen, stellen sich als unverhältnismässigen Aufwand für die Luftverkehrsunternehmen und eine Verletzung der Persönlichkeitsrechte der Passagiere dar.

Datenaufbewahrung

Der erläuternde Bericht (S. 35f.) führt bereits aus, dass es sich bei der Aufbewahrungsfrist von fünf Jahren für Daten (in pseudonymisierter Form gemäss Art. 16 Abs. 1 FPG) bereits um eine vergleichsweise lange Frist handelt. Die Speicherung der Daten über den üblichen Zeitraum hinaus ohne jegliche Hinweise auf eine verübte Straftat erweist sich als ein Eingriff in die Grundrechte der Passagiere, dies insbesondere, weil das persönliche Auskunftsrecht nach der Pseudonymisierung, gemäss Art. 18 Abs. 2 FPG nicht mehr wahrgenommen werden kann. Trotz der Pseudonymisierung sind die vorliegenden PNR-Daten weiterhin persönliche Daten gemäss dem Datenschutz, welches einen

besonderen Schutz unterliegt und ein persönliches Auskunftsrecht bedarf. Damit der Vorwurf einer unverhältnismässigen Vorratsdatenspeicherung nicht gemacht werden kann und kein Widerspruch gegen die europäische Rechtsprechung entsteht, sollte die Aufbewahrung der Daten entsprechend dem kürzlich veröffentlichten EuGH-Urteil angepasst werden und das Auskunftsrecht gemäss Art. 18 Abs.1 i.V.m. Art. 25-28 DSGVO beibehalten werden.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und für die Berücksichtigung unserer Überlegungen.

Freundliche Grüsse

FDP.Die Liberalen

Der Präsident



Thierry Burkart
Ständerat

Der Generalsekretär



Jon Fanzun



GRÜNE Schweiz

Waisenhausplatz 21

3011 Bern

rahel.estermann@gruene.ch

031 326 66 15

Eidgenössisches Justiz- und Sicherheitsdepartement EJPD

Frau Bundesrätin Karin Keller-Sutter
3003 Bern

per E-Mail an:

kd-rechtsabteilung@fedpol.admin.ch

Bern, 28. Juli 2022

**Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG):
Vernehmlassung**

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Sie haben die GRÜNEN eingeladen, sich zum Entwurf für das Flugpassagierdatengesetz (FPG) zu äussern. Wir danken Ihnen dafür und nehmen gerne Stellung.

Der Bundesrat hält richtigerweise fest, dass heute Flugpassagier*innendaten (Passenger Name Records, PNR) so oder so anfallen und deren Übermittlung und Nutzung einer gesetzlichen Grundlage Bedarf. Der vorliegende Entwurf beinhaltet jedoch massive, unverhältnismässige Eingriffe in die Grundrechte der Flugpassagier*innen. Er verlangt, dass automatisch und zentralisiert sämtliche Daten gesammelt werden, und das verdachtsunabhängig. Damit erfolgt eine Massenüberwachung, eine Vorratsdatenspeicherung für den Flugbereich, die faktisch einer anlasslosen Rasterfahndung gleichkommt. Dass solche Praktiken grundrechtswidrig sind, wurde bereits mehrfach von europäischen Gerichten bestätigt; zuletzt hat sich der Europäische Gerichtshof (EuGH) im Juni 2022 sogar explizit zu den europäischen Richtlinien für PNR bzw. deren Umsetzung geäussert. Und das sehr kritisch: Die Verarbeitung von PNR muss gemäss dem Urteil von den EU-Ländern stark eingeschränkt werden.¹ Auch die UNO-Resolutionen, welche die Nutzung von PNR für die Staaten verbindlich machen, weisen auf die zwingend nötige Achtung der Grundrechte.²

¹ <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220105de.pdf> (25.07.2022)

² beispielsweise die Resolution 2482 (2019): « , to ensure PNR data is used by and shared with competent national authorities, with full respect for human rights and fundamental freedoms, » (<http://unscr.com/en/resolutions/doc/2482>, 25.07.2022)

Der Bundesrat rechtfertigt den Grundrechtseingriff mit der Bekämpfung von Terrorismus und einer Erhöhung der Sicherheit – diese Versprechen sind aber äusserst fraglich und auch nicht überprüfbar. Zur Unverhältnismässigkeit des Entwurfs tragen zudem weitere Faktoren bei: Der Katalog an Delikten, für deren Bekämpfung PNR genutzt werden dürfen, geht weit über Terrorismus und schwere Straftaten hinaus. Die GRÜNEN lehnen zudem die Möglichkeit ab, dass die neue Organisation Passenger Information Unit (PIU) Risikoprofile und Beobachtungslisten erstellen darf. Ebenso lehnen wir ab, dass der Nachrichtendienst des Bundes (NDB) automatisch die PNR bestimmter Flugstrecken erhalten soll. Zudem sind die Aufbewahrungsdauer und das Auskunftsrecht grundrechtsfreundlicher auszugestalten.

Die GRÜNEN lehnen in der Konsequenz das FPG in der vorliegenden Form ab und verlangen vom Bundesrat, dass er ein neues FPG entwirft, welches den individuellen Grundrechten mehr Achtung verschafft und den Bedenken und Entscheiden des EuGH Rechnung trägt, keine neuen und intransparenten Überwachungsmechanismen schafft sowie die Nutzung von PNR in einem engen und effektiven Rahmen hält.

Zu einzelnen, besonders gewichtigen Punkten nehmen wir wie folgt Stellung:

Informationspflicht (Art. 5)

Art. 5 hält zwar eine Informationspflicht fest, verzichtet aber auf weitere Details. Die Erläuterungen detaillieren dazu, dass eine Information der Passagier*innen über die AGB möglich ist. Somit ist es möglich, diese Information an einem Ort im Kleingedruckten anzubringen, das in der Regel nicht gelesen wird. Das Ziel der wirklichen Aufklärung über die Datenübermittlung und -bearbeitung wird damit klar verfehlt. Für uns GRÜNE ist zwingend, dass eine aktive, verständliche und gut sichtbare Information über die Verwendung der PNR erfolgen muss, und zwar vor der Buchung der Flugtickets. Zudem muss der Bund Verfahren und Sanktionen klären, falls die Fluggesellschaften der Informationspflicht nicht nachkommen.

Deliktskatalog und Straftaten-Definitionen (Art. 6 und 7)

Aus Sicht der GRÜNEN muss der vorgesehene Deliktskatalog von «terroristischen und anderen schweren Straftaten» zwingend substanziell verkleinert werden, um den Grundrechtseingriff abzuschwächen und auch dem neuesten Urteil des EuGH vom Juni 2022 (siehe oben) Rechnung zu tragen, wonach ein mittelbarer objektiver Zusammenhang mit der Beförderung von Fluggästen bestehen muss. Der im Anhang 2 festgehaltene Deliktskatalog muss daraufhin überarbeitet bzw. verkleinert werden. Es ist beispielsweise wenig einleuchtend, weshalb die Verfolgung von Produktpiraterie mittels PNR eine Massenüberwachung rechtfertigen soll, weil dies nichts mit dem Schutz vor Terrorismus zu tun hat.

Weitere problematische Aspekte der Straftaten-Definitionen sind die ungenügend geklärte Definition von «Terrorismus» und die gleichzeitig weitgehende Anwendung dieses Begriffs – beispielsweise im Zusammenhang mit Landfriedensbruch. Auch dieses Delikt muss aus dem Katalog gestrichen werden. Weiter verlangen die GRÜNEN, den Begriff der «geplanten Straftaten» (Art. 7 Abs. 1) zu streichen, weil unklar ist, was damit gemeint ist.

Risikoprofile und Beobachtungslisten (Art. 9)

Zu den gravierendsten ungerechtfertigten Grundrechtseingriffen des Entwurfs gehört der Vorschlag, dass die neu entstehende PIU, welche die PNR zusammenzieht und abgleicht,

selbst Risikoprofile und Beobachtungslisten erstellen darf. Die GRÜNEN verlangen, dass dieser Artikel ersatzlos gestrichen wird. Es soll keine neue Überwachungsbehörde geschaffen werden, welche Daten selbst analysieren kann. Die PIU soll höchstens nach Treffern suchen und das Resultat weitergeben können. Danach hat sie die erhaltenen (und die entstandenen) Daten zu löschen.

Wird Art. 9 nicht gestrichen, muss genau geregelt werden, wie diese Analysen gemacht werden, damit Transparenz hinsichtlich der Risikoprofile und Beobachtungslisten geschaffen wird und insbesondere keine diskriminierenden Merkmale Grundlage der Risikoprofile und Beobachtungslisten sind. Zudem müssen die Ergebnisse der Überprüfung gemäss Art. 9 Abs. 5 veröffentlicht und es muss eine wirksame Aufsicht definiert werden.

Zusammenarbeit mit dem NDB (Art. 10)

Der Entwurf ermöglicht die automatisierte Übermittlung von PNR auf vom NDB bestimmten Flugstrecken. Aufgrund der bisherigen, ausufernden Datensammel-Praxis des NDB ist davon auszugehen, dass sehr viele Strecken davon betroffen sein werden. Dies weitet die Massenüberwachung auf eine Behörde aus, welche keine unmittelbare Strafverfolgung betreibt. Zudem bleibt für die Flugpassagier*innen intransparent, dass ihre Daten automatisiert zum Nachrichtendienst weitergeleitet werden. Der NDB hat über die letzten Jahrzehnte mehrfach die Rahmenbedingungen für die Informationssammlung und die gesetzlich vorgegebenen Löschfristen nicht beachtet – bevor in diesem Bereich keine Befolgung der gesetzlichen Regelungen durch den NDB sichergestellt ist, sollten keine weiteren riesigen Datensammlungen durch den NDB angehäuft werden. Die GRÜNEN verlangen, Art. 10 ersatzlos zu streichen.

Verzichtet der Bundesrat auf eine Streichung, so müssen eventualiter zumindest die vom NDB bestimmten Strecken veröffentlicht und die Passagier*innen vor der Buchung aktiv über die generelle Weiterleitung ihrer PNR an den NDB informiert werden, um für sie Transparenz herzustellen. PNR, die beim NDB zu keinen Übereinstimmungen führen, sind zudem umgehend (und nicht erst nach 96 Stunden) zu löschen.

Fristen und Aufbewahrungsdauer (Art. 14 und 16)

Die äusserst lange Aufbewahrungsdauer von fünf Jahren bedeutet einen weiteren massiven Grundrechtseingriff, dieser muss unbedingt abgeschwächt werden. Die GRÜNEN verlangen, dass die Daten unmittelbar nach dem Abgleich durch die PIU gelöscht werden. Sollte der Bundesrat an einer Speicherung festhalten, so muss mindestens die Pseudonymisierung schneller erfolgen, nämlich automatisiert und umgehend nach dem Abgleich der Daten.

Zudem ist es nötig, dass auch die Aufbewahrungsdauer von Daten, die aus dem Abgleich nach Art. 7 und 9 resultieren, im Gesetz (und nicht in der Verordnung) festgehalten wird (Art. 16 Abs. 2). Es handelt sich hier um besonders schützenswerte persönliche Daten, welche nur aufgrund einer formalgesetzlichen Grundlage bearbeitet werden dürfen.

Auskunftsrecht (Art. 15 und 18)

Auch pseudonymisierte Daten sind persönliche und schützenswerte Daten, welche (mithilfe der Konkordanztafel) einem Individuum zuordenbar bleiben. Deshalb ist es eine Einschränkung der Grundrechte, wenn das Auskunftsrecht für pseudonymisierte Daten nicht mehr gilt. Es gibt für die Streichung des Auskunftsrechts keine verständliche Begründung, Art. 18 Abs. 2 ist deshalb zu streichen. Ebenso müssen Flugpassagier*innen das Recht haben, die für die

Wahrnehmung des Auskunftsrechts nötige Aufhebung der Pseudonymisierung zu beantragen (Art. 15 Abs. 1).

Weitere Punkte

Für die folgenden weiteren Punkte verweisen wir zustimmend auf die detaillierten Ausführungen in der Stellungnahme der Digitalen Gesellschaft:

- Datensicherheit: Regelung der technischen Einzelheiten in Gesetz oder Verordnung
- Übermittlung der Daten: nur einfache (nach Abschluss des Boardings), aber nicht zweifache Übermittlung der Daten
- Definition von «Verdacht»: «hinreichender» statt «konkreter» oder «begründeter»
- völkerrechtliche Verträge: Sicherstellung des Datenschutzniveaus in anderen Staaten gemäss dem Standard des neuen Datenschutzgesetzes

Wir danken Ihnen, Frau Bundesrätin, sehr geehrte Damen und Herren, für die Berücksichtigung unserer Kritikpunkte am vernehmlasssten Gesetzesentwurf.

Freundliche Grüsse



Balthasar Glättli
Präsident



Rahel Estermann
stv. Generalsekretärin, Leiterin Politik

Bundesrat Karin Keller-Sutter
Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Elektronisch an:
kd-rechtsabteilung@fedpol.admin.ch

Bern, 22. Juli 2022

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten

Vernehmlassungsantwort der Schweizerischen Volkspartei (SVP)

Sehr geehrte Damen und Herren

Wir nehmen im Rahmen der rubrizierten Vernehmlassung Stellung zur Vorlage. Wir äussern uns dazu wie folgt:

Die SVP lehnt das Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten ab. Das Gesetz führt zu einer Verwässerung der Zuständigkeiten des NDB und führt zur Bildung einer zu teuren Fachstelle PIU (Passenger Information Unit), welche eine umfassende Datenbank anlegt, in welcher auf Vorrat Personendaten gespeichert werden. Ausserdem kommt das Gesetz zu einem Zeitpunkt, wo mehrere Urteile bezüglich des Umgangs mit PNR und API noch ausstehen und somit eventuell erneute Anpassungen des Gesetzes bald notwendig würden. Die Auswertung solcher Flugpassagierdaten sollte in der Kompetenz des NDB bleiben, wo sie bis heute in eingeschränkter Masse angesiedelt war. Die Errichtung einer PIU sollte lediglich zur Koordination des Informationsaustausches im In- und Ausland errichtet werden und könnte mit einem minimalen Personalaufwand betrieben werden.

Die SVP befürwortet grundsätzlich Massnahmen zur Bekämpfung von Terrorismus und schwerer Kriminalität, lehnt dieses Gesetz in dieser Form jedoch ab. Der Austausch von Personendaten von verdächtigen oder steckbrieflich gesuchten Personen ist zu begrüssen, die pauschale Speicherung aller Personendaten für 6 Monate, bzw. in pseudonymisierter Form für 5 Jahre, ist jedoch eine unnötige und zu teure Massnahme. Die definierten Zeiträume von 6 Monaten, bzw. 5 Jahren sind aus der Sicht der SVP sowohl aus finanzieller wie auch aus datenschutztechnischen Gründen zu lange. Die Vorratsdatenspeicherung von Personendaten ist unverhältnismässig und stellt einen Eingriff in die Grundrechte der Passagiere dar. Der EuGH stuft in seinem Urteil C-817/19 vom 21. Juni 2022 diese Frist als ebenfalls zu lange ein. Dementsprechend fordert die SVP die Richtlinie des EuGH zu übernehmen und alle Personendaten nach 6 Monaten zu löschen, insofern es keinen expliziten Bedrohungsverdacht bei bestimmten Personen gibt.

Weiter führt das Urteil des EuGH aus, dass Personendaten nicht automatisiert weitergegeben oder ausgewertet werden dürfen. Der Austausch darf nur verdachtsabhängig stattfinden und nur mit Ländern geschehen, in denen es Hinweise auf Gefahren durch Terrorismus oder schwere Kriminalität im Zusammenhang mit Flügen gibt. Die bisherige Praxis des NDB bewegt sich sehr nahe an diesem Gerichtsurteil. Aus dieser Perspektive ist es sinnvoller die Befugnisse des NDB in diesem Bereich minimal anzupassen, anstatt eine neue, teure und überbürokratische PIU zu schaffen, welche genau die Arbeit übernimmt, welche der NDB bereits heute erledigt.

Terrorismusbekämpfung ist Angelegenheit des NDB. Jegliche Aufweichung dieser Zuständigkeit macht die Schweiz potenziell anfälliger für Terrorismus. Die Übertragung eines Teiles der Terrorismusbekämpfung führt zu bürokratischem Mehraufwand, welcher sowohl zeitliche als auch finanzielle Kosten haben wird. Die Einrichtung einer Anlaufstelle für die Koordination des Informationsaustausches zwischen fedpol, NDB, SEM, den Kantonen, dem Bund, den Fluggesellschaften und ausländischen Partnerdiensten ist notwendig und sollte nicht vom NDB übernommen werden. Hier reicht jedoch das Einrichten eines kleinen Büros mit minimalem Personalaufwand. Alle weiteren Massnahmen und Befugnisse sollten jedoch beim NDB bleiben. Die SVP setzt sich für eine PIU mit minimalem Personalaufwand ein, die nur den Informationsfluss sicherstellt. Im Bereich Terrorismusbekämpfung lehnt die SVP eine Schwächung des NDB zu Gunsten einer neuen Abteilung ab.

Der Gesetzesentwurf kommt zum falschen Zeitpunkt. Vor dem EuGH ist nach wie vor eine Klage aus Deutschland hängig. Gleichzeitig ist in der Schweiz eine Richtlinie für die Handhabung von API-Daten immer noch in Arbeit. Die Schweiz riskiert hier also ein Gesetz zu verabschieden, dass unter Umständen einen grossen Anpassungsprozess durchlaufen muss, sobald API-Richtlinien definiert wurden oder ein neues EuGH Urteil vorliegt. Die SVP plädiert daher dafür die bisherige Praxis des Datenaustausches, welche seit 2018 provisorisch umgesetzt wird, so lange weiterlaufen zu lassen, bis eine Gesetzesgrundlage sowohl für API als auch für PNR verabschiedet werden kann und internationale Rechtszweifel beseitigt sind.

Aus den obenerwähnten Gründen kann die SVP Gesetz zur Bearbeitung von Flugpassagierdaten nicht unterstützen.

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

SCHWEIZERISCHE VOLKSPARTEI

Der Parteipräsident

Der Generalsekretär

Marco Chiesa
Ständerat

Peter Keller
Nationalrat



Per E-Mail

**Fedpol
Bundesamt für Polizei
Guisanplatz 1A
3003 Bern**

kd-rechtsabteilung@fedpol.admin.ch

Vernehmlassungsantwort zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG);

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zur Stellungnahme, die wir gerne wahrnehmen:

1 Grundsätzliche Bemerkungen

Die SP Schweiz steht der mit diesem neuen Bundesgesetz vorgesehene umfassende, verdachtsunabhängige und systematische Bearbeitung von Flugpassagierdaten durch die Sicherheitsbehörden grundsätzlich kritisch gegenüber.¹ Eine solche systematische Bearbeitung der Daten aller Flugpassagiere ist für uns aus Gründen der Datensparsamkeit, der Verhältnismässigkeit und des Datenschutzes heikel. So sehen wir dabei insbesondere Risiken in Bezug auf die Datensicherheit und den potentiellen Missbrauch dieser Daten. Wir sind grundsätzlich der Ansicht, dass sowohl der Staat wie auch Private von den Bürger:innen nur so viel Daten bearbeiten sollen wie zwingend notwendig.² Dies soll auch für Flugpassagiere gelten. Zudem erachten wir das Argument nicht als überzeugend, dass mit einer solchen systematischen Bearbeitung von zahlreichen Flugpassagierdaten Terror und weitere Schwerstkriminalität tatsächlich wirksam bekämpft werden kann: Es ist fraglich, ob Terrorist:innen und weitere Schwerstkriminelle tatsächlich Linienflüge benutzen und dabei ihre wahren Identitätsangaben³ preisgeben. Selbstverständlich ist auch der SP

¹ Vgl. Sendung Echo der Zeit Radio SRF, «Bund will Daten von Flugpassagieren», 25.4.2022.

² Vgl. Legislaturziele der SP-Fraktion 2019 bis 2023, S. 59, Februar 2019.

³ Vgl. Erläuternder Bericht, S. 21f.

Schweiz die Bekämpfung von Terrorismus und weiterer Schwerstkriminalität ein wichtiges Anliegen⁴. Dafür braucht es von Seiten der schweizerischen Behörden aber v.a. eine schlagkräftige, effizient aufgestellte und international gut vernetzte Bundesanwaltschaft. Ein Anliegen, für welches sich die SP Schweiz im Parlament aktiv einsetzt.⁵

Verbesserungsbedarf sehen wir bei dieser Vorlage insbesondere bei der Weitergabe der Flugpassagierdaten an die Strafverfolgungsbehörden (siehe untenstehend Ziff. 2.5.), der Aufbewahrungsdauer der Flugpassagierdaten (siehe Ziff. 2.7. nachstehend) sowie den Voraussetzungen für die Übermittlung von Flugpassagierdaten an ausländische Stellen (siehe Ziff. 2.8. untenstehend).

2 Kommentar zu den wichtigsten Bestimmungen

2.1. Regelung der technischen Einzelheiten zur Übermittlung der Flugpassagierdaten (Art. 2 Abs. 4 VE-FPG)

Gemäss dem neuen Flugpassagierdatengesetz sollen die Luftverkehrsunternehmen verpflichtet werden, zahlreiche sensible Daten aller Fluggäste⁶ wie z.B. Name, Postadresse, Telefonnummer und E-Mail-Adressen aber auch die Beziehung zu Begleitpersonen an das fedpol übermitteln müssen.⁷ Bei so sensiblen Daten in einem solch enormen Umfang ist die Gewährleistung der Datensicherheit zentral (siehe dazu oben stehend unter Ziff. 1). Folglich reicht es aus staatspolitischen Gründen nicht aus, die technischen Einzelheiten dieser Datenübermittlungen durch das zuständige Bundesamt fedpol regeln zu lassen, wie dies der Vorentwurf des Bundesrates vorsieht.⁸ Vielmehr müssten die Grundsätze dieser Datenübermittlung im FPG als Gesetz im formellen Sinne und die Einzelheiten in einer Bundesratsverordnung festgehalten sein.

Folglich beantragt die SP Schweiz in **Art. 2 Abs. 4 VE-FPG** die **Grundsätze der Datenübermittlung** zwischen Luftverkehrsunternehmen und fedpol **im FPG selbst** und **die Einzelheiten in einer Bundesratsverordnung zu regeln**.

2.2. Auflistung der Delikte, zu deren Aufklärung die übermittelten Flugpassagierdaten bearbeitet werden dürfen (Art. 6 VE-FPG)

Im Sinne des verfassungsrechtlichen und datenschutzrechtlichen Verhältnismässigkeitsprinzips ist es für die SP Schweiz – wenn überhaupt – nur denkbar, die sensiblen Daten von Flugpassagier:innen vom fedpol weiter zu bearbeiten, wenn dies

⁴ Vgl. Erläuternder Bericht, S. 19.

⁵ Vgl. Motionen 21.3970 / 21.3972 RK-S / RK-N Reform der Bundesanwaltschaft und ihrer Aufsicht.

⁶ Vgl. Erläuternder Bericht, S. 21.

⁷ Siehe Anhang I VE-FPG.

⁸ Siehe Erläuternder Bericht, S. 21.

für die Verhinderung und Aufklärung von sehr schwerwiegenden Straftaten notwendig ist. Die in Art. 6 VE-FPG aufgelisteten Delikte werden diesem Anspruch nicht alle gerecht: So ist es im Bereich der terroristischen Straftaten gemäss Art. 6 Abs. 2 aus unserer Sicht klar, dass Delikte wie Terrorismusfinanzierung oder Beteiligung an terroristischen und kriminellen Organisationen als terroristische Straftaten zu gelten haben.⁹ Problematisch erachten wir hingegen die Auflistung eines sog. «terroristisch motivierten» Landfriedensbruch¹⁰ unter diese Kategorie. Insbesondere deshalb, weil der Begriff der terroristischen Motivation nicht zuletzt auch im Zuge des Erlasses Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT) unscharf und tendenziell ausufernd verwendet wird. Ebenfalls erscheint es uns als übertrieben, Delikte im Bereich der Produktpiraterie¹¹ als schwere Straftaten gemäss Art. 6 Abs. 3 lit. a VE-FPG qualifizieren zu wollen.

Folglich beantragt die SP Schweiz, das Delikt eines **terroristisch motivierten Landfriedensbruchs gemäss Art. 260 StGB** aus dem **Deliktskatalog der terroristischen Straftaten gemäss Art. 6 Abs. 2 VE-FPG** sowie die **Delikte der Produktpiraterie aus dem Deliktskatalog der schweren Straftaten** gemäss Art. 6 Abs. 3 lit. a VE-FPG zu streichen.

2.3. Plausibilisierung des Abgleichs der Flugpassagierdaten mit Informationssystemen bei Übereinstimmung (Art. 7 Abs. 3 VE-FPG)

Wie der Bundesrat im Erläuternden Bericht selbst einräumt, sind Übereinstimmungen von Flugpassagierdaten mit Einträgen in polizeilichen Informationssystemen fehleranfällig. Insbesondere ist nicht leichthin festzustellen, ob entsprechende Einträge in diesen Informationssystemen tatsächlich im Zusammenhang mit Katalogstraftaten von Art. 6 VE-FPG stehen.¹² Vor diesem Hintergrund fordern wir das fedpol dazu auf, im Vollzug die notwendigen Plausibilisierungen ausreichend vorzunehmen und die entsprechenden Flugpassagierdaten bei fehlendem Zusammenhang mit einer Katalogstraftat konsequent zu löschen.

⁹ Vgl. Erläuternder Bericht, S. 22f.

¹⁰ Anhang I, Erläuternder Bericht, S. 52.

¹¹ Anhang II, Erläuternder Bericht, S. 54.

¹² Vgl. Erläuternder Bericht, S. 26.

2.4. Regelung der Datenweitergabe an den NDB (Art. 10 VE-FPG)

Die SP Schweiz begrüsst die relativ restriktive Regelung der Weitergabe der Flugpassagierdaten an den Nachrichtendienst.¹³ Diese darf folglich keinesfalls abgeschwächt werden, insbesondere ist für uns ein direkter Zugriff des NDB auf das PNR-Informationssystem nicht denkbar.

2.5. Voraussetzung für Meldung an Strafverfolgungsbehörde (Art. 12 Abs. 1 VE-FPG)

Da es sich bei den vom fedpol an die Strafverfolgungsbehörden bei Verdacht auf terroristische oder schwere Straftaten gestützt auf Art. 12 Abs. 1 gemeldeten Flugpassagierdaten¹⁴ um sensible Daten handelt (siehe dazu oben stehend unter Ziff. 2.1.) rechtfertigt sich eine solche Weitergabe aus Gründen der Verhältnismässigkeit nur bei einem hinreichend dringenden Tatverdacht.

Folglich beantragt die SP Schweiz, Art. 12 Abs. 1 VE-FPG folgendermassen zu ändern:

Art. 12 Abs. 1 FPG Meldung bei einem Verdacht

1 Besteht der **dringende** Verdacht, dass eine terroristische oder andere schwere Straftat begangen wurde oder werden soll, so meldet die PIU dies den zuständigen Strafverfolgungsbehörden.

2.6. Zugriff auf das PNR-Informationssystem (Art. 13 Abs. 2 VE-FPG)

Da es sich bei den im PNR-Informationssystem enthaltenden Daten um besonders sensitive Personendaten in grossem Umfang handelt (siehe dazu oben stehend unter Ziff. 1), dürfen nach Ansicht der SP Schweiz aus Gründen des Datenschutzes und der Datensicherheit nur öffentlich-rechtliche Angestellte Zugriff auf das PNR-Informationssystem haben.¹⁵ Ein Zugriff von Privaten auf das PNR-Informationssystem ist für uns ausgeschlossen. Dies muss auf Gesetzesstufe so in Art. 13 VE-FPG festgehalten werden.

¹³ Vgl. Erläuternder Bericht, S. 29.

¹⁴ Siehe Erläuternder Bericht, S. 32.

¹⁵ Vgl. Erläuternder Bericht, S. 33.

2.7. Dauer der Frist bis zur Pseudonymisierung der Flugpassagierdaten (Art. 14 VE-FPG)

Wie der Bundesrat im Erläuternden Bericht zutreffenderweise einräumt, wird die Anwendung dieses Gesetzes dazu führen, dass Daten von Flugpassagieren ohne Bezug zu einer Straftat herangezogen werden.¹⁶ Dies ist an sich schon problematisch. Vor diesem Hintergrund ist es umso wichtiger, dass die erhobenen Flugpassagierdaten so rasch wie möglich zumindest pseudonymisiert werden. Die vom Bundesrat dazu vorgeschlagene Frist von 6 Monaten erscheint uns daher als zu lange.

Folglich beantragt die SP Schweiz, Art. 14 VE-FPG folgendermassen zu ändern:

Art. 14 FPG Pseudonymisierung

Das PNR-Informationssystem pseudonymisiert die Flugpassagierdaten drei Monate nach ihrer Übermittlung durch die Luftverkehrsunternehmen automatisch.

2.8. Aufbewahrungsdauer der Flugpassagierdaten (Art. 16 Abs. 1 VE-FPG)

Der Bundesrat schreibt im Erläuternden Bericht selbst, dass die vorgeschlagene Aufbewahrungsdauer für diese Flugpassagierdaten von fünf Jahren mit Blick auf die Tatsache, dass es sich dabei um Daten von einer Vielzahl von unbescholtenen Bürger:innen handelt, als lang und einen Paradigmenwechsel.¹⁷ Für den Schutz der Daten der Bürger:innen erachtet es die SP Schweiz als zentral, dass von Behörden gesammelte Daten nur so lange wie zwingend notwendig vom Staat aufbewahrt werden. Vor diesem Hintergrund ist es angezeigt, diese Aufbewahrungsfrist markant zu verkürzen.

Art. 16 Abs. 1 FPG Aufbewahrungsdauer und Löschung

1 Die Flugpassagierdaten werden zwei Jahre nach ihrem Eingang im PNR-Informationssystem automatisch gelöscht.

¹⁶ Siehe Erläuternden Bericht, S. 33.

¹⁷ Siehe Erläuternden Bericht, S. 36.

2.9. Voraussetzungen für die Übermittlung von Flugpassagierdaten an ausländische Stellen (Art. 22 Abs. 3 VE-FPG)

Der Bundesrat stellt im Erläuternden Bericht fest, dass eine Übermittlung von Flugpassagierdaten des fedpols an ausländische Stellen ohne bestehenden Staatsvertrag nur in begründeten Ausnahmefällen zulässig sein.¹⁸ Folglich soll die Hürde für eine solche Übermittlung entsprechend hoch sein. Unserer Ansicht nach erfordert dies das Bestehen eines dringenden Verdachts für eine terroristische oder anderweitig schwere Straftat (vgl. dazu auch obenstehend unter Ziff. 2.5.)

Folglich beantragt die SP Schweiz, Art. 22 Abs. 3 VE-FPG folgendermassen zu ändern:

Art. 22 Abs. 3 FPG Amtshilfe

3 Die Übermittlung von Flugpassagierdaten ist unzulässig, wenn gegen die betreffende Person kein **dringender** Verdacht vorliegt, eine terroristische oder andere schwere Straftat zu planen oder begangen zu haben.

Wir bitten Sie, unsere Anliegen bei der Überarbeitung der Vorlage zu berücksichtigen.

Mit freundlichen Grüssen

SOZIALDEMOKRATISCHE PARTEI DER SCHWEIZ



Mattea Meyer

Co-Präsidentin



Cédric Wermuth

Co-Präsident



Claudio Marti

Politischer Fachsekretär

¹⁸ Siehe Erläuternder Bericht, S. 40.



Sehr geehrter Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Stellungnahme der Piratenpartei Schweiz zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Vernehmlassung 2021/80)

Bezugnehmend auf Ihre Vernehmlassungseröffnung zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 13.04.2022 nehmen wir gerne Stellung und würden es zukünftig sehr begrüssen, wenn wir in Ihre Adressatenliste aufgenommen werden.

Im Weiteren finden wir Piraten 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.

Vorbemerkungen

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 Risikoanalyse und Folgeabschätzung.

Im Speziellen erachten wir eine anlasslose Vorratsdatenspeicherung, wie sie im vorliegenden Gesetzesentwurf der Fall ist ab. Solche massenhafte Überwachung der Bevölkerung ist vor allem auch in der Abwägung Nutzen - Grundrechtseingriff nie positiv. "Ein Zeichen setzen", Zitat aus dem Einladungsschreiben, ist offensichtlich genau das Gegenteil von einer sorgfältigen Abwägung beim Eingriff in Grundrechte, nur weil man etwas kann, weil Daten vorhanden sind, heisst das noch lange



nicht, dass dies notwendig, wirksam oder verhältnismässig ist. Ein Zeichen setzen bedeutet, dass genau diese Abwägung offensichtlich nicht gemacht wurde.

Stellungnahme zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten

Gerne nehmen wir zu den einzelnen Artikeln wie folgt Stellung:

Artikel 2

Abs. 1 sieht eine Übermittlung von Daten bei allen Flügen von und in die Schweiz vor. Der EuGH hat hingegen das Datensammeln für Flüge innerhalb der EU deutlich auf besondere Fälle eingeschränkt [1]. Es sollte entsprechend, um der Datensparsamkeit zu genügen, ebenfalls auf die Daten der meisten Flüge im Schengenraum verzichtet werden.

In Abs. 2 wird eine Übermittlung der Flugpassagierdaten 48-24 Stunden vor Abflug festgelegt. Indes ist keine Löschung der Daten von Passagieren, die den Flug nicht antreten, festgeschrieben. Diese fehlende Regelung ist nicht nachvollziehbar.

Für die in Abs. 3 angedachte Löschung von besonders schützenswerten Daten fehlt eine Instanz, welche eine allfällige Löschung kontrolliert. Ferner stellt sich die Frage, was nach der in Art. 14 geplanten Pseudonymisierung geschieht, da hier Betroffene ihr Auskunftsrecht verlieren.

Art. 2 Abs. 4

Im FPG werden in grossem Masse schützenswerte Daten gespeichert und übermittelt. Deshalb ist es unabdingbar dem Datenschutz eine sehr grosse Rolle beizumessen. Es ist unzureichend die technischen Einzelheiten der Datenübermittlung dem Fedpol zu überlassen. Das Fedpol muss diese zwingend gemeinsam mit dem EDÖB festlegen, wobei dem EDÖB die finale Entscheidung obliegt.

Artikel 5

Die Übermittlung der persönlichen Daten der Flugpassagiere stellt einen schwerwiegenden Eingriff in die Grundrechte dar, der klar kommuniziert werden muss. Die aktuelle Formulierung lässt jedoch offen, wie und in welcher Form dies geschehen soll. Hier ist eine Präzisierung erforderlich, dass Passagiere klar, verständlich mit expliziter Nennung aller Daten, und auch



gesondert, und nicht verklausuliert und versteckt, vor der Buchung auf diesen Vorgang hingewiesen werden und einwilligen müssen. Diese Einwilligung muss eine bewusste Entscheidung darstellen.

Artikel 6

Die Piratenpartei hält es weiterhin für rechtsstaatlich äusserst fragwürdig den Begriff der "schweren Straftat" wie in Absatz 1 zu verwenden, welcher bekanntermassen nicht genauer definiert ist und auch in der Lehre die Meinungen weit auseinandergehen. Bevor dieser Begriff in neuen Gesetzen (oder in Gesetzesanpassungen) genutzt wird muss diese Definitionslücke geschlossen werden. Siehe auch Urteil 6B_1468/2019 des Bundesgerichtes [2]:

"1.4.2. Der Gesetzgeber verzichtete darauf, schwere Straftaten im Sinne von Art. 141 Abs. 2 StPO zu definieren. Das Bundesgericht klärte bisher nicht abschliessend, was generell unter diesem Begriff zu verstehen ist (vgl. Urteil 6B_287/2016 vom 13. Februar 2017 E. 2.4.4). Auch in der Lehre finden sich keine Vorschläge für eine Definition und die Ansichten gehen auseinander."

Absatz 3 zeigt, wie so häufig bei Überwachungsgesetzen, dass es bei diesem Gesetz entgegen den grossen Versprechungen nicht um Terrorismus oder besonders schwere Straftaten geht, sondern abermals um einen nicht zu rechtfertigenden möglichst breiten Deliktskatalog. Dass der tiefe Grundrechtseingriff beispielsweise mit "Handel mit Hormonen" oder "Produktpiraterie" begründet wird, steht in keinem Verhältnis. Spannend wird es sicher bei Computerstraftaten. Hier stellt sich die Frage, ob hierunter dann auch die Mitarbeiter der (ausländischen) Geheimdienste, welche weithin auch für Wirtschaftsspionage bekannt sind, fallen und beispielsweise auch die Führungsriege des CIA betroffen sind, oder ob hier grosszügige Ausnahmen gelten sollen.

Wir fordern, dass die PNR-Daten ausschliesslich für terroristische Straftaten oder für Straftaten, für die der Gesetzgeber eine Mindeststrafe von 3 Jahren Haft vorsieht, bearbeitet werden dürfen. Darüber hinaus ist unbedingt eine explizite Terrorismusdefinition festzulegen, damit nicht wie im PMT ein Grossteil der Bevölkerung als potentielle Terroristen verfolgt werden können [3]

Absatz 6 widerspricht Art. 2 Abs. 3, welcher den Luftverkehrsunternehmen verbietet besonders schützenswerte Personendaten zu übermitteln, was biometrische Daten einschliesst, und eine sofortige Löschung bei der PIU vorsieht. Ausserdem sind biometrische Daten im Anhang 1 "Flugpassagierdaten" (inkl. dem Verweis in Punkt 18) nicht vorgesehen und sollten somit per se nicht Teil der Daten sein.



Weiter ist bekannt, dass das US-Department for homeland-security diese Daten vollumfänglich abrufen will, was zu verhindern ist und mit Datensparsamkeit zusätzlich erschwert werden sollte [4].

Darüber hinaus hat auch der der EuGH vor wenigen Wochen geurteilt, dass das durch die PNR-Richtlinie eingeführte System sich nur auf die in den Rubriken ihres Anhangs I aufgeführten, klar identifizierbaren und umschriebenen Informationen erstrecken darf [1].

Deshalb fordern wir die ersatzlose Streichung dieses Absatzes.

Artikel 9

Die unklare Definition von Analysen, Risikoprofilen und Beobachtungslisten führt zu Unsicherheiten. Hier muss eine entsprechende Präzisierung ergänzt werden.

Auch zu Risikoprofilen und Beobachtungslisten äusserte sich der EuGH insoweit, dass: "keine Technologien der künstlichen Intelligenz im Rahmen selbstlernender Systeme („machine learning“)" herangezogen werden dürfen, da diese in fünf von sechs Fällen zu Falschbeschuldigungen führen [1,5] +).

"Schon jetzt definieren Algorithmen - unter anderem auf Basis der „flight history“ einer Person - die Vorauswahl jener Personen, deren Datensätze rund um den Grenzübertritt genau analysiert werden. Auch das ist nicht statthaft. Der EuGH merkt dazu an, dass eine Überprüfung dieser Methode durch die Kommission aus den Jahren 2018 und 2019 ergeben habe, dass fünf von sechs so generierten „Treffern“ völlig Unbeteiligte trafen. In Folge wurden diese Personen bei jedem neuen Flug beobachtet und nach ihrer Landung oft eingehend „befragt“. Nach diesem Urteil ist ein solcher Automatismus unzulässig, wenn diese Vorabselektion nicht durch Beamte überprüft wird." [6]

Oben genannte Einschränkung sollte in Art. 9 ebenfalls explizit festgehalten werden. Sofern die oben genannte Präzisierung der Definitionen von Analyse, Risikoprofilen und Beobachtungslisten nicht möglich ist, sollte der Artikel 9 ersatzlos gestrichen werden.

Artikel 10

Die aktuelle Formulierung lässt dem NDB die Möglichkeit offen, sämtliche Flugstrecken zu erhalten. Diese offene Formulierung ist unhaltbar und benötigt dringend eine stark einschränkende Präzisierung. Wir schlagen vor, dass die vom NDB erbetenen Strecken von den



GPK des Bundesparlamentes genehmigt werden müssen. Des Weiteren muss eine Löschung der übermittelten Daten direkt nach negativem Abgleich erfolgen.

Artikel 11

Die aktuelle Formulierung lässt ebenfalls eine massenhafte Übermittlung von Daten zu. Diese Einzelfälle müssen die Ausnahme bleiben und gut begründet sein. Über einen solchen Antrag müsste zwingend eine richterliche Behörde entscheiden. Wobei sich hier die Frage stellt, weshalb dieser Artikel überhaupt existiert. An die Behörden in Art. 11 Abs. 2 Bst. a und b können und werden mit der Vorlage schon alle nach Art. 6 Abs. 1 relevanten Daten übermittelt. Es drängt sich der Verdacht auf, dass hier auf Zuruf und ausserhalb des Geltungsbereiches von Art. 6 Daten übermittelt werden sollen. Wir fordern eine Streichung des Artikels.

Artikel 13

Personen, die für die Programmierung des Systems zuständig sind, können für diese Aufgabe Dummy-Daten verwenden.

Personen, die für die Wartung des Systems zuständig sind, benötigen ebenfalls nie Zugriff auf die Daten des Systems.

Abs. 2 Bst. b ist daher ersatzlos zu streichen.

Artikel 14

Diese Pseudonymisierung ist per se umkehrbar und damit keine Verbesserung bezüglich der Grundrechtseingriffe. Es wäre dringend angebracht die Speicherzeit an sich drastisch zu senken (siehe Art. 16).

Artikel 16

Der EuGH hat auf der europäischen Ebene den Normalfall der Speicherfrist von 5 Jahren auf 6 Monate gekürzt [1]. Dies wäre die von der Schweiz mindeste, notwendige Anpassung. Es erschliesst sich der Piratenpartei aber nicht, weshalb eine Abwägung zwischen der massenhaften Speicherung von persönlichen Daten unzähliger Unschuldiger und den äusserst seltenen Fällen der zu erwartenden positiven Treffer bezüglich Terrorismus zu einem positiven Ergebnis kommen



sollte. Deshalb schlagen wir vor, dass die Daten innerhalb von 24 Stunden nach Landung gelöscht werden müssen - inklusive eines funktionierenden Kontroll- und Sanktionsmechanismus.

Artikel 18

Absatz 2 ist besonders bedenklich bezüglich der Gewichtung der Grund- und Menschenrechte der Bürgerinnen und Bürgern seitens des Gesetzgebers.

Die Daten können weiterhin problemlos jederzeit von Behörden abgerufen werden (siehe Art. 15), während Betroffene gleichzeitig jegliches Auskunftsrecht durch die Pseudonymisierung verlieren.

Die Pseudonymisierung der Daten ist damit de facto eine massive Schlechterstellung aller Betroffenen - ohne Grund. Es handelt sich immer noch um besonders schützenswerte Personendaten und damit muss man weiterhin vom Auskunftsrecht Gebrauch machen können, alles andere ist eine Farce. Falls die Daten nicht wie von uns vorgeschlagen innert 24 Stunden nach Landung gelöscht werden, müssen Betroffene auf jeden Fall über den gesamten Zeitraum der Speicherung der Daten (mit oder ohne Pseudonymisierung) von ihrem Auskunftsrecht Gebrauch machen können.

Artikel 20

Aus dem Gesetzestext und dem erläuternden Bericht geht kein ausreichender Grund hervor weshalb ein solch kompliziertes Konstrukt zwingend notwendig sein sollte. Für die Piraten stellt sich die Frage, weshalb nicht die Kantone einfach die Kosten übernehmen anstatt, die Hälfte der Mitarbeitenden zu stellen?

Artikel 21

In diesem Artikel wird festgehalten, dass der Bundesrat mit anderen Staaten völkerrechtliche Verträge zur Bearbeitung der Daten abschliessen kann, "soweit ihr nationales Recht einen mit der Schweiz vergleichbaren Schutz dieser Daten gewährleistet." Wir halten hier eine Präzisierung von "vergleichbar" für notwendig, da unklar ist, ob dies auch "etwas schlechter" beinhalten kann. Und der einzige "Datenschutz" im Schweizer Gesetz ist ja auch nur eine Pseudonymisierung, welche auch noch rückgängig gemacht werden kann, und entspricht somit eigentlich gar keinem Datenschutz.



Artikel 22

In Absatz 3 ist die Präzisierung erforderlich, wer entscheidet, ob ein begründeter Verdacht vorliegt? Wir schlagen ein Gremium aus Bundesrichtern in 5er-Besetzung vor.

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.

Kontakt details für Rückfragen finden Sie in der Begleit-E-Mail.

Quellen:

[1] <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220105de.pdf>

[2]

https://www.bger.ch/ext/eurospider/live/fr/php/aza/http/index.php?highlight_docid=aza%3A%2F%2F01-09-2020-6B_1468-2019&lang=fr&type=show_document&zoom=YES&

[3] <https://www.piratenpartei.ch/2021/05/20/abstimmungsbeschwerde-der-piratenpartei-gegen-pmt/>

[4] <https://www.patrick-breyer.de/internes-libe-treffen-mit-homeland-security-plaene-fuer-biometrie-datenbanken-bringen-daten-von-eu-buergerinnen-in-gefahr/>

[5] <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:62019CJ0817&from=EN>

[6] https://home-affairs.ec.europa.eu/system/files/2020-07/20200724_swd-2020-128_en.pdf—

—

Piratenpartei Schweiz, Arbeitsgruppe Vernehmlassungen, 28. Juli 2022



Eidgenössisches Justiz- und
Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter
Postfach
3003 Bern

Versand per E-Mail: kd-rechtsabteilung@fedpol.admin.ch

28. Juli 2022

**Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung
von terroristischen und anderen schweren Straftaten: Stellungnahme economiessuisse**

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Mit Ihrem Schreiben vom 13. April haben Sie uns eingeladen, zum Vorentwurf des
Flugpassagierdatengesetzes (FPG) Stellung zu nehmen. Wir danken Ihnen für diese Möglichkeit.

economiesuisse vertritt als Dachverband der Schweizer Wirtschaft rund 100'000 Unternehmen jeglicher
Grösse mit insgesamt 2 Millionen Beschäftigten in der Schweiz und weiteren 2 Millionen Beschäftigten
im Ausland. Unser Mitgliederkreis umfasst 100 Branchenverbände, 20 kantonale Handelskammern so-
wie diverse Einzelfirmen.

Generell sind unsere Mitglieder an verlässlichen, international abgestimmten Rahmenbedingungen im
Bereich der sicherheitsrelevanten Datenbearbeitung interessiert. Im Sinne der Rechtssicherheit
begrüssen wir daher die Schaffung einer Rechtsgrundlage für die hoheitliche Bearbeitung von PNR-
Daten. Diese dürfte den direkt betroffenen Unternehmen der Luftfahrt die Zusammenarbeit mit den
Strafverfolgungsbehörden künftig erleichtern. Aufgrund der hohen internationalen Vernetzung der
Branche sind viele von ihnen bereits heute mit ähnlichen Regelungen aus anderen Jurisdiktionen
konfrontiert.

In den Einzelheiten verweisen wir auf die Kritikpunkte unserer direkt betroffenen Mitglieder Aérosuisse,
SWISS International Airlines sowie der Landesflughäfen. Die technischen Übermittlungssysteme für die
Umsetzung des LPG sollten sich an etablierten Lösungen orientieren. Darüber hinaus unterstützen wir
im Sinne der Verhältnismässigkeit die Streichung eines Aspekts der administrativen Sanktionen (Art.
23 Abs. 2 lit. b E-FPG).

Seite 2

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten: Stellungnahme economiesuisse

Herzlichen Dank für die Berücksichtigung unserer Eingabe. Gerne stehen wir bei Rückfragen jederzeit zur Verfügung.

Freundliche Grüsse
economiesuisse



Alexander Keberle
Mitglied der Geschäftsleitung,
Leiter Infrastruktur, Energie & Umwelt



Lukas Federer
Projektleiter Infrastruktur, Energie & Umwelt

Sehr geehrter Herr Dolder

Wir danken Ihnen bestens für die Gelegenheit, in eingangs erwähnter Sache Stellung nehmen zu können.

Da diese Vorlage gemäss Dossieraufteilung zwischen economiesuisse und dem Schweizerischen Arbeitgeberverband von economiesuisse bearbeitet wird, verzichten wir auf eine Stellungnahme zu dieser Vernehmlassung.

Ich wünsche Ihnen einen schönen Tag.

Freundliche Grüsse
Sabine Maeder

Assistentin
SCHWEIZERISCHER ARBEITGEBERVERBAND
Hegibachstrasse 47
Postfach
8032 Zürich
Tel. +41 44 421 17 17
Fax +41 44 421 17 18
Direktwahl: +41 44 421 17 42
maeder@arbeitgeber.ch
<http://www.arbeitgeber.ch>



Eidg. Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter
3003 Bern

per Mail an:
kd-rechtsabteilung@fedpol.admin.ch

Bern, 14. Juli 2022

Vernehmlassung zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG)

Sehr geehrte Frau Bundesrätin

Besten Dank für die Einladung zur oben erwähnten Vernehmlassung. Der Schweizerische Gewerkschaftsbund (SGB) nimmt in enger Absprache mit seinen Verbänden aus der Flugindustrie wie folgt Stellung.

Bei der Buchung eines Fluges werden durch die Airlines Informationen der einzelnen Passagierinnen und Passagiere in je einem Fluggastdatensatz (sogenannter Passenger Name Record, kurz PNR) zusammengefasst – auch in der Schweiz. Bei Flügen in ein Land, das PNR nutzt, sind Luftverkehrsunternehmen heute verpflichtet, den dortigen Behörden die Flugpassagierdaten zur Verfügung zu stellen. Fluggesellschaften, die von der Schweiz aus starten und in der EU, in den USA oder in Kanada landen, müssen diese Daten an die Behörden der Zieldestination bereits heute weitergeben.

Weltweit haben 62 Länder – darunter alle EU-Staaten – Stellen eingerichtet, die diese Informationen über Flugpassagiere für die Bekämpfung von schwerer Kriminalität und Terrorismus auswerten. Die Schweiz selber muss die Daten zwar sammeln, kann diese aber nicht nutzen/auswerten, weil derzeit eine entsprechende Rechtsgrundlage fehlt. Damit riskiert sie, dass Personen, die eine Gefahr für die öffentliche Sicherheit darstellen, unerkannt in die Schweiz und in den Schengen-Raum gelangen können und insbesondere die Sicherheit der Schweizer Flugindustrie und seines Personals gefährdet.

Hier soll das vorliegende FPG Abhilfe und eine Rechtsgrundlage schaffen. Der Schutz der Daten und Persönlichkeitsrechte der Flugpassagiere ist dabei durch das FPG gewährleistet: Einzig das Personal der Zentralstelle PIU darf zur Erfüllung der Aufgaben auf die Flugpassagierdaten zugreifen. Gleichzeitig wird so der Schutz für das Flugpersonal (endlich) erhöht und auch eine Kompatibilität mit dem (EU-)Ausland hergestellt.

Der SGB begrüsst deshalb die Einführung der vorliegenden Revision vollumfänglich.

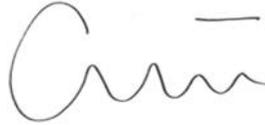
Wir danken Ihnen herzlich für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

SCHWEIZERISCHER GEWERKSCHAFTSBUND

A handwritten signature in black ink, appearing to read 'Maillard', with a long, sweeping underline.

Pierre-Yves Maillard
Präsident

A handwritten signature in black ink, appearing to read 'Cirigliano', with a horizontal line above the end.

Luca Cirigliano
Zentralsekretär

Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal



Der Generalsekretär
CH - 1000 Lausanne 14
Tel. 021 318 91 02
Fax 021 323 37 00
Korrespondenznummer 003.1_2022

Bundesamt für Polizei
Herr Hanspeter Dolder

per E-Mail an:
Hanspeter.Dolder@fedpol.admin.ch
kpr-rm@fedpol.admin.ch

Lausanne, 27. Juli 2022 / wai

Vernehmlassung Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz FPG)

Sehr geehrter Herr Dolder

Mit E-Mail vom 20. Juni 2022 haben Sie das Bundesgericht eingeladen, in oben erwähnter Vernehmlassung Stellung zu nehmen; dafür danken wir Ihnen bestens.

Wir teilen Ihnen mit, dass das Bundesgericht auf eine Stellungnahme verzichtet.

Freundliche Grüsse

Nicolas Lüscher

Kopie an
- Bundesverwaltungsgericht
- Bundesstrafgericht



Verwaltungskommission
Viale Stefano Franscini 7
CH-6500 Bellinzona
Tel. +41 58 480 68 68
Fax +41 58 480 68 42
info@bstger.ch

Registratur Nummer: 1.1.1.8

Eidgenössisches Justiz- und
Polizeidepartement
Frau Bundesrätin Karin Keller-Sutter
Bundeshaus West
3003 Bern

per E-Mail an:

kd-rechtsabteilung@fedpol.admin.ch

Bellinzona, 5. Juli 2022/BOM

**Vernehmlassung: Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur
Bekämpfung von terroristischen und anderen schweren Straftaten
(Flugpassagierdatengesetz, FPG)**

Sehr geehrte Frau Bundesrätin

Mit E-Mail vom 13. April 2022 haben Sie das Bundesstrafgericht eingeladen, in der oben
erwähnten Vernehmlassung Stellung zu nehmen; dafür danken wir Ihnen bestens.

Wir teilen Ihnen mit, dass das Bundesstrafgericht auf eine Stellungnahme verzichtet.

Wir versichern Sie, sehr geehrte Frau Bundesrätin, unserer ausgezeichneten Hochachtung.

Alberto Fabbri
Präsident



Marc-Antoine Borel
Generalsekretär

Kopie an

- Bundesgericht
- Bundesverwaltungsgericht
- Bundespatentgericht



Die Präsidentenkonferenz

Postfach, 9023 St. Gallen
Telefon +41 58 70 52727
Registrierungsnummer: 024.1
Geschäftsnummer: 2022-127

A-Post

Eidgenössisches Justiz- und
Polizeidepartement
Frau Bundesrätin Karin Keller-Sutter
Bundeshaus West
3003 Bern

PDF- und Word-Version per E-Mail an:

Kd-rechtsabteilung@fedpol.admin.ch

St. Gallen, 28. Juni 2022 / moq

Vernehmlassung: Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG)

Sehr geehrte Frau Bundesrätin

Für Ihre Einladung vom 13. April 2022 zur Stellungnahme im eingangs erwähnten Vernehmlassungsverfahren danken wir Ihnen bestens. Wir haben den Entwurf sowie den erläuternden Bericht mit Interesse zur Kenntnis genommen. Das Bundesverwaltungsgericht ist durch die neue Gesetzgebung im Bereich Flugpassagierdatenbearbeitung direkt betroffen und wir äussern uns wie folgt:

In Art. 15 Abs. 4 FPG ist vorgesehen, dass die Präsidentin oder der Präsident der zuständigen Abteilung des Bundesverwaltungsgerichts als Einzelrichter/in (siehe auch Art. 23 Abs. 2 Bst. d und Art. 36c E-VGG) innerhalb von maximal fünf Arbeitstagen nach Erhalt des Antrags um Aufhebung der Pseudonymisierung (Depersonalisierung) bestimmter Daten einer Person im Zusammenhang mit einer begangenen oder bevorstehenden terroristischen oder anderen schweren Straftat zu entscheiden hat, wobei sie oder er eine andere Richterin oder einen anderen Richter mit dem Entscheid beauftragen kann.

Bei der in Art. 23 Abs. 2 Bst. d E-VGG vorgesehenen Änderung ist der Hinweis auf das FPG nicht korrekt. Es muss Art. 15 Absatz 4 und nicht Absatz 3 heissen.

Das Bundesverwaltungsgericht geht davon aus, dass Entscheide nach Art. 15 Abs. 4 FPG nicht weiterziehbar sind. Eine unmittelbare Beschwerde in öffentlich-rechtlichen Angelegenheiten ans Bundesgericht ist gemäss Art. 83 Ziff. a BGG wohl unzulässig, zum einen aufgrund der Besonderheiten des nicht kontradiktorischen Genehmigungsverfahrens, zum anderen weil es um Entscheide auf dem Gebiet der inneren und äusseren Sicherheit des Landes geht.

Das FPG sieht in seiner jetzigen Fassung keine Mitteilungspflicht (*a posteriori*) an die betroffene Person bezüglich der Aufhebung der Pseudonymisierung vor. Im Gegensatz dazu besteht gemäss Art. 33 NDG eine Mitteilungspflicht in Bezug auf die Überwachung mit genehmigungs-

pflichtigen Beschaffungsmassnahmen, welche u.U. eine Beschwerdemöglichkeit auslöst. Im Lichte des Völkerrechts sowie der bundesgerichtlichen Rechtsprechung zu Art. 8 und 13 EMRK (siehe z.B. BGE 138 I 6 E. 1.3.2) erschiene es allerdings angezeigt sich zu überlegen, ob sich auch im Rahmen des FPG eine analoge nachträgliche Mitteilungspflicht mitsamt Beschwerdemöglichkeit aufdrängt, zumal der Passagier in diesen Fällen ebenfalls unwissentlich von einer genehmigungspflichtigen Staatshandlung betroffen ist, die mitunter seine personenbezogenen Daten betrifft. Eine allfällige Mitteilung hätte durch die PIU zu erfolgen.

Nach Art. 15 Abs. 5 FPG kann das Bundesverwaltungsgericht auch eine Ergänzung der Akten oder weitere Abklärungen verlangen. Dem Wortlaut lässt sich nicht entnehmen, ob das Verfahren für die Zeit der Aktenergänzung oder der zusätzlichen Abklärungen beim Bundesverwaltungsgericht anhängig bleibt. Sollte dem so sein, wäre es je nach Konstellation nicht immer möglich, innert 5 Arbeitstagen zu entscheiden, wie dies Art. 15 Abs. 4 FPG verlangt. Um in diesem Punkt Missverständnisse zu vermeiden, wäre eine klarere Formulierung wünschenswert. Sollte man der Meinung sein, dass das Verfahren während der zusätzlichen Abklärungen beim Bundesverwaltungsgericht anhängig bliebe, könnte sich eine gesetzliche Verlängerung der Bearbeitungsfrist aufdrängen. Alternativ müsste eine möglichst rasche und informelle Kommunikationsart zwischen dem Bundesverwaltungsgericht und der Vorinstanz ermöglicht werden, um die zusätzlichen Abklärungen unmittelbar vornehmen und innerhalb der gesetzlichen Ordnungsfrist entscheiden zu können.

Darüber hinaus verzichtet das Bundesverwaltungsgericht auf eine weitergehende Stellungnahme zum FPG.

Mit vorzüglicher Hochachtung

Der Vorsitzende der
Präsidentenkonferenz

David Weiss



Der stellvertretende
Generalsekretär

Bernhard Fasel

Kopie an

- Bundesgericht
- Bundesstrafgericht
- Bundespatentgericht

Chère Madame,
Cher Monsieur,

Nous vous remercions pour la possibilité de prise de position.

Nous n'avons rien à ajouter du point de vue du MPC.

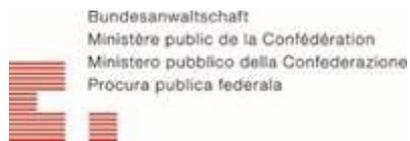
En vous souhaitant une belle journée,

Meilleures salutations,

Droz Elodie BA

Elodie Droz

Juriste Service juridique
Ministère public de la Confédération MPC
Guisanplatz 1, 3003 Berne
elodie.droz@ba.admin.ch
www.bundesanwaltschaft.ch



AEROSUISSE

Dachverband der
schweizerischen
Luft- und Raumfahrt

Fédération faïtière de
l'aéronautique et de
l'aérospatiale suisses

Associazione mantello
dell'aeronautica e
dello spazio svizzeri

Umbrella Organisation
of Swiss Aerospace

Bundesamt für Polizei fedpol
3003 Bern

per Mail: kd-rechtsabteilung@fedpol.admin.ch

Bern, 29. Juli 2022

**Stellungnahme AEROSUISSE zur Vernehmlassung Bundesgesetz über die
Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und
anderen schweren Straftaten**

Sehr geehrte Damen und Herren

Die AEROSUISSE dankt für die Einladung zum Vernehmlassungsverfahren und nimmt
dazu wie folgt Stellung:

Die AEROSUISSE unterstützt das Flugpassagierdatengesetz als international harmo-
nisiertes Instrument, mit dem die Schweiz Terrorismus und andere schwere Straftaten
bekämpfen kann. Seit rund 20 Jahren wird es namentlich in den USA, Kanada und im
Vereinigten Königreich eingesetzt und seit rund 10 Jahren in den meisten Mitgliedstaaten
der EU. In der Schweiz fehlte bis anhin eine ausreichende gesetzliche Grundlage, welche
Zugriff auf Passagierdaten durch die Strafverfolgungsbehörden regelte. AEROSUISSE
begrüssst deshalb die Schaffung des Flugpassagierdatengesetzes.

Gleichzeitig ist darauf zu achten, dass die Übernahme dieses Instruments in das
Schweizer Recht nicht mit einem Swiss-Finish erfolgt. Aus diesem Grund beantragt die
AEROSUISSE, dass Artikel 23 Abs. 2 lit. b E-FPG ersatzlos gestrichen wird.

Begründung

Die Fluggesellschaften können die Richtigkeit der erfassten Daten nicht gewährleisten
oder überprüfen bzw. verifizieren. Die Flugpassagierdaten werden von den Fluggästen
selbst oder von den Agenten erfasst, welche die Buchung erstellen. Aus diesem Grund
dürfen und können die Fluggesellschaften nicht haftbar gemacht werden für fehlerhafte
und/oder falsche Informationen, die bei den Flugpassagierdaten (im PNR) eingetragen
werden. Hinzu kommt, dass es keinen Standard für richtige oder falsche Flugpassagier-
daten gibt. Es handelt sich um Informationen, welche die Fluggesellschaften erfassen, um
eine Buchung kommerziell abwickeln zu können. Würde die Schweiz eine Strafandrohung
für falsche Flugpassagierdaten ins Gesetz aufnehmen, wäre sie weltweit das einzige
Land, das eine solche Sanktionsmöglichkeit im Zusammenhang mit Flugpassagierdaten
einführt.

Sekretariat:

Kapellenstrasse 14
Postfach

CH-3001 Bern

T +41 (0)58 796 98 90

F +41 (0)58 796 99 03

info@aerosuisse.ch

www.aerosuisse.ch

Zusammenfassend betont die AEROSUISSE, dass grundsätzlich nur Daten erhoben werden, die im Zusammenhang mit der Bekämpfung von Terror und Kriminalität in Verbindung stehen. Die Erhebung von zu vielen Daten ohne Zusammenhang mit der Sicherheit führt bei Airlines und Passagieren zu zusätzlichem Zeit- und Kostenaufwand. Diesen gilt es zu vermeiden. Konkret heisst das, dass sich die Schweiz technisch an bestehenden Standards orientiert, damit die benötigten Daten von im Einsatz stehenden Systemen bei den Fluggesellschaften ohne viel zusätzlichen Aufwand generiert und den Behörden zur Verfügung gestellt werden können. Entscheidend ist, dass sich die Schweiz in punkto technischer Systeme der Datenübermittlung an bestehenden Lösungen orientiert.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und verbleiben

mit freundlichen Grüssen

AEROSUISSE
Dachverband der schweizerischen
Luft- und Raumfahrt

Der Geschäftsführer:



Philip Kristensen

Bonjour,

Nous, easyJet Switzerland SA, n'avons pas d'objection à l'implémentation des données PNR pour la Suisse. Nous le faisons déjà pour d'autres pays.

Cordialement,
Andreas Haerer

ANDREAS HAERER

security & compliance monitoring manager
easyJet Switzerland SA (EZS/DS)

contact me: andreas.haerer@easyJet.com

call me - one: +41 79 214 51 54

call me - two: +41 22 717 88 36

fly us : www.easyjet.com

holiday with us : www.easyJet/holidays

tweet us : www.twitter.com/easyJet

friend us: www.facebook.com/easyJet

follow us: www.instagram.com/easyJet



easyJet Switzerland S.A., 5 Route de l'Aéroport, 1215 Geneva 15, SWITZERLAND

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter
Postfach
3003 Bern

Versand per E-Mail: kd-rechtsabteilung@fedpol.admin.ch

Zürich-Flughafen, 22. Juli 2022

Vernehmlassung Flugpassagierdatengesetz (FPG) – Stellungnahme SWISS

Sehr geehrte Frau Bundesrätin,
sehr geehrte Damen und Herren

Besten Dank für die Einladung zum Vernehmlassungsverfahren für den Entwurf des Bundesgesetzes über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (E-FPG). Gerne übermitteln wir Ihnen die nachfolgenden Anliegen und Bemerkungen.

Swiss International Air Lines AG (SWISS) erfasst und bearbeitet im Rahmen ihrer Geschäftstätigkeit eine Vielzahl von Daten von und über die Fluggäste, die mit unserer Fluggesellschaft reisen. Als global agierendes Unternehmen haben wir dabei jeweils stets die einschlägigen gesetzlichen Vorgaben der betroffenen Jurisdiktionen zu beachten, insbesondere auch in Bezug auf Datenschutz. SWISS anerkennt, dass die erfassten Daten – namentlich auch die von Erlass ins Recht gefassten PNR-Daten – für Ermittlungsbehörden von grosser Bedeutung sein können, wenn es darum geht, Terror und andere schwere Straftaten abzuwehren und zu bekämpfen. Bisher fehlte in der Schweiz eine ausreichende gesetzliche Grundlage dafür, weshalb SWISS mit Blick auf geltende Datenschutzbestimmungen im Ausland regelmässig die gewünschten Daten nicht zur Verfügung stellen konnte. Mit dem E-FPG wird diese Lücke geschlossen. SWISS begrüsst diese gesetzliche Grundlage, die helfen wird, die Zusammenarbeit mit den schweizerischen Strafverfolgungsbehörden künftig deutlich zu erleichtern.

Wesentlich für die Umsetzung des FPG im Alltag ist, dass sich die Schweiz bezüglich technischer Übermittlungssysteme an etablierten Lösungen orientiert. Das reduziert das Risiko für die Fluggesellschaften, dass es bei der Datenübermittlung an die Behörden zu technischen Problemen kommt. Insbesondere werden damit aber auch unnötige Zusatzkosten zulasten der Fluggesellschaften vermieden, was für die Branche nach der bisher mit Abstand schwersten wirtschaftlichen Krise, ausgelöst durch die Corona-Pandemie, von grosser Bedeutung ist. SWISS begrüsst denn auch die beabsichtigte Schaffung eines «single window», das eine einzige Schnittstelle zur Übermittlung der API und PNR Daten ermöglichen soll.

In Bezug auf die administrativen Sanktionen (Art. 23 ff. E-FPG) enthält der Entwurf eine rechtlich problematische Bestimmung. Gemäss Art. 23 Abs. 2 lit. b. kann eine Fluggesellschaft administrativ sanktioniert werden, wenn «offensichtlich falsche Daten übermittelt werden». SWISS beantragt die ersatzlose Streichung von Art. 23 Abs. 2 lit. b. E-FPG.

PNR-Daten werden von den Fluggesellschaften vornehmlich für die kommerzielle Abwicklung einer Flugbuchung verwendet. Erfasst werden die Daten durch die Agenten, welche die Buchung erstellen, oder durch die Fluggäste selbst. Eine Fluggesellschaft hat keine Möglichkeit, PNR Daten zu verifizieren. Aus diesem Grund und auch mit Blick auf die enormen Datenmengen, die täglich verarbeitet werden, ist es rechtlich nicht haltbar, wenn die übermittelnden Fluggesellschaften für falsche und/oder fehlerhafte Daten zur Rechenschaft gezogen werden und dafür haften sollen. Diese Bestimmung ist weder zweckmässig noch sachgerecht und überschießt deutlich. Ferner kennt kein anderer

Staat, der die Fluggesellschaften zur Übermittlung von PNR-Daten verpflichtet, eine solche Sanktionsbestimmung für eine Pflichtverletzung durch Übermittlung «offensichtlich falscher Daten». Es würde sich um einen Schweizer Sonderfall handeln, der weder rechtlich noch sachlich begründbar ist. Angesichts dieser Ausgangslage würde es SWISS ausserordentlich begrüessen, wenn Art. 23 Abs. 2 lit. b E-FPG ersatzlos gestrichen wird.

Wir bedanken uns für die wohlwollende Prüfung unserer Anträge und Anliegen. Gerne stehen wir Ihnen für Fragen zur Verfügung.

Freundliche Grüsse

Swiss International Air Lines AG

A handwritten signature in blue ink, consisting of several overlapping loops and a long horizontal stroke extending to the right.

Ronald Abegglen
Public Affairs
Advisor to the CEO

fedpol
Bundesamt für Polizei
Guisanplatz 1A
CH-3003 Bern

Die Eingabe dieser Stellungnahme
erfolgt per E-Mail an:
kd-rechtsabteilung@fedpol.admin.ch

Zürich, 28. Juli 2022

Stellungnahme im Rahmen der Vernehmlassung zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG)

Sehr geehrte Damen und Herren

Wir beziehen uns auf die titelerwähnte Vernehmlassung und bedanken uns für die Inkludierung unseres Verbandes in die Liste der zur Stellungnahme eingeladenen Organisationen. Die durch unseren Verband vertretenen Flugplätze wären mit dem Erlass des FPG indirekt – das heisst, über deren Flugplatznutzer (in der Terminologie des FPG als «Luftverkehrsunternehmen» bezeichnet) – betroffen. Wir nehmen zur Kenntnis, dass nicht als Luftverkehrsunternehmen gilt, was unter die sogenannte Leichtaviatik fällt. Dazu gehören Schul-, Übungs- und Kontrollflüge, Touristikflüge, Luftsport sowie Privatflüge.¹ Vor diesem Hintergrund reichen wir die vorliegende kurze Stellungnahme mit den folgenden Punkten ein:

1. Die Schweiz verfügt derzeit nicht über ein Informationssystem für die Bearbeitung von PNR. Gemäss der bei der Umsetzung des PNR-Systems in der Schweiz gewählten PUSH-Methode soll auf technischer Ebene ein «single window» definiert werden. Zu begrüssen ist, dass damit den Luftverkehrsunternehmen unnötiger Aufwand erspart werden soll. Bedauerlich ist, dass der vorliegende Entwurf ohne nähere Angaben auf den Inhalt der zugehörigen Verordnung ergeht. Somit ist die Einschätzung der Auswirkungen auf die Luftverkehrsunternehmen nicht ausreichend möglich.

¹ Hingegen sollen als Luftverkehrsunternehmen gemäss FPG gelten: "Inländische oder ausländische Unternehmen mit einer Betriebsbewilligung oder einer anderen gleichwertigen Bewilligung, die sie zur gewerbmässigen Beförderung von Flugpassagierinnen und -passagieren berechtigt." Diese Definition wurde in Zusammenhang mit dem vom Stimmvolk am 13.06.2021 abgelehnten CO2-Gesetz vom 25. September 2020 (Art. 2 Bst. i) entwickelt.

2. ad Art. 4 FPG "Sorgfaltspflicht": Obwohl dem Erläuterungsbericht Beispiele zu entnehmen sind, erweist sich die Sorgfaltspflicht als ein dehnbarer Begriff. Somit ist die Einschätzung der Auswirkungen auf die Luftverkehrsunternehmen nicht ausreichend möglich.
3. ad Art. 23 Abs. 5 FPG "Sanktionen bei Pflichtverletzungen durch Luftverkehrsunternehmen": Weil die Verletzung der Sorgfalts- und der Informationspflicht nach den Artikeln 4 und 5 FPG unabhängig von einem Verschuldensnachweis geahndet werden soll, ergeben sich mitunter schwer abschätzbare Risiken für das einzelne Luftverkehrsunternehmen. Auf die Risiken wird auch nicht unter Kapitel 6 "Rechtliche Aspekte" im Erläuterungsbericht eingegangen.

Wir regen an, die obigen Punkte bei der weiteren Bearbeitung des FPG in Erwägung zu ziehen, verweisen dabei auch auf die Expertise der Swiss Business Aviation Association, SBAA und bedanken uns für die Kenntnisnahme.

Der Unterzeichnende steht bei Rückfragen zu Ihrer Verfügung.

Mit freundlichen Grüßen

VERBAND SCHWEIZER FLUGPLÄTZE



Jorge V. Pardo, Geschäftsführer

Kopie:

Swiss Business Aviation Association, SBAA, Sekretariat, 8060 Zürich-Flughafen

Beilagen: NIL

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

Per Email an
kd-rechtsabteilung@fedpol.admin.ch

Zürich-Flughafen, 25. Juli 2022

Vernehmlassung über das Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten - Stellungnahme

Sehr geehrte Frau Weber, sehr geehrter Herr Matthys

Mit Schreiben vom 13. April 2022 hat Frau Bundesrätin Karin Keller-Sutter interessierte Kreise zur Teilnahme an der erwähnten Vernehmlassung eingeladen. Gerne nehmen wir die Gelegenheit wahr, unsere Anliegen zur Einführung eines Flugpassagierdatengesetzes zur Bekämpfung von terroristischen und anderen schweren Straftaten zu äussern. Die Flughafen Zürich AG ist Eigentümerin und Betreiberin des grössten Landesflughafens mit über 30 Millionen Passagieren im Jahr (vor der Pandemie).

Die Flughafen Zürich AG begrüsst das geplante Flugpassagierdatengesetz und unterstützt die Vorlage als international harmonisiertes Instrument, mit dem die Schweiz Terrorismus und schwere Straftaten bekämpfen kann. In diesem Zusammenhang verweisen wir auf die Stellungnahme des Dachverbandes der Schweizerischen Luftfahrt Aerosuisse, die wir ebenfalls unterstützen.

Wichtig erscheint uns, dass das neue Gesetz keine operationellen Auswirkungen auf Flughäfen und den Betrieb eines Drehkreuzes mit kurzen Umsteigeverbindungen hat, wie sie am Flughafen Zürich vorgefunden werden. Insbesondere sollen längere Wartezeiten im Check-In und Boarding-Prozess vermieden werden, indem die Daten bereits bei der Buchung erhoben werden müssen. Damit kann der Flughafen Zürich die Vorgabe des Bundes, den Betrieb eines Drehkreuzes zu ermöglichen, weiterhin erfolgreich erfüllen (Luftfahrtpolitischer Bericht 2016). Dieses wird durch den Hub-Carrier SWISS gewährleistet. Mit einem Drehkreuz verbunden ist eine hohe Anzahl an Passagieren, die den Flughafen Zürich lediglich als Umsteige-Flughafen nutzt. Diese Fluggäste schätzen den Flughafen aufgrund der kurzen Wege und Umsteigezeit.

Das bedeutet auch, dass jegliche Massnahmen im Zusammenhang mit Flugpassagierdaten international koordiniert sein müssen und die Wettbewerbsfähigkeit der Schweizer Luftfahrt nicht einschränken dürfen. Einerseits soll die Schweiz internationale Standards erfüllen, um den Zugang zu Direktverbindungen zwischen der Schweiz und dem Ausland weiterhin zu gewährleisten. Andererseits sollen lediglich diejenigen Daten erhoben werden, die nötig sind, um die Meldepflicht im Ausland zu erfüllen. Unverhältnismässige Auflagen, die über internationale Standards hinausgehen, werden abgelehnt. Es gilt zu verhindern, dass im internationalen Reiseverkehr zusätzliche und möglicherweise wettbewerbs-hemmende Hindernisse für die Schweiz geschaffen werden.

Wir danken Ihnen für die Berücksichtigung unseres Anliegens und stehen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse



David Karrer
Leiter Public Affairs



Andrew Karim
Stv. Leiter Public Affairs



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

Eidgenössisches Justiz- und Polizeidepartement EJPD

Per E-Mail

kd-rechtsabteilung@fedpol.admin.ch

Bern, 20. Juli 2022

05.08 dub.

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten; Stellungnahme

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

Mit Schreiben vom 13. April 2022 haben Sie uns eingeladen, zur erwähnten Vorlage Stellung zu nehmen. Hierfür danken wir Ihnen bestens.

Wie wir Ihnen bereits mit Schreiben vom 1. Juli 2019 mitgeteilt haben, erachtet die KKJPD die Möglichkeit, Flugpassagierdaten in der Bekämpfung von Terrorismus und Schwerstkriminalität zu nutzen, für sinnvoll und notwendig. Namens und Auftrags unseres Vorstands darf ich Ihnen mitteilen, dass wir die nun vorgeschlagene gesetzliche Umsetzung begrüssen. Dies gilt auch für den Vorschlag der Ansiedelung der „PIU“ bei fedpol sowie für die zwischen fedpol und der Konferenz der kantonalen Polizeikommandantinnen und -kommandanten verhandelte Beteiligung der Kantone an eben dieser Stelle im Rahmen des Entsendemodells.

Mit bestem Dank für die gute Zusammenarbeit und

freundlichen Grüssen

Florian Düblin
Generalsekretär



KKPKS
CCPCS

Konferenz der kantonalen Polizeikommandantinnen und – kommandanten
Conférence des commandantes et des commandants des polices cantonales
Conferenza delle e dei comandanti delle polizie cantonali

Der Präsident

Eidgenössisches Justiz- und Polizeidepartement
EJPD

Per E-Mail:
kd-rechtsabteilung@fedpol.admin.ch

Bern, 24. Mai 2022

Vernehmlassungsantwort der KKPKS zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten

Sehr geehrte Frau Bundesrätin

Sehr geehrte Damen und Herren

Die Konferenz der Kantonalen Polizeikommandanten der Schweiz (KKPKS) bedankt sich für die Möglichkeit, zu oben genannter Vernehmlassung Stellung nehmen zu können.

Die KKPKS begrüsst die vorgesehene Einführung der systematischen Bearbeitung von Flugpassagierdaten zur Unterstützung der Verhinderung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten sehr. Weiter ist es aus unserer Sicht richtig, für die dafür benötigten Rechtsgrundlagen ein neues Gesetz zu schaffen. Auch stimmen wir der Gesetzesvorlage in Bezug auf die technologieneutrale Formulierung zu, womit auf zukünftige technologische Entwicklungen auch ohne die Notwendigkeit einer Gesetzesrevision reagiert werden kann. Diesbezüglich wird die in Art. 2 Abs. 4 festgelegte Zuordnung der Festlegung der technischen Einzelheiten der Übermittlung ans Bundesamt für Polizei (fedpol) gutgeheissen.

Weiter befürworten wir seitens KKPKS die in der Vernehmlassungsvorlage vorgesehene organisatorische Ansiedelung der PIU beim Bund. Erneut möchten wir unsere Bereitschaft zur personellen Beteiligung an der PIU sowie zur Ausarbeitung einer entsprechenden Vereinbarung bestätigen. Wir unterstützen das vorgesehene Entsendemodell, wonach sich die PIU je hälftig aus Mitarbeitenden des Bundes und der Kantone zusammensetzt und die entsendende Behörde dafür die Kosten trägt. Wie in der Vernehmlassungsvorlage erwähnt, erlaubt dieses Entsendemodell einen Kompetenztransfer von der PIU in die Kantone, welcher insbesondere für das Konzipieren von Risikoprofilen und Beobachtungslisten nützlich sein kann.

Abschliessend kann festgehalten werden, dass die KKPKS die Vernehmlassungsvorlage vollumfänglich unterstützt und für die Ausarbeitung der genannten Vereinbarung zwischen dem Bund und den Kantonen zur Verfügung steht.



KKPKS
CCPCS

Konferenz der kantonalen Polizeikommandantinnen und – kommandanten
Conférence des commandantes et des commandants des polices cantonales
Conferenza delle e dei comandanti delle polizie cantonali

Der Präsident

Besten Dank für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

Der Präsident

Mark Burkhard, Kdt Polizei Basel-Landschaft

Kopie z.K.:

- Mitglieder der KKPKS
- GS KKJPD



VSPB · FSFP

Verband Schweizerischer Polizei-Beamter
Fédération Suisse Fonctionnaires de Police
Federazione Svizzera Funzionari di Polizia

Geht an
Bundesamt für Polizei fedPol
media@fedpol.admin.ch

Luzern, 29. August 2022

Vernehmlassungsantwort des Verbandes Schweizerischer Polizei-Beamter zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten – 2021/80

Sehr geehrter Herr Bundesrat

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Möglichkeit zur Stellungnahme zum vorgeschlagenen Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten. Wir entschuldigen uns für die verspätete Antwort und hoffen trotzdem auf die Annahme unserer Stellungnahme.

Der Verband Schweizerischer Polizei-Beamter VSPB vertritt 59 Sektionen mit insgesamt über 26'500 Mitglieder. Davon sind fast 20'000 im aktiven Polizeidienst für Gemeinden, Kantone und Bund, was zu einem Deckungsgrad des VSPB von 95% aller Polizistinnen und Polizisten führt.

Mit dem Flugpassagierdatengesetz kann die Schweiz künftig ein international bewährtes Instrument zur Bekämpfung von Terrorismus und schweren Straftaten einsetzen. Der VSPB begrüsst eine solche Vorgabe, da die Kriminalität auch die Schweiz betrifft.

Ohne die nötigen Instrumente wird demzufolge eine gute und starke Fahndung in Frage gestellt und somit auch die Innere Sicherheit der Schweiz gefährdet. Wir sind uns bewusst, dass dies ein Eingriff in die Privatsphäre der Passagiere ist. Im Endeffekt ist es jedoch ein kleiner Verlust, wenn man dies dem hohen Risiko von schweren Straftaten gegenüberstellt.

Dieses Vorgehen ist schon seit rund 20 Jahren, namentlich in den USA, Kanada sowie im Vereinigten Königreich und seit rund 10 Jahren in den meisten Mitgliedstaaten der EU im Einsatz. Das heisst, dass die Schweiz mit diesem Gesetz endlich ihren internationalen Verpflichtungen nachkommt.

Die Flugpassagierdaten werden automatisch nach Ablauf von sechs Monaten pseudonymisiert und nach insgesamt fünf Jahren gelöscht. Dies scheint eine lange Zeit zu sein, gibt aber dem Instrument die nötige zeitliche Sicherheit.

Was der VSPB aber kritisch hinterfragt ist der Entscheid, dass die Hälfte der Mitarbeitenden, die bei der PIU tätig sein sollte von den Kantonen entsendet und von diesen finanziert werden sollen. Dies können wir nur akzeptieren, wenn Massnahmen getroffen werden, damit das nötige Personal neu rekrutiert wird. Weiterhin die knappen Ressourcen in den kantonalen Polizeikörpern zu verpflichten ist eben auch ein Risiko für die innere Sicherheit der Schweiz.



VSPB · FSFP

Verband Schweizerischer Polizei-Beamter
Fédération Suisse Fonctionnaires de Police
Federazione Svizzera Funzionari di Polizia

Der VSPB unterstützt demzufolge diese Vorlage und wird sich konsequent im Rahmen der eventuellen Kampagne auch dafür einsetzen.

Für die Aufnahme und Berücksichtigung unserer Position danken wir Ihnen bestens.

Freundliche Grüsse

Max Hofmann

Generalsekretär VSPB

Eidgenössisches Justiz- und Polizeidepartement
EJPD

Per E-Mail:
kd-rechtsabteilung@fedpol.admin.ch

Bern, den 21. Juli 2022

Stellungnahme zum Vorentwurf Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (FPG)

Sehr geehrte Damen und Herren

Mit Schreiben vom 21. Juni 2022 haben Sie unsere Konferenz per Mail nachträglich eingeladen, zur erwähnten Vorlage Stellung zu nehmen. Hierfür danken wir Ihnen bestens.

Die SSK befürwortet die vorgesehene Einführung der systematischen Bearbeitung von Flugpassagierdaten zur Unterstützung der Verhinderung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten ausdrücklich.

Weiter begrüssen wir es sehr, dass die Vorlage technologieneutral formuliert ist, damit auf zukünftige technologische Entwicklungen auch ohne Gesetzesrevisionen reagiert werden kann.

Auf folgende, wenige Punkte im Vorentwurf zum FPG möchten wir dennoch gerne im Einzelnen eingehen:

PNR-Deliktskategorien (Art. 6 i.V.m. Anhang 2):

Art. 6 i.V.m. Anhang 2 regelt, welche Straftaten vorliegen müssen, damit eine Datenbearbeitung zulässig ist.

Gemäss **Art. 6 Abs. 2** gelten als terroristische Straftaten solche, welche in Anhang 1 Ziff. 22 des Schengen-Informationsaustausch-Gesetzes vom 12. Juni 2009 (SlaG; SR 362.2) enthalten sind. Ziffer 22 enthält jedoch nur den Straftatbestand der Finanzierung des Terrorismus (Art. 260quinquies StGB). Gemäss erläuterndem Bericht gelten auch die Tatbestände nach Art. 1-4 des Rahmenbeschlusses des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (Rahmenbeschluss 2002/475/JI) als terroristische Straftaten. Diese decken sich mit Anhang 1a der N-SIS-Verordnung. Entsprechend muss für die Definition der terroristischen Straftaten auf Anhang 1a N-SIS-Verordnung verwiesen werden.

Art. 6 Abs. 3 lit. a und b FPG:

Es ist stossend, dass die Bearbeitung von PNR-Daten gemäss lit. a nur bei Straftaten mit einer Strafandrohung von mehr als drei Jahren (also ausschliesslich Verbrechen) und bei "Zolldelikten" gemäss lit. b bei Verbrechen **und** Vergehen erlaubt sein soll.

Wir beantragen deshalb, sowohl für lit. a und lit. b eine maximale Freiheitsstrafe von mindestens 3 Jahren (also Verbrechen und Vergehen) vorzusehen.

Art. 6 lit. a ist zu eng gefasst, weil zum Beispiel bei Betäubungsmitteldelikten zu Beginn der Ermittlungen oft nicht klar ist, ob der Tatvorwurf auf ein Verbrechen oder "nur" ein Vergehen lautet. Dies könnte dazu führen, dass sich die Bearbeitung von PNR-Daten im Nachhinein als unzulässig erweist. Die Kriminalität im Bereich von Betäubungsmitteldelikten ist jedoch hochgradig organisiert: So werden auf den allermeisten Flügen nicht die Haupttäter verhaftet, sondern Betäubungsmittelkurier als Gehilfen. Deren Verhaftung ist in der Bekämpfung der organisierten Kriminalität im Betäubungsmittelbereich zentral: Insbesondere dadurch können die Strafverfolgungsbehörden Netzwerke und Organisationen aufdecken und letztlich auch bekämpfen. Die Bearbeitung von Flugpassagierdaten gibt den Ermittlern ein effektives Mittel zur Erkennung der Abläufe in die Hand. Ähnlich verhält es sich in anderen Bereichen der organisierten Kriminalität, zum Beispiel beim Menschenschmuggel. Diesem Umstand trägt der Deliktskatalog zu wenig Rechnung. Entsprechend ist für die Definition der anderen schweren Straftaten auf den Deliktskatalog von Anhang 1b N-SIS-Verordnung zu verweisen.

Art. 11 FPG:

Der Erläuternde Bericht schränkt die Möglichkeit der Abfragen ein und verbietet "Generische Abfragen, die nicht spezifiziert sind und zu einer Vielzahl von unterschiedlichsten Suchergebnissen führen können". Diese Einschränkung findet im Gesetzeswortlaut aber keinerlei Grundlage. Nur schon deshalb ist sie aus dem Erläuternden Bericht zu entfernen. Zudem ist die Formulierung im Erläuternden Bericht selbst sehr unspezifisch und kaum praktikabel (was ist eine Vielzahl unterschiedlichster Ergebnisse?). Es muss aus Sicht der SSK möglich sein, beispielsweise alle Passagiere eines bestimmten Fluges abzufragen.

Art. 12 FPG (betrifft nur die deutsche Version):

Der Begriff "konkreter Verdacht" in Abs. 1 ist pleonastisch, ein Verdacht ist immer konkret. Ausserdem gibt es diese Kategorie im Strafrecht sonst auch nicht (prozessual richtig ist der Anfangsverdacht, der hinreichende Tatverdacht und der dringende Tatverdacht). Unseres Erachtens ist die Schwelle aber zu hoch, für eine solche Meldung überhaupt einen Verdacht zu verlangen. Es müsste genügen, wenn "Hinweise" oder "Anhaltspunkte" für eine solche Straftat vorliegen. Ein Verdacht wird ja auch für eine Abfrage durch eine Strafverfolgungsbehörde gem. Art. 11 FPG nicht verlangt.

Es wäre daher wenig zielführend, einen Verdacht für eine Spontanmitteilung durch die PIU zu verlangen. Falls am Verdacht für eine Spontanmitteilung festgehalten wird, muss aus der deutschen Version das "konkret" gestrichen werden in "wenn ein Verdacht besteht".

Art. 22 Abs. 3 FPG (betrifft nur die deutsche Version):

Daten sollen an eine ausländische PIU nicht übermittelt werden dürfen, wenn "gegen die betreffende Person kein begründeter Verdacht vorliegt". In Art. 12 FPG ist von einem "konkreten" Verdacht die Rede, bei Art. 22 FPG braucht es nun einen "begründeten" Verdacht. Auch dieser Begriff kein terminus technicus im oben dargelegten Sinne, der zu Verwirrung oder Auslegungsproblemen führt, weshalb er zu streichen ist.

Auch hier gilt wie bei Art. 12: Die deutsche Version ist der französischen Version " pas lieu de soupçonner que." anzugleichen in "wenn gegen die betreffende Person kein Verdacht vorliegt."

Wir danken Ihnen bestens für die Berücksichtigung unserer Anliegen.

Mit freundlichen Grüßen



Michel-André Fels
Präsident SSK-CPS

Sehr geehrter Herr Dolder

Namens der Schweizerischen Kriminalistischen Gesellschaft danke ich Ihnen für die Einladung zur Vernehmlassung. Die Vorlage scheint uns unbestritten, weshalb wir auf eine Vernehmung verzichten.

Besten Dank für Ihre Kenntnisnahme.

Freundliche Grüsse
Martina Weber

SKG | **Schweizerische Kriminalistische Gesellschaft**
SSDP | **Société Suisse de droit pénal**
Società svizzera di diritto penale

Die Sekretärin: lic.iur. Martina Weber
c/o Staatsanwaltschaft des Kantons Zug
An der Aa 4, 6300 Zug
041 728 46 00
www.skg-ssdp.ch

Bundesamt für Polizei (fedpol)
Guisanplatz 1A
3003 Bern

Per Mail:
kd-rechtsabteilung@fedpol.admin.ch

Bern, 31. Juli 2022

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten; Vernehmlassungsverfahren

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zum Vorentwurf eines neuen Gesetzes über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG) Stellung nehmen zu können. Aus datenschutzrechtlicher Sicht ergeben sich folgende Hinweise:

1. Allgemeine Bemerkungen

Das neue FPG soll die Rechtsgrundlage für die Bearbeitung (inkl. Analyse) von Flugpassagierdaten schaffen, wobei sich die Nutzung der Daten durch die *Passenger Information Unit* (PIU) in zwei Schritte bzw. Ausprägungen unterscheiden lässt:

- a) den automatischen Abgleich der Flugpassagierdaten mit Daten aus polizeilichen Informationssystemen unmittelbar nach dem Erhalt von den Luftverkehrsunternehmen (Art. 7 VE-FPG) sowie den Abgleich mit von der PIU selbst erstellten Risikoprofilen und Beobachtungslisten (Art. 9 VE-FPG);
- b) die Aufbewahrung aller Flugpassagierdaten auf Vorrat und die Übermittlung von Daten im Einzelfall an bestimmte andere Behörden (Art. 11 VE-FPG) auf deren Antrag hin.

Die Ausprägung a) gleicht der Automatischen Fahrzeugfahndung (AFV), wo Kontrollschilder automatisiert erfasst und mit polizeilichen Datenbanken abgeglichen werden, wobei die Daten ohne Treffer (sog. «no hits») i.d.R. sofort oder innert kürzester Zeit wieder gelöscht werden. Letzteres geschieht hier wegen der zusätzlichen Ausprägung b), die ihrerseits an die Videoüberwachung zur Ahndung von Straftaten erinnert, nicht. Allen Fällen ist gemeinsam, dass die Daten einer sehr grossen Mehrzahl von Personen, welche weder Störer noch

Täter oder Tatverdächtige sind, erfasst und weiterverarbeitet werden. Schon allein für die AFV ohne weitere Aufbewahrung aller Daten während fünf Jahren stellte das Bundesgericht im [Urteil 6B_908/2018](#) fest, dass ein schwerer Eingriff in das Grundrecht auf informationelle Selbstbestimmung vorliegt (E. 3.2.).

Sofern der Gesetzgeber grundsätzlich ein überwiegendes öffentliches Interesse an der systematischen Beschaffung und weiteren Bearbeitung aller Flugpassagierdaten als gegeben erachtet, so sind der Eingriffsintensität entsprechend hohe Anforderungen an die Massnahmen zum Schutz der Daten gegen missbräuchliche Verwendung zu stellen.

2. Zu einzelnen Bestimmungen

a. Art. 9 VE-FPG

Während der Abgleich mit Daten aus polizeilichen Informationssystemen unmittelbar nach Erhalt der Daten von den Luftverkehrsunternehmen erfolgen muss (Art. 7 Abs. 2 VE-FPG) und automatisch erzielte Übereinstimmungen vor ihrer Übermittlung an die zuständige Behörde manuell auf ihre Plausibilität hin zu überprüfen sind (Art. 7 Abs. 3 VE-FPG), fehlen entsprechende Vorgaben für den Datenabgleich mit von der PIU erstellten Risikoprofilen und Beobachtungslisten. Auch dieser Abgleich muss u.E. unmittelbar nach Erhalt der Daten erfolgen und kann nicht nach Belieben der PIU wiederholt werden, solange die Daten nicht pseudonymisiert wurden. Zudem sind auch hier Treffer zu plausibilisieren, bevor die Daten an andere Behörden übermittelt werden, damit Betroffene nicht zu Unrecht in Verdacht geraten (vgl. zu diesem Risiko auch den zitierten Bundesgerichtsentscheid). Diese Schranken sind im Gesetz zu statuieren und nicht zur Regelung an den Bundesrat zu delegieren.

b. Art. 13 VE-FPG

Betreffend technische und organisatorische Massnahmen zum Schutz der Flugpassagierdaten werden nur – aber immerhin – die Zugriffsrechte auf die Daten im Informationssystem *Passenger-Name-Record* (PNR-System) geregelt. Zudem ist vorgeschrieben, dass die Daten nach sechs Monaten automatisch pseudonymisiert werden. Mit Blick auf die Datenmenge und das damit verbundene Missbrauchspotenzial halten wir es für erforderlich, dass der Bundesrat weitere Anforderungen an die Datensicherheit festlegt. Im Vorentwurf für ein BG über die Mobilitätsdateninfrastruktur (VE-MODIG), in der nur ausnahmsweise Personendaten bearbeitet werden sollen, verlangt das Gesetz selbst die Gewährleistung der Datensicherheit und beauftragt den Bundesrat, die Anforderungen an die Sicherheit der Daten festzulegen (Art. 9 Abs. 1 Bst. g und Abs. 2 VE-MODIG; vgl. [Vernehmlassungsunterlagen](#)). Für ein Informationssystem wie das PNR-System muss dies erst recht gelten, weshalb auch im FPG eine entsprechende Regelung aufzunehmen ist.

c. Art. 20 VE-FPG

In Art. 20 Abs. 3 VE-FPG wird festgehalten, dass das Personal der PIU Informationen, über die sie im Zusammenhang mit ihrem Einsatz Kenntnis erlangen, nur zur Erfüllung ihrer Aufgaben bei der PIU verwenden dürfen; laut dem Erläuternden Bericht soll damit die Pflicht zur Verschwiegenheit statuiert werden (S. 39). Nach unserem Verständnis adressiert der Wortlaut von Art. 20 Abs. 3 VE-FPG jedoch eher den datenschutzrechtlichen Grundsatz der Zweckbindung (vgl. Art. 6 Abs. 3 des neuen Datenschutzgesetzes) und keine Geheimhaltungspflicht. Gerade wenn die Verschwiegenheitspflicht auch gegenüber dem vertraglichen Arbeitgeber der Mitarbeitenden der PIU gelten soll – was wir als sachgerecht erachten –,

so erscheint es uns als sinnvoll, dies im Gesetz unmissverständlich festzuhalten. Nur wenn die Geheimhaltungspflicht im Gesetz klar statuiert ist, lässt sich daraus auch ableiten, dass ihre Verletzung eine Amtsgeheimnisverletzung im Sinne von [Art. 320 StGB](#) darstellt und als solche sanktioniert wird.

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

Freundliche Grüsse

Ueli Buri
Präsident privatim



Schweizerischer Anwaltsverband
Fédération Suisse des Avocats
Federazione Svizzera degli Avvocati
Swiss Bar Association

Eidgenössisches Justiz- und Polizeidepartement
(EJPD)
Bundesamt für Polizei (Fedpol)
Guisanplatz 1A
3003 Bern

Per Email versandt:

kd-rechtsabteilung@fedpol.admin.ch

Bern, der 26. Juli 2022

Stellungnahme des Schweizerischen Anwaltsverbands (SAV-FSA) zum Vorentwurf des Bundesgesetzes über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG)

Sehr geehrter Frau Bundesrätin,

Sehr geehrte Damen und Herren

Der Schweizerische Anwaltsverband bedankt sich für die Einladung zum oben genannten Vernehmlassungsverfahren und nimmt nachfolgend Stellung.

Der SAV lehnt den vorliegenden Entwurf für das neue Flugpassagierdatengesetz (FPG) ab. Der SAV fordert den Bundesrat auf, einen neuen Entwurf vorzulegen, der insbesondere die aktuelle europäische Rechtsprechung berücksichtigt sowie das anwaltliche Berufsgeheimnis ausdrücklich schützt.

Das FPG legalisiert die bestehende Massenüberwachung von bereits vielen Flugpassagieren und dehnt diese auf alle Flugpassagiere aus. Die Massenüberwachung aller Flugpassagiere mit entsprechender Vorratsdatenspeicherung erfolgt ohne Anlass und Verdacht. Dabei kollidiert bereits die bestehende strafprozessuale Vorratsdatenspeicherung, wie sie in vielen europäischen Staaten von höchsten Gerichten für unzulässig erklärt wurde, mit den Grund- und Menschenrechten, untergräbt aber auch das Anwaltsgeheimnis sowie weitere gesetzlich geschützte Berufsgeheimnisse. Die bestehende strafprozessuale Vorratsdatenspeicherung mit einer Speicherdauer von sechs Monaten ist Gegenstand eines Verfahrens am Europäischen Gerichtshof für Menschenrechte (EuGH). Das FPG sieht sogar eine Vorratsdatenspeicherung mit einer Speicherdauer von fünf Jahren vor.

Der SAV verweist bei seiner Ablehnung insbesondere auf das Urteil C-817/19 des Europäischen Gerichtshofes (EuGH) vom 21. Juni 2022.¹ Das Urteil ist von erheblicher Bedeutung für die Schweiz, nachdem das FPG inhaltlich ausdrücklich auch mit dem einschlägigen europäischen Recht begründet wird. Die Schweiz zählt nicht nur zum europäischen Sicherheitsraum, insbesondere mit den Schengener Abkommen, sondern auch zum europäischen Grundrechtsraum gemäss der Europäische Menschenrechtskonvention.

Der EuGH hielt im erwähnten Urteil fest, dass die *«Achtung der Grundrechte eine Beschränkung der in der PNR-Richtlinie vorgesehenen Befugnisse auf das absolut Notwendige»* erfordert. Die Überwachung aller Flüge ist gemäss dem EuGH nur *«in einer Situation [zulässig], in der es nach der Einschätzung des betreffenden Mitgliedstaats hinreichend konkrete Umstände für die Annahme gibt, dass er mit einer als real und aktuell oder vorhersehbar einzustufenden terroristischen Bedrohung konfrontiert ist»* und dabei *«die Grenzen des absolut Notwendigen nicht überschritten»* werden.

Und: *«Ohne eine solche terroristische Bedrohung darf die Anwendung der Richtlinie nicht auf alle EU-Flüge ausgedehnt werden, sondern muss sich auf EU-Flüge beschränken, die etwa bestimmte Flugverbindungen, bestimmte Reismuster oder bestimmte Flughäfen betreffen, für die es nach der Einschätzung des betreffenden Mitgliedstaats Anhaltspunkte gibt, die eine Anwendung der Richtlinie rechtfertigen können. Die absolute Notwendigkeit ihrer Anwendung auf die ausgewählten EU-Flüge muss nach Maßgabe der Entwicklung der Bedingungen, die ihre Auswahl gerechtfertigt haben, regelmäßig überprüft werden.»*

Im Hinblick auf den geforderten neuen Entwurf nehmen wir zum vorliegenden Entwurf dennoch Stellung, um handwerkliche und inhaltliche Fehler und Probleme sowie mögliche Anpassungen und Verbesserungen bereits zum jetzigen Zeitpunkt aufzuzeigen. Der vorliegende Entwurf wird aufgrund der neuen europäischen Rechtsprechung grundlegend überdacht werden müssen.

¹ Urteil: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62019CJ0817> ;

Medienmitteilung auf Deutsch: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220105de.pdf> ;

Medienmitteilung auf Französisch: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220105fr.pdf>.

Bemerkungen zu einzelnen Artikeln des VE-FPG

	Antrag Proposition	Begründung / Bemerkungen Justification / Remarques
Art. 1 lit. a / b FPG	Umgekehrte Reihenfolge von lit. a und lit. b	Die Litera sollten der Reihenfolge bzw. Systematik im Gesetz entsprechen, das heisst, zuerst die Pflichten der Luftfahrtunternehmen (2. Abschnitt) und danach die Bearbeitung von Daten (3. Abschnitt) und schliesslich die PIU (6. Abschnitt)
Art. 2 Abs. 3 FPG	Ergänzung: «[...] <i>keine besonders schützenswerten Personendaten nach Artikel 5 Buchstabe c des Datenschutzgesetzes (DSG) vom 25. September 2020 übermitteln.</i> »	Mit dem Verweis auf das neue Datenschutzgesetz wird klargestellt, dass das FPG keine eigene Definition von «besonders schützenswerten Personendaten» kennt.
Art. 2 Abs. 4 FPG	Ergänzung: « <i>Die Übermittlung erfolgt insbesondere geschützt durch Ende-zu-Ende-Verschlüsselung. Das fedpol veröffentlicht die festgelegten technischen Einzelheiten der Übermittlung.</i> »	Ende-zu-Ende-Verschlüsselung und offengelegte Protokolle gelten als «Best Practice» um die Datensicherheit zu gewährleisten. Mit der ausdrücklichen Erwähnung in Art. 2 Abs. 2 FPG wird auf Gesetzesstufe sichergestellt, dass diese «Best Practice» auch für die Übermittlung von Flugpassagierdaten gilt.
Art. 3 FPG	Ergänzung: « <i>und die Gesetzgebung im betreffenden Staat für die Flugpassagierdaten einen angemessenen oder geeigneten Schutz gewährleistet.</i> »	Art. 16 Abs. 1 u. 2 des neuen Datenschutzgesetzes (nDSG) sehen vor, dass die Bekanntgabe von Personendaten in andere Staaten bedingt, dass die dortige Gesetzgebung einen angemessenen (Abs. 1) oder geeigneten (Abs. 2) Datenschutz gewährleistet. Mit der ausdrücklichen Erwähnung in Art. 3 FPG wird sichergestellt, dass dieser Standard, den das nDSG vorgibt, auch für Flugpassagierdaten gilt. Da in der Schweiz ausserdem Völkerrecht grundsätzlich Vorrang vor Landesrecht genießt, wird mit der ausdrücklichen Erwähnung sichergestellt, dass der Standard gemäss nDSG nicht ausgehöhlt wird.
Art. 5	Ersetzung: « <i>angemessen,</i>	Die Beschränkung auf eine schriftliche Information, das heisst grundsätzlich auf

	Antrag Proposition	Begründung / Bemerkungen Justification / Remarques
	<i>verständlich und in leicht zugänglicher Form statt «schriftlich».</i>	Papier, ist nicht zeitgemäss. Die Information sollte unabhängig vom verwendeten Kommunikationsmedium angemessen erfolgen, so wie es auch Art. 19 Abs. 1 des neuen Datenschutzgesetzes vorsieht, wobei die weitere Ergänzung <i>«verständlich und in leicht zugänglicher Form»</i> sicherstellt, dass die betroffenen Personen tatsächlich informiert werden und die Informationen beispielsweise nicht in schwer verständlichen und umfangreichen allgemeinen Geschäftsbedingungen (AGB) versteckt werden können.
Art. 6 Abs. 1–4 FPG	Ersetzung: <i>«Als terroristische und andere schwere Straftaten gelten die Straftaten gemäss Anhang 1.»</i>	Die betroffenen Straftaten sollten für Rechtssicherheit und Verständlichkeit der betroffenen Personen in einem Anhang zum Gesetz und mit Verweis auf schweizerisches Strafrecht bzw. Nebenstrafrecht ausdrücklich als Katalog aufgeführt werden. Ein Anhang genügt, so dass die vorgesehenen einzelnen Anhänge 1 und 2 durch einen einzelnen Anhang 1 ersetzt werden Der EUGH hat im erwähnten Urteil unter anderem die Anwendung der Sammlung von Passagier auf Fälle beschränkt, welche einen objektiven Zusammenhang mit Passagierflügen aufweisen, unter Ausschluss von sogenannter «üblichen Kriminalität», selbst wenn sie schwer sein sollte. Aus diesem Grund sollten folgende Deliktskategorien von Anhang 2 gemäss Entwurf ausgenommen werden sollten: 3, 4, 6, 7, 8, 9, 12, 15, 17, 18, 21, 24, 25, 26.
Art. 6 Abs. 6 FPG	Ergänzung: <i>«c. Daten gemäss Art. 2 Abs. 3 FPG, um sie zu löschen.»</i>	Gemäss Art. 2 Abs. 3 FPG muss die PIU besonders schützenswerte Personendaten, die Luftverkehrsunternehmen fälschlicherweise liefern, umgehend löschen. Die Löschung stellt eine Bearbeitung von besonders schützenswerten Personendaten dar, die entsprechend ausdrücklich erwähnt werden muss.
Art. 7 Abs. 1 lit. d FPG	Streichung: <i>«oder geplanten».</i>	Litera d lässt offen, was unter «geplanten Straftaten» zu verstehen ist und der erläuternde Bericht schweigt sich dazu aus. Alternativ könnte der Begriff definiert werden.

	Antrag Proposition	Begründung / Bemerkungen Justification / Remarques
Art. 7 Abs. 2 FPG	Ergänzung: «[...] auf ihre Richtigkeit hin zu überprüfen. Das Ergebnis der Überprüfung ist zu dokumentieren. »	Die Übermittlung ihrer Daten an Behörden kann für die betroffenen Personen erhebliche Auswirkungen haben. Die Übereinstimmungen müssen deshalb nicht nur plausibel, sondern richtig sein. Auch ist das Ergebnis der Überprüfungen zu dokumentieren, damit eine wirksame Aufsicht und ein wirksamer Rechtsschutz gewährleistet sind.
Art. 7 Abs. 3 FPG	Ergänzung: «Automatisch erzielte Übereinstimmungen sind vor ihrer Übermittlung an die zuständige Behörde unverzüglich manuell [...] zu überprüfen. Die Überprüfung muss dokumentiert werden. »	Automatisch erzielte Übereinstimmungen sind wenig verlässlich, wie es der EuGH im erwähnten Urteil festgehalten hat. Auch haben automatisch erzielte Übereinstimmungen direkte rechtliche Folgen wie beispielsweise eine längere Aufbewahrungsdauer gemäss Art. 16 Abs. FPG. Daher müssen automatisch erzielte Übereinstimmungen unverzüglich manuell überprüft zu werden. Die Überprüfung muss dokumentiert werden. Dadurch wird sichergestellt, dass die Überprüfung effektiv und gewissenhaft durchgeführt wird sowie zu einem späteren Zeitpunkt überprüfbar ist. Wird zu einem späteren Zeitpunkt, insbesondere bei Ermittlungen, festgestellt, dass eine automatisch erzielte Übereinstimmung falsch war – und damit auch der daraus fließende Verdacht –, dann das falsch positive Ergebnis korrigiert werden.
Art. 8 Abs. 1 FPG	Ersetzung: Bestätigung durch eine richterliche Behörde.	Ob eine Straftat vorliegt, bestätigen in einem Rechtsstaat richterliche Behörden, wozu die PIU offensichtlich nicht zählt. Im vorliegenden Sachzusammenhang wäre eine Bestätigung durch das Bundesverwaltungsgericht naheliegend.
Art. 8 Abs. 1 lit. b FPG	Streichung von «lit. b der Nachrichtendienst des Bundes (NDB).»	Das FPG dient gemäss Art. 1 lit. a FPG der Ermittlung, Verfolgung usw. von Straftaten. Der Nachrichtendienst des Bundes ist keine Strafverfolgungsbehörde (vgl. Art. 6 NDG e contrario).
Art. 9 FPG	Streichung.	Mit diesem Art. würde eine allgemeine Rasterfahndung ohne Anlass und Verdacht eingeführt. Eine solche Rasterfahndung geht erheblich über den bereits weitreichenden, personenbezogenen Datenabgleich mit Informationssystemen gemäss Art. 7 hinaus und ist offensichtlich unverhältnismässig.

	Antrag Proposition	Begründung / Bemerkungen Justification / Remarques
Art. 9 Abs. 3	Sofern keine Streichung von Art. 9 FPG erfolgt: Ergänzung: <i>«Es dürfen dabei keine selbstlernende Systeme eingesetzt werden.»</i>	Die Kriterien müssen vorgängig festgelegt werden. Es ist deshalb, auch im Einklang mit dem erwähnten EuGH-Urteil, festzuhalten, dass die Kriterien nicht mit Technologien der künstlichen Intelligenz im Rahmen von selbstlernenden Systemen (maschinelles Lernen) festgelegt werden dürfen.
Art. 9 Abs. 5 FPG	Sofern keine Streichung von Art. 9 FPG erfolgt: Ergänzung: <i>«Die Ergebnisse der Überprüfung werden veröffentlicht.»</i>	Mit der Veröffentlichung wird ein Anreiz für die PIU geschaffen, die gesetzlichen Vorgaben einzuhalten, und gleichzeitig das Vertrauen der Rechtsunterworfenen durch Transparenz gestärkt.
Art. 9 Abs. 6 lit. b FPG	Sofern keine Streichung von Art. 9 FPG erfolgt: Ersetzung als Art. 9 Abs. 6 FPG: <i>«Als Straftaten nach Artikel 6 Absätze 2–3, für deren Bekämpfung Beobachtungslisten eingesetzt werden dürfen, gelten Straftaten gemäss Anhang 2.»</i> (Und Art. 9 Abs. 6 lit. a FPG als Art. 7 FPG).	Die betroffenen Straftaten sollten für Rechtssicherheit und Verständlichkeit der betroffenen Personen in einem Anhang zum Gesetz und mit Verweis auf schweizerisches Strafrecht bzw. Nebenstrafrecht ausdrücklich als Katalog aufgeführt werden.
Art. 10 FPG	Streichung.	Das FPG dient gemäss Art. 1 lit. a FPG der Ermittlung, Verfolgung usw. von Straftaten. Der Nachrichtendienst des Bundes ist keine Strafverfolgungsbehörde (vgl. Art. 6 NDG e contrario).
Art. 11 FPG	Ergänzung: Überprüfung und Dokumentation von Anträgen sowie um einen zweiten Absatz: <i>«Der Rechtsschutz richtet sich nach dem Gesetz, welches die Tätigkeit der adressierten Behörde regelt.»</i>	Die Übermittlung ihrer Daten an Behörden kann für die betroffenen Personen auch im Einzelfall erhebliche Auswirkungen haben. Es muss deshalb klar festgelegt werden, wie ein Antrag zu prüfen ist. Auch ist das Ergebnis der Überprüfungen zu dokumentieren, damit eine wirksame Aufsicht und ein wirksamer Rechtsschutz gewährleistet sind. Der Rechtsschutz soll sich nach dem jeweiligen Gesetz, welches die Tätigkeit der adressierten Behörde regelt, richten.

	Antrag Proposition	Begründung / Bemerkungen Justification / Remarques
Art. 11 lit. b FPG	Streichung.	Das FPG dient gemäss Art. 1 lit. a FPG der Ermittlung, Verfolgung usw. von Straftaten. Der Nachrichtendienst des Bundes ist keine Strafverfolgungsbehörde (vgl. Art. 6 NDG e contrario).
Art. 11 lit. c FPG	Streichung	Die Weiterleitung an eine ausländische Behörde sollte ausschliesslich dem dafür geschaffenen Gesetz, nämlich dem Bundesgesetz über internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz, IRSG), unterstellt sein. Der Europol-Staatsvertrag bildet keine ausreichende Grundlage.
Art. 12 FGP	Verschiebung	Systematisch sollte Art. 12 FGP zwischen Art. 9 und dem (jetzigen) Art. 10 FGP positioniert werden.
Art. 12 Abs. 1 FPG	Ersetzung: « <i>Besteht der hinreichende Verdacht [...].</i> »	Die StPO kennt keinen «konkreten Verdacht». Es nicht erforderlich oder sinnvoll, eine neue Verdachtskategorie einzuführen, zumal eine Koordination mit der StPO wünschenswert ist. Dieses Ziel wird mit «hinreichend» statt «konkret» erreicht.
Art. 12 Abs. 2 FPG	Ergänzung: « <i>[...] einschliesslich besonders schützenswerter Personendaten gemäss Art. 6 Abs. 6 FPG [...].</i> » <i>Ergänzung mit neuem Absatz: «3 Übereinstimmungen, die keinen Anlass zu einer Meldung geben, werden nicht gespeichert.»</i>	Klarstellung, welche besonders schützenswerten Personendaten übermittelt werden dürfen, nämlich jene, die bearbeitet werden dürfen. Klarstellung, dass Übereinstimmungen gemäss Art. 9 FGP, die keinen Anlass zu einer Meldung geben, nicht gespeichert werden, weil es dafür an der Erforderlichkeit fehlt.
Art. 14 FPG	Ergänzung: « <i>Pseudonymisieren ist das Ersetzen von Namen und anderen Identifikationsmerkmalen durch ein Kennzeichen mit dem Zweck, die Bestimmung der</i>	Pseudonymisieren ist kein Rechtsbegriff und deshalb zu definieren. Die Ergänzung orientiert sich an der entsprechenden Definition im deutschen Datenschutzrecht.

	Antrag Proposition	Begründung / Bemerkungen Justification / Remarques
	<i>betroffenen Personen wesentlich zu erschweren.»</i>	
Art. 15 Abs. 6 FPG	Ergänzung: « <i>Das Bundesverwaltungsgericht veröffentlicht seine Entscheidungen.</i> »	Mit der Veröffentlichung der Entscheide wird ein Anreiz für die PIU und das Bundesverwaltungsgericht geschaffen, die gesetzlichen Vorgaben einzuhalten, und gleichzeitig das Vertrauen der Rechtsunterworfenen durch Transparenz gestärkt. Die Praxis des Bundesgerichts bei überwachungsrechtlichen Entscheidungen zeigt, dass solche Entscheide früher oder später im Rahmen der verfassungsmässig garantierten Justizöffentlichkeit veröffentlicht werden können. Auch bei den Passagierdaten soll keine Kabinettsjustiz stattfinden.
Art. 16 Abs. 1 FPG	Ersetzung: [...] werden sechs Monate nach ihrem Eingang [...].»	Die Frist von sechs Monaten entspricht der umstrittenen Frist bei der bestehenden strafprozessualen Vorratsdatenspeicherung. Die Tatsache, dass die Daten nach sechs Monaten pseudonymisiert werden, heilt die datenschutz- und grundrechtlichen Bedenken einer exzessiven Speicherung auf Vorrat nicht; diese Pseudonymisierung bietet eigentlich nur Schutz gegen gewisse Datenlecks und gewährt (durch Art. 15 Abs. 1 FPG) eine etwas höhere Schranke für die Auswertung. Es wäre aber möglich, nach sechs Monaten ausgewählte Flugpassagierdaten (pseudonymisiert) zu speichern, falls die Prüfung gemäss Art. 7 FGP einen Treffer ergeben hat, die Rasterprüfung gemäss Art. 9 Anlass zu einer Übermittlung gegeben hat, oder sonstwie (auch auf Anfrage hin) die Daten übermittelt wurden. Eine solche Regelung könnte sich in einem weiteren Absatz finden.
Art. 16 Abs. 2 FPG	Ersetzung: Regelung der maximalen Aufbewahrungsdauer im Gesetz.	Die maximale Aufbewahrungsdauer für alle Daten und nicht allein jene gemäss Art. 16 Abs. 1 FPG ist im Gesetz zu regeln.
Art. 17 FPG	Ersetzung/ Ergänzung: « <i>Die Datenschutzstelle von fedpol</i>	Mit der Veröffentlichung wird ein Anreiz für die PIU geschaffen, die gesetzlichen Vorgaben einzuhalten, und für die Datenschutzstelle, eine

	Antrag Proposition	Begründung / Bemerkungen Justification / Remarques
	<i>überwacht die Einhaltung der Bearbeitung von Personendaten gemäss diesem Gesetz. Die Datenschutzstelle veröffentlicht einen jährlichen Aufsichtsbericht.</i>	wirksame Aufsichts auszuüben, und gleichzeitig das Vertrauen der Rechtsunterworfenen durch Transparenz gestärkt. Mit der Formulierung «Bearbeitung von Personendaten» wird die Formulierung gemäss allgemeinem Datenschutzrecht verwendet und klargestellt, dass es – auch mit Blick auf den Schutz der betroffenen Personen vor Missbrauch – um die Aufsicht über Bearbeitungsvorgänge geht.
Art. 18 Abs. 2 FPG	Streichung.	Pseudonymisierte Daten sind Personendaten gemäss Art. 5 lit. a des neuen Datenschutzgesetzes und müssen deshalb sachlogisch vom Auskunftsrecht erfasst sein. Art. 14 Abs. 1 FPG zeigt, dass die PIU die Pseudonymisierung auch tatsächlich aufheben kann.
Art. 18 Abs. 3 FPG	Streichung.	Die Konsultation der Behörden ist überflüssig. Art. 18 Abs. 1 FPG verweist auf das Auskunftsrecht gemäss dem neuen Datenschutzgesetz (nDSG). Bei Bedarf kann die Auskunft gemäss Art. 26 Abs. 2 lit. b nDSG verweigert, eingeschränkt oder aufgeschoben werden.
Art. 21 Abs. 1 FPG	Ersetzung: «[...] einen angemessenen oder geeigneten Schutz [...]»	Art. 16 Abs. 1 u. 2 des neuen Datenschutzgesetzes (nDSG) sehen vor, dass die Bekanntgabe von Personendaten in andere Staaten bedingt, dass die dortige Gesetzgebung einen angemessenen (Abs. 1) oder geeigneten (Abs. 2) Datenschutz gewährleistet. Mit der ausdrücklichen Erwähnung in Art. 3 FPG wird sichergestellt, dass dieser Standard, den das nDSG vorgibt, auch für Flugpassagierdaten gilt. Da in der Schweiz ausserdem Völkerrecht grundsätzlich Vorrang vor Landesrecht genießt, wird mit der ausdrücklichen Erwähnung sichergestellt, dass der Standard gemäss nDSG nicht ausgehöhlt wird.
Art. 21 Abs. 2 FPG	Ergänzung: «[...] abschliessen, soweit das jeweilige nationale Recht einen angemessenen oder geeigneten Schutz dieser Daten gewährleistet. »	Mit der Ergänzung wird der Standard gemäss nDSG auch für Fedpol gewährleistet.

	Antrag Proposition	Begründung / Bemerkungen Justification / Remarques
Art. 22 Abs. 2 FPG	<p>Ergänzung: «<i>c. und ein angemessener oder geeigneter Schutz der Daten gewährleistet ist.</i>»</p> <p>Ergänzung mit neuem Absatz: «<i>4 Die betreffende Person wird über die Ermittlung informiert.</i>»</p>	<p>Mit der Ergänzung wird der Standard gemäss nDSG auch bei solcher Amtshilfe gewährleistet.</p> <p>Die betreffende Person hat durch die Information die Möglichkeit, einen effektiven Rechtsschutz beanspruchen zu können.</p>
Art. 23 Abs. 3 FPG	<p>Ersetzung: «<i>[...] kein hinreichender Verdacht [...].</i>»</p>	<p>Die StPO kennt keinen «begründeten Verdacht» in einem passenden Zusammenhang. Es nicht erforderlich oder sinnvoll, eine neue Verdachtskategorie einzuführen. Die StPO kennt hingegen einen «hinreichenden Verdacht», so insbesondere bei Zwangsmassnahmen (Art. 1987 Abs. 1 lit. b StPO).</p>

Der Schweizerische Anwaltsverband dankt Ihnen für Ihre Kenntnisnahme.

Präsidentin SAV

Birgit Sambeth Glasner

A handwritten signature in blue ink, appearing to read 'Sambeth Glasner', followed by a long horizontal flourish.

Generalsekretär SAV

René Rall

A stylized handwritten signature in black ink, consisting of a large, bold, looped initial 'R' followed by a horizontal stroke.

/ Stellungnahme

Vernehmlassungsantwort zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG)

15. Juli 2022

Sehr geehrte Damen und Herren

Wir danken für die Möglichkeit zur Stellungnahme zum titelerwähnten Gesetzesentwurf.

AlgorithmWatch Schweiz ist eine zivilgesellschaftliche Organisation, die sich mit den gesellschaftlichen Auswirkungen des Einsatzes von algorithmischen Entscheidungssystemen befasst. Wir setzen uns dafür ein, dass die Verwendung der Systeme Mensch und Gesellschaft zugutekommt, Grundrechte und Gemeinwohl achtet und deren Nutzen gerecht verteilt wird.

Wir nehmen zum vorgeschlagenen Gesetzesentwurf wie folgt Stellung, wobei wir uns auf die für unsere Organisation zentralen Aspekte beschränken. Zusätzlich zu den hier erwähnten unterstützen wir auch die Ausführungen in der Stellungnahme der Digitalen Gesellschaft, die im Rahmen des Vernehmlassungsprozess eingebracht wird.

Grundsätzliche Anmerkungen

Wir halten die verdachtsunabhängige Erhebung von Personendaten grundsätzlich für sehr problematisch. Gemäss dem erläuternden Bericht stellt die verdachtsunabhängige Bearbeitung von Personendaten einen Paradigmenwechsel für die Schweiz dar. Als Rechtfertigung für diesen Paradigmenwechsel wird mit der Erhöhung der Sicherheit für die ganze Gesellschaft argumentiert. Das FPG soll der Verhinderung, Aufdeckung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten dienen (vgl. Art. 1 lit. a FPG). Die Erhebung sämtlicher, verdachtsunabhängiger Flugpassagierdaten ist jedoch nicht verhältnismässig. Eine verdachtsunabhängige Übermittlung sämtlicher Flugpassagierdaten zu zwei verschiedenen Zeitpunkten schafft eine riesige Datenmenge, die nicht der Bekämpfung des Terrorismus dienen kann. Es ist äusserst fraglich, ob die Erhebung sämtlicher Flugpassagierdaten tatsächlich zur Erhöhung der Sicherheit führt.

Mit dem Übermitteln, Speichern und Abgleichen sämtlicher Flugpassagierdaten wird stark in die Grundrechte der Individuen eingegriffen. Gerade weil damit ein Paradigmenwechsel stattfindet, muss der Schutz der Betroffenen besonders gewährleistet sein. Es braucht einen starken Datenschutz und ein Auskunftsrecht. Das FPG bietet jedoch keinen genügenden Datenschutz.

Von dieser grundsätzlichen Ablehnung abgesehen, weist das FPG in vielerlei Hinsicht problematische Ansätze und Formulierungen auf. Im Folgenden greifen wir einige für unsere Organisation zentralen Aspekte davon auf.

Weitere Informationssysteme

Gem. Art. 7 Abs. 3 FPG sind automatisch erzielte Übereinstimmungen vor ihrer Übermittlung an die zuständige Behörde manuell und nötigenfalls unter Zugriff auf weitere Informationssysteme zur Klärung der Identität einer Person oder der Ausschreibungsgründe auf ihre Plausibilität hin zu überprüfen. Es ist unklar, welche Informationssysteme unter «weitere» fallen. Auch im erläuternden Bericht wird nur erwähnt, dass die PIU für die Erfüllung ihrer Aufgabe Zugriff auf verschiedene Informationssysteme des Bundes hat. Welche damit gemeint sind, wird nicht erwähnt.

Es ist ausdrücklich zu regeln, auf welche Informationssysteme die PIU Zugriff hat. Ansonsten ist für die Rechtsunterworfenen nicht ersichtlich, wohin ihre Daten überall gehen. Das widerspricht auch der Idee des FPG, Rechtssicherheit und Transparenz für die Flugpassagier*innen zu schaffen. Wie im erläuternden Bericht erwähnt wird, ist es das Ziel des FPG, ein neues Gesetz zu schaffen, das die Bearbeitung von Flugpassagierdaten umfassend regelt, um grösstmögliche Transparenz und Kohärenz zu schaffen: «Für Flugpassagiere soll einfach erkennbar sein, wofür und zu welchen Bedingungen ihre Daten staatlich bearbeitet werden dürfen und welche Rechte ihnen als Betroffene zustehen». Das FPG muss entsprechend ausdrücklich regeln, auf welche Informationssysteme die PIU Zugriff hat.

Risikoprofile und Beobachtungslisten

Gem. Art. 9 FPG kann die PIU aufgrund eigener Analysen oder auf Antrag der Behörden Risikoprofile und Beobachtungslisten erstellen und die Flugpassagierdaten mit diesen abgleichen. Worin diese eigenen Analysen bestehen, wird nicht geregelt. Das führt zu einer enormen Unsicherheit. Die Rechtsunterworfenen wissen nicht, auf welcher Datengrundlage die Risikoprofile oder Beobachtungslisten erstellt werden und wie ihre Daten in diesem Zusammenhang bearbeitet werden. Dies entspricht nicht dem bereits oben erwähnten Ziel, dass für Flugpassagier*innen einfach erkennbar sein soll, wofür und zu welchen Bedingungen ihre Daten bearbeitet werden.

Wir fordern, dass solche Risikoprofile und Beobachtungslisten grundsätzlich unterlassen werden und der ganze Artikel ersatzlos gestrichen wird. Alternativ muss genau geregelt werden, wie diese Analysen gemacht werden, damit Transparenz für die Risikoprofile und Beobachtungslisten geschaffen wird. Insbesondere ist jedoch sicherzustellen, dass keine direkt oder indirekt diskriminierenden Merkmale als Grundlage für Risikoprofile und Beobachtungslisten herangezogen werden. Wichtig ist dabei, dass diskriminierende Auswirkungen auch indirekt auftreten können, da gewisse Merkmale stellvertretend für besonders schützenswerte Personendaten herangezogen werden könnten (Proxies). Beispielsweise können diskriminierende Auswirkungen auch auftreten, indem der Wohnort einer Person in den Risikoprofilen berücksichtigt wird.

Informationspflicht

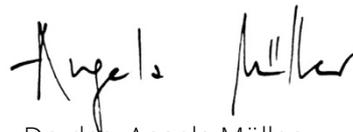
Gemäss Art. 5 FPG müssen die Luftverkehrsunternehmen die Flugpassagier*innen schriftlich informieren, dass die sie betreffenden Flugpassagierdaten bearbeitet werden. Mehr wird dazu nicht gesagt – weder ob das in den AGB stehen darf oder ob dies eventuell erst bei Abflug geschehen darf. Es muss klar geregelt sein, dass bereits vor Buchung der Tickets informiert werden muss, da ansonsten unter Umständen nicht mehr in die Übermittlung eingewilligt werden kann, wenn dann bereits schon übermittelt wurde. Ausserdem sieht das Gesetz zwar Sanktionen vor, wenn die Fluggesellschaften die Daten nicht richtig an die PIU übermitteln, aber keine Sanktionen, wenn sie die Gäste nicht richtig informieren. Fraglich ist, wie sich die Flugpassagier*innen gegen eine fehlende Information wehren können und wie die Fluggesellschaften dafür sanktioniert werden können.

Wir beschränken uns in dieser Stellungnahme auf einige unserer Kernanliegen. Der Verzicht auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Artikeln in dieser Stellungnahme bedeutet keine Zustimmung von AlgorithmWatch Schweiz.

Freundliche Grüsse



Dr. Anna Mätzener
Managing Director



Dr. des. Angela Müller
Head of Policy & Advocacy

Digitale Gesellschaft, CH-4000 Basel

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei
Guisanplatz 1A
3003 Bern

Per E-Mail an: kd-rechtsabteilung@fedpol.admin.ch

27. Juli 2022

Stellungnahme zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG)

Sehr geehrte Damen und Herren

Am 13. April 2022 eröffnete der Bundesrat die Vernehmlassung zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG). Wir bedanken uns für die Möglichkeit zur Stellungnahme.

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 Entwurf wie folgt Stellung:

1. Grundsätzliches

Mit dem Flugpassagierdatengesetz (FPG) müssen verdachtsunabhängig alle Flugpassagierdaten von den Airlines an eine neu geschaffene Stelle (Passenger Information Unit, PIU), die dem fedpol angegliedert ist, übermittelt werden. Diese bearbeitet die Daten, insbesondere durch Speichern, Abgleichen und Weiterleiten oder kann sogar Risikoprofile daraus erstellen.

Gemäss dem erläuternden Bericht stellt die verdachtsunabhängige Bearbeitung von Personendaten einen «Paradigmenwechsel» für die Schweiz dar. Als Rechtfertigung für diesen Paradigmenwechsel wird mit der Erhöhung der Sicherheit für die ganze Gesellschaft argumentiert. Das FPG soll der Verhinderung, Aufdeckung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten dienen (vgl. Art. 1 lit. a FPG). Mit dem Übermitteln, Speichern und Abgleichen sämtlicher Flugpassagierdaten wird dabei stark in die Grundrechte der Individuen eingegriffen.

Trotz diesem Paradigmenwechsel und den schwerwiegenden Grundrechtseingriffen bietet das FPG aber keinen genügenden Datenschutz. Die Erhebung sämtlicher, verdachtsunabhängiger Flugpassagierdaten ist nicht verhältnismässig. Zudem ist äusserst fraglich, ob die verdachtsunabhängige Erhebung sämtlicher Flugpassagierdaten tatsächlich der Bekämpfung des Terrorismus dient und zur Erhöhung der Sicherheit führt.

Dass dies nur leere Schlagwörter sind, die das tatsächliche Ziel des Gesetzes, die Massenüberwachung, verschleiern, wird u. a. durch die zu weitgehenden Deliktskataloge deutlich. Unter dem Vorwand des Terrorismus und der Sicherheit werden mit dem FPG digitale Ein- und Ausreisekontrollen geschaffen. Auch das erklärte Ziel, für mehr Transparenz bei den Flugpassagier:innen zu sorgen, wird durch das Unwissen darüber, auf welche Informationssysteme zugegriffen werden kann, die Erstellung von Risikoprofilen und Beobachtungslisten sowie die Streckenbestimmung des Nachrichtendienst des Bundes (NDB) vollkommen unglaubwürdig.

Die Digitale Gesellschaft lehnt die verdachtsunabhängige Erhebung von Personendaten und damit das Flugpassagierdatengesetz ausdrücklich ab.

Wir positionieren uns deutlich gegen Massenüberwachungsmassnahmen, so z. B. auch gegen die Vorratsdatenspeicherung (gemäss Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, BÜPF), bei der die Telekommunikationsprovider Daten aufbewahren müssen. Das FPG geht aber noch

darüber hinaus, da die Airlines die Daten direkt an die PIU weiterleiten müssen, wie wenn bei der Vorratsdatenspeicherung die Provider die Daten direkt an die Überwachungsbehörde weiterleiten müssten. Das FPG geht damit nicht nur eindeutig zu weit, sondern ist gänzlich abzulehnen.

Von dieser allgemeinen Ablehnung gegenüber dem Flugpassagierdatengesetz und der damit verbundenen Massenüberwachung abgesehen, weist das FPG in vielerlei Hinsicht problematische Ansätze und Formulierungen auf, die folgend im Detail thematisiert werden. Die Kritik und Änderungsforderungen zu den einzelnen Artikeln bedeuten keine grundsätzliche Zustimmung zum FPG. Wir erachten das FPG als nicht revidierbar und lehnen es ausdrücklich ab.

2. Übermittlung der Daten i.S.v. Art. 2 FPG

2.1 Datensicherheit

Gemäss Art. 2 Abs. 1 FPG müssen die Luftverkehrsunternehmen der zuständige Stelle (Passenger Information Unit, PIU) die Flugpassagierdaten für alle Flüge von der Schweiz ins Ausland und vom Ausland in die Schweiz übermitteln. Darunter fallen gemäss Anhang 1 z. B. Name, Adresse, Kreditkarten-Nummer und die Beziehung zu Begleitpersonen. Es handelt sich dabei um Personendaten, welche schützenswert sind. Der erläuternde Bericht erkennt richtig, dass dem Datenschutz ein hohes Gewicht zukommen muss, besonders deshalb, weil auch bzw. vor allem Daten von Personen ohne jeglichen Bezug zu Straftaten bearbeitet werden. Auch die Datensicherheit bei der Übermittlung ist von grösster Bedeutung. Art. 2 Abs. 4 FPG sieht jedoch nur vor, dass die technischen Einzelheiten der Übermittlung durch das Bundesamt für Polizei (fedpol) festgelegt werden. Diese Delegation ist ungenügend. Die Datenübermittlung muss im FPG selbst festgehalten werden. Einzelheiten müssen zumindest in einer Verordnung des Bundesrates geregelt werden, nicht aber durch das fedpol.

Zur technischen Regelung der Datenübermittlung ins Ausland gemäss Art. 3 FPG wird gar nichts geregelt. Auch die Datenübermittlung ins Ausland muss im FPG selbst geregelt werden, damit die Datensicherheit bei der Übermittlung gewährleistet ist.

2.2 Zeitpunkt der Übermittlung i.S.v. Art. 2 Abs. 2 FPG

Gemäss Art. 2 Abs. 2 FPG sind die Daten frühestens 48 bis spätestens 24 Stunden vor der planmässigen Abflugzeit sowie unmittelbar nach Abschluss des Boardings zu übermitteln. Damit müssen die Flugpassagierdaten zu zwei unterschiedlichen

Zeitpunkten von den Fluggesellschaften an die PIU übermittelt werden. Gemäss erläuterndem Bericht sind die Daten zu zwei Zeitpunkten zu übermitteln, um der PIU eine gewisse Vorlaufzeit bis zum Eintreffen des Fluges zu geben, was allerdings nur bei kurzen Flügen von Bedeutung sein dürfte. Dies scheint zudem kein ausreichender Grund zu sein, da erst die zweite Übermittlung die definitive Datenbekanntgabe zu allen sich an Board befindenden Flugpassagieren erlaubt. Wenn eine Person einen Flug erst kurzfristig, weniger als 24 Stunden vor Abflug bucht, wird die erste Datenübermittlung umgangen und somit das Ziel der Vorlaufzeit unterlaufen. Die Vorlaufzeit ist also kein geeignetes Argument, die Übermittlung der Daten zu einem ersten Zeitpunkt zu rechtfertigen.

Gemäss Ziff. 10 Anhang 1 werden auch die Daten von nicht angetretenen Flügen übermittelt. Es werden also nicht nur die Daten aller tatsächlichen Passagiere an Board weitergegeben, sondern auch Daten derjenigen, welche einen Flug buchen, aber dann nicht auf dem Flug sind. Es ist nicht ersichtlich, wie die Daten einer potenziellen Passagierin, welche dann vielleicht ihren Flug verpasst, zur Verhinderung von schweren Straftaten dienen soll, zumal diese Straftaten gemäss dem Europäischen Gerichtshof (EuGH) zumindest einen mittelbar objektiven Zusammenhang mit der Beförderung von Fluggästen aufweisen müssen (vgl. Urteil C-817/19 des EuGH vom 21. Juni 2022). Die Übermittlung der Daten bis spätestens 24 Stunden vor der Abflugzeit ist nicht mit dem öffentlichen Interesse der Sicherheit zu rechtfertigen.

Es ist unverständlich, weshalb die Übermittlung an zwei verschiedenen Zeitpunkten stattfinden muss. Die zweifache Übermittlung führt einzig dazu, dass eine zweifache Menge an Daten entsteht. Wir fordern, dass die Daten nicht bereits vor dem Abschluss des Boardings übermittelt werden.

3. Informationspflicht i.S.v. Art. 5 FPG

Gemäss Art. 5 FPG müssen die Luftverkehrsunternehmen die Flugpassagier:innen schriftlich informieren, dass die sie betreffenden Flugpassagierdaten bearbeitet werden. Gemäss erläuterndem Bericht kann hierzu in den AGB stehen, dass «auch nach dem Flugpassagierdatengesetz bearbeitet werden». Dies ist ungenügend und zu wenig präzise. Es muss klar geregelt sein, dass vor der Buchung der Tickets verständlich über die Bearbeitung der Daten informiert werden muss. Die Information muss sämtliche Daten aufzählen, die übermittelt werden und darf nicht nur pauschal auf die Übermittlung «nach dem Flugpassagierdatengesetz» hinweisen.

4. Bearbeiten der Daten i.S.v. Art. 6 FPG

Gemäss Art. 6 Abs. 1 FPG dürfen die Flugpassagierdaten nur zur Verhinderung, Aufdeckung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten bearbeitet werden. Als Bearbeiten von Daten gilt gemäss Glossar des erläuternden Berichts aber jeder Umgang mit Personendaten, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten. Damit stellt das Weiterleiten schon das Bearbeiten von Daten dar sowie auch das Speichern der Daten vom PIU. Da die Daten ja gerade verdachtsunabhängig übermittelt werden, kann Art. 6 Abs. 1 FPG gar nicht erfüllt werden.

Zudem steht im Glossar, dass das Flugpassagierdatengesetz die Bearbeitung von Daten für die Bekämpfung von Terrorismus und anderen schweren Straftaten vorsieht und ergänzend zum Datenschutzgesetz ihren Schutz regelt. Das FPG regelt das Bearbeiten von Daten aber nicht ergänzend zum Datenschutz, sondern stellt durch das verdachtsunabhängige Bearbeiten von Flugpassagierdaten vielmehr eine Ausnahme des Datenschutzes dar. Wir fordern, dass das FPG das Datenschutzgesetz tatsächlich ergänzt und damit den Datenschutz weiter stärkt, statt ihn einzuschränken, indem z. B. das Auskunftsrecht bei pseudonymisierten Daten verwehrt wird.

5. Terroristische oder andere schwere Straftaten

Das FPG regelt klar, dass es die Bearbeitung der Flugpassagierdaten nur zur Verhinderung, Aufdeckung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten (Art. 1 lit. a und Art. 6 Abs. 1 FPG) erlaubt. In mehreren Artikeln wird dann jedoch nicht mehr ausdrücklich festgehalten, dass es sich dabei nur um terroristische oder andere schwere Straftaten handeln darf, womit Unsicherheit besteht, ob es sich wirklich nur um terroristische und andere schwere Straftaten handelt.

So regelt Art. 6 Abs. 6 lit. b FPG, dass die PIU besonders schützenswerte Personendaten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen bearbeiten darf. Es muss ausdrücklich festgehalten werden, dass sich «strafrechtliche Verfolgungen und Sanktionen» nur auf terroristische und andere schwere Straftaten beziehen darf. Das Bearbeiten von verwaltungsrechtlichen Verfolgungen oder Sanktionen ist aus Art. 6 Abs. 6 lit. b FPG zu streichen.

Auch in Art. 7 Abs. 1 FPG soll nochmals ausdrücklich festgehalten werden, dass sich die Zwecke von lit. a - d nicht auf alle Straftaten beziehen dürfen, sondern nur auf terroristische und andere schwere Straftaten im Sinne dieses Gesetzes. Zudem werden gemäss Art. 7 Abs. 1 lit. d FPG Flugpassagierdaten zum Zweck der Informationen in Zusammenhang mit ungeklärten oder geplanten Straftaten automatisch abgeglichen. Dabei ist unklar, was unter «geplanten Straftaten» zu verstehen ist. Daher ist «oder geplanten» aus Art. 7 Abs. 1 lit. d FPG zu streichen.

Die Deliktskataloge der terroristischen und anderen schweren Straftaten sind umfassender als für den Zweck der Sicherheit der Gesellschaft notwendig. Der Europäische Gerichtshof (EuGH) hat entschieden, dass sich die Straftaten auf diejenigen beschränken müssen, bei welchen zumindest ein mittelbarer objektiver Zusammenhang mit der Beförderung von Fluggästen bestehen (vgl. Urteil C-817/19 des EuGH vom 21. Juni 2022). Deshalb sollen sämtliche Deliktskategorien aus dem Anhang 2 ausgenommen werden, welche keinen mittelbaren objektiven Zusammenhang mit der Beförderung von Fluggästen aufweisen, namentlich Nr. 3, 4, 6, 7, 8, 9, 12, 15, 17, 18, 21, 24, 25, 26.

Als besonders problematisch erachten wir, dass der Landfriedensbruch i.S.v. Art. 260 StGB unter terroristische Straftaten fällt, sofern er «terroristisch motiviert» ist, da die Verwendung und Abgrenzung dieses Begriffs insbesondere seit dem Bundesgesetz über die polizeilichen Massnahmen zur Bekämpfung von Terrorismus (PMT) unklar und zu weitgehend ist. Auch die Delikte der betrügerischen Nachahmung und Produktpiraterie gemäss Anhang 2 werden dem Anspruch an schwere Straftaten i.S.v. Art. 6 Abs. 3 FPG nicht gerecht. Damit wird deutlich, dass es nur vordergründig um die Verhinderung von Terrorismus und schweren Straftaten geht. Vielmehr wird unter dem verschleiernenden Schlagwort des Terrorismus und der Sicherheit für die Bevölkerung ein weitgehender Deliktskatalog und eine ausufernde Überwachung geschaffen, die in keinem Verhältnis mit dem Sicherheitsbedürfnis der Gesellschaft stehen.

Wir fordern, dass der Delikt des Landfriedensbruchs gemäss Art. 6 Abs. 2 FPG und die Delikte der betrügerischen Nachahmung und Produktpiraterie aus dem Deliktskatalog (Nr. 17 in Anhang 2) der schweren Straftaten gemäss Art. 6 Abs. 3 lit. a FPG gestrichen werden sowie die Nr. 3, 4, 6, 7, 8, 9, 12, 15, 17, 18, 21, 24, 25, 26 aus Anhang 2.

6. Weitere Informationssysteme i.S.v. Art. 7 Abs. 3 FPG

Gemäss Art. 7 Abs. 3 FPG sind automatisch erzielte Übereinstimmungen vor ihrer Übermittlung an die zuständige Behörde manuell und nötigenfalls unter Zugriff auf weitere Informationssysteme zur Klärung der Identität einer Person oder der Ausschreibungsgründe auf ihre Plausibilität hin zu überprüfen. Im Gesetz ist nicht geregelt, welche Informationssysteme unter «weitere» fallen. Im erläuternden Bericht sind zwar verschiedene Informationssysteme aufgelistet. Dies ist jedoch ungenügend.

Es ist ausdrücklich zu regeln, auf welche Informationssysteme die PIU Zugriff hat. Ansonsten ist für die Rechtsunterworfenen nicht ersichtlich, wohin ihre Daten gehen. Das widerspricht der Idee des FPG, Rechtssicherheit und Transparenz für die Flugpassagier:innen zu schaffen. Der Zugriff muss ausserdem protokolliert werden, damit nachvollziehbar ist, warum welche Personen auf welche Daten zugreifen. Diese Zugriffsprotokollierung kann auch auf Verordnungsebene geregelt werden.

Wie im erläuternden Bericht erwähnt wird, ist es das Ziel des FPG, ein neues Gesetz zu schaffen, das die Bearbeitung von Flugpassagierdaten umfassend regelt, um grösstmögliche Transparenz und Kohärenz zu schaffen. «Für Flugpassagier:innen soll einfach erkennbar sein, wofür und zu welchen Bedingungen ihre Daten staatlich bearbeitet werden dürfen und welche Rechte ihnen als Betroffene zustehen.» Aus dem Gesetz gehen aber keine Rechte der Flugpassagier:innen hervor. Im Gegenteil, diese werden weiter eingeschränkt, wie das verwehrte Auskunftsrecht zeigt. Dies zeigt deutlich auf, dass das Gesetz nicht für die Überwachten, sondern für die Überwachenden geschrieben wurde. Der Schutz der Betroffenen ist nicht gewährleistet. Umso mehr lehnen wir grundsätzlich die Übermittlung der Daten ab.

Das FPG muss ausdrücklich regeln, auf welche Informationssysteme die PIU Zugriff hat. Zudem muss die Zugriffsprotokollierung auf Verordnungsebene geregelt werden.

7. Vorliegen einer Straftat i.S.v. Art. 8 FPG

Gemäss Art. 8 Abs. 1 FPG übermittelt die PIU die Daten an die zuständige Behörde, soweit die Überprüfung das Vorliegen einer Straftat nach Artikel 6 Absätzen 2-3 bestätigt hat. Hier muss ausdrücklich festgehalten werden, dass nur eine richterliche Behörde das Vorliegen einer Straftat überprüfen und bestätigen kann und die PIU diese Überprüfung nicht selbst vornehmen kann.

8. Risikoprofile und Beobachtungslisten i.S.v. Art. 9 FPG

Gemäss Art. 9 FPG kann die PIU aufgrund eigener Analysen oder auf Antrag der Behörden Risikoprofile und Beobachtungslisten erstellen. Worin diese eigenen Analysen bestehen, wird nicht geregelt. Dies führt zu einer enormen Unsicherheit. Die Rechtsunterworfenen wissen nicht, auf welcher Grundlage ihre Daten zu Risikoprofilen oder Beobachtungslisten erstellt werden. Dies entspricht nicht dem bereits oben erwähnten Ziel, dass für Flugpassagier:innen einfach erkennbar sein soll, wofür und zu welchen Bedingungen ihre Daten bearbeitet werden.

Wir fordern, dass solche Risikoprofile und Beobachtungslisten unterlassen werden und der ganze Artikel ersatzlos gestrichen wird. Es soll keine neue Überwachungsbehörde geschaffen werden, welche Daten selber analysieren kann. Die PIU soll höchstens nach Treffern suchen und das Resultat weitergeben können. Danach hat sie die Daten sofort zu löschen. Wird Art. 9 FPG nicht gestrichen, muss genau geregelt werden, wie diese Analysen gemacht werden, damit Transparenz hinsichtlich der Risikoprofile und Beobachtungslisten geschaffen wird und insbesondere keine diskriminierenden Merkmale Grundlage der Risikoprofile und Beobachtungslisten sind. Zudem müssen die Ergebnisse der Überprüfung gemäss Art. 9 Abs. 5 FPG veröffentlicht werden.

9. Zusammenarbeit mit dem NDB i.S.v. Art. 10 FPG

Gemäss Art. 10 FPG kann der Nachrichtendienst des Bundes (NDB) Strecken bestimmen, für die ihm die PIU im automatisierten Verfahren die Daten übermittelt. Mit Art. 8 Abs. 2 lit. b FPG besteht bereits die Möglichkeit, dass die PIU Daten an den NDB weiterleitet. Es ist nicht ersichtlich, weshalb, und völlig unverhältnismässig, dass der NDB die Flugpassagierdaten für von ihm bestimmten Strecken automatisch erhält.

Es ist anzunehmen, dass dies alle möglichen Strecken sein werden, damit auch «Umwege» ersichtlich werden (und dies nicht zur Umgehung der Überwachung verwendet werden könne). Der NDB wird diese Strecken vermutlich geheim halten und die Rechtsunterworfenen damit nicht erfahren, ob ihre Daten direkt an den NDB weitergeleitet werden. Diese Intransparenz ist inakzeptabel und widerspricht ebenfalls dem bereits erwähnten Ziel, Transparenz für die Flugpassagier:innen zu schaffen. Zudem widerspricht Art. 10 FPG auch dem Zweck der Verhinderung, Aufdeckung, Ermittlung und Verfolgung von Straftaten gemäss Art. 1 lit. a FPG, da der NDB keine Strafverfolgungsbehörde ist.

Wir fordern, dass Art. 10 FPG restlos gestrichen wird. Andernfalls ist sicherzustellen, dass, wenn der NDB solche Strecken bestimmt, diese öffentlich gemacht werden müssen, damit für die Flugpassagier:innen klar ersichtlich ist, welche Daten direkt an den NDB weitergeleitet werden.

Gemäss Art. 10 Abs. 3 FPG sind die Daten innerhalb von 96 Stunden nach Erhalt zu löschen, wenn der Abgleich zu keiner Übereinstimmung geführt hat. Diese Frist ist zu lang. Es ist nicht verständlich, weshalb diese Daten noch 96 Stunden aufbewahrt werden dürfen, wenn sie offensichtlich nicht dem Zweck des FPG entsprechen, zumal sie ja beim PIU noch vorhanden wären, sollte es zu einem Vorfall kommen. Art. 6 Abs. 5 FPG regelt, dass Ergebnisse von Bearbeitungen, die den Zwecken nach Art. 6 Abs. 1 FPG nicht entsprechen, umgehend gelöscht werden. Dies ist auch vom NDB zu verlangen. Wir fordern, dass der Art. 10 Abs. 3 FPG ausdrücklich festhält, dass die Daten umgehend zu löschen sind, wenn der Abgleich zu keiner Übereinstimmung geführt hat.

10. Meldung bei einem Verdacht i.S.v. Art. 12 FPG

Gemäss Art. 12 FPG meldet die PIU der zuständigen Strafverfolgungsbehörde einen konkreten Verdacht. Die StPO kennt den hinreichenden Verdacht, jedoch keinen konkreten. Es sollen keine neuen Verdachtskategorien mit dem FPG eingeführt werden, weshalb die Begriffe an die StPO anzupassen sind. Art. 12 Abs. 1 ist deshalb zu einem «hinreichenden Verdacht» zu ändern. Auch in Art. 22 Abs. 3 FPG wird der «begründete Verdacht» erwähnt, welchen die StPO ebenfalls nicht kennt. Art. 22 Abs. 3 FPG soll im Sinne der Vereinheitlichung zu «kein hinreichender Verdacht» geändert werden.

In Art. 12 Abs. 2 FPG soll ergänzt werden, dass es sich um schützenswerte Personendaten gemäss Art. 6 Abs. 6 FPG handeln muss. Damit soll ausdrücklich festgestellt werden, dass nur jene besonders schützenswerten Personendaten übermittelt werden dürfen, welche auch bearbeitet werden dürfen.

11. Zugriff auf das PNR-Informationssystem i.S.v. Art. 13 FPG

Gemäss Art. 13 Abs. 2 lit. a FPG haben die Mitarbeitenden der PIU zur Erfüllung ihrer Aufgaben Zugriff auf das Informationssystem «Passenger Name Record» (PNR-Informationssystem). Das muss konkretisiert werden. Es muss organisatorisch klar geregelt werden, wer Zugriff auf welche Daten hat. Zudem soll ein Vier-Augen-Prinzip

eingeführt werden, wenn Daten manuell bearbeitet werden müssen.

Gemäss Art. 13 Abs. 2 lit. b FPG haben die für die Wartung und Programmierung des Systems zuständigen Personen Zugriff auf das PNR-Informationssystem, soweit dies zur Erfüllung ihrer Wartungs- und Programmierarbeiten unbedingt erforderlich ist. Da Mitarbeitende mit Zugriff auf die Personendaten Beispiel-Daten erstellen können, mit denen programmiert werden kann, ist es nicht erforderlich, dass Personen, die für die Wartung und Programmierung des Systems Zugriff darauf haben. Es gibt keinen Grund, weshalb dabei der Zugriff auf das PNR-Informationssystem notwendig sein sollte. Art. 13 Abs. 2 lit. b ist zu streichen.

12. Datenschutz, Auskunftsrecht und Pseudonymisierung i.S.v. Art. 14 f. FPG

Der Datenschutz bekommt zwar einen eigenen Abschnitt im FPG, mehr aber auch nicht. Im erläuternden Bericht steht, dass der Datenschutz bei der Datenbearbeitung nach dem Flugpassagierdatengesetz eine zentrale Rolle spielt; alles was dieser Abschnitt «Datenschutz» jedoch vorsieht, ist die Pseudonymisierung der Daten, welche wieder rückgängig gemacht werden kann.

Pseudonymisierte Daten gelten gemäss Glossar des erläuternden Berichts weiterhin als Personendaten im Sinne des Datenschutzes, solange die Konkordanztafel noch verfügbar ist. Es handelt sich dabei um sehr persönliche und damit schützenswerte Daten, welche dies auch nach der Pseudonymisierung bleiben. Somit ist die Pseudonymisierung kein ausreichendes Mittel für einen starken Datenschutz. Im Gegenteil, sie schränkt die Rechte der Betroffenen noch weiter ein, da durch die Pseudonymisierung das Auskunftsrecht verloren geht (Art. 18 Abs. 2 FPG). So lassen sich die Daten noch auf eine Person zurückführen, ohne dass diese aber ein Auskunftsrecht hat, welche Daten das sind. Es ist völlig unverständlich, weshalb man mit der Pseudonymisierung das Auskunftsrecht verlieren sollte, da es sich weiterhin um Personendaten handelt. Dieser Widerspruch ist aufzulösen, indem bei pseudonymisierten Daten das Auskunftsrecht gewährt bleibt, genauso wie bei allen anderen Personendaten auch. Art. 18 Abs. 2 FPG ist zu streichen.

Im erläuternden Bericht werden Elemente eines Datensatzes einer Person aufgezählt, welche pseudonymisiert werden müssen. Diese Aufzählung stimmt nicht vollständig mit den zu übermittelnden Daten gemäss Anhang 1 des FPG überein. Es müssen sämtliche Daten gemäss Anhang 1 des FPG pseudonymisiert werden.

Die Frage bleibt, weshalb die pseudonymisierten Daten überhaupt aufbewahrt werden. Es scheint, als sei die Pseudonymisierung eher eine Sicherstellung, dass die Daten nur zweckmässig verwendet werden. Dann geht es dabei aber nicht um Datenschutz, sondern um die zweckmässige Verwendung dieser Daten. Die Pseudonymisierung als Mittel zur Zweckbindung der Daten ist grundsätzlich nicht falsch, hat aber nichts mit der Verletzung der Grundrechte der Betroffenen zu tun.

Wenn allerdings eine Pseudonymisierung durchgeführt werden soll, so ist unerlässlich, dass die pseudonymisierten Daten und die Konkordanztafel sowohl technisch als auch organisatorisch wirklich voneinander getrennt sind. Die Konkordanztafel muss bei einer anderen Organisation aufbewahrt werden und der Zugriff darauf darf für die zuständige Stelle (Passenger Information Unit, PIU) nicht möglich sein. So müsste die Konkordanztafel z. B. bei einem Treuhänder liegen, damit die Pseudonymisierung wirklich nur durch einen Gerichtsbeschluss rückgängig gemacht werden kann.

13. Aufbewahrungsdauer i.S.v. Art. 16 FPG

Die Aufbewahrungsdauer von fünf Jahren gemäss Art. 16 Abs. 1 FPG ist zu lang. Dies hat auch der Europäische Gerichtshof (EuGH) so entschieden: Eine allgemeine, unterschiedslos für alle Fluggäste geltende Speicherfrist von fünf Jahren überschreitet demnach die Grenzen des absolut Notwendigen (vgl. Urteil C-817/19 des EuGH vom 21. Juni 2022). Auch im erläuternden Bericht wird anerkannt, dass es sich um eine verhältnismässig lange Aufbewahrungsdauer handelt, und auch hier wird von einem «Paradigmenwechsel» gesprochen.

Die Digitale Gesellschaft lehnt die Übermittlung und Speicherung der Flugpassagierdaten ausdrücklich ab. Werden diese dennoch übermittelt, so müssen sie unmittelbar nach der Trefferanalyse gelöscht werden und dürfen nicht aufbewahrt werden. Die Aufbewahrungsdauer stellt einen Grundrechtseingriff dar, egal, wie lange die Daten effektiv aufbewahrt werden. Wir fordern, dass die Daten sofort gelöscht werden, wenn sie beim Abgleich zu keinem wesentlichen Ergebnis im Sinne eines konkreten Verdachts auf eine terroristische oder andere schwere Straftat führen. Dieser Abgleich hat gemäss Art. 7 Abs. 2 unmittelbar nach Erhalt der Daten zu erfolgen. Es ist nicht ersichtlich, weshalb die Daten danach noch weiter aufbewahrt werden sollten, wenn dieser Abgleich zu keinem Ergebnis geführt hat. Die Aufbewahrungsdauer in Art. 16 Abs. 1 FPG ist gänzlich zu streichen.

Wird die Aufbewahrungsdauer nicht gestrichen, so muss zumindest die Pseudonymisierung effektiv durchgeführt werden (s. u. Datenschutz und Pseudonymisierung). Gemäss Art. 14 FPG werden die Flugpassagierdaten sechs Monate nach ihrer Übermittlung automatisch pseudonymisiert. Diese Frist ist zu lang. Die Pseudonymisierung hat unmittelbar und automatisiert nach dem Abgleichen der Daten zu geschehen, wenn dabei kein wesentlicher Verdacht auf eine terroristische oder andere schwere Straftat resultiert.

Gemäss Art. 16 Abs. 2 FPG legt der Bundesrat die maximale Aufbewahrungsdauer der Daten, die aus einem Abgleich nach den Artikeln 7 und 9 resultieren, in einer Verordnung fest. Es ist anzunehmen, dass die Aufbewahrungsdauer länger als fünf Jahre sein wird, wenn gemäss Abs. 1 die Daten auch bei keinem Ergebnis fünf Jahre aufbewahrt werden dürfen. Die Aufbewahrung der Daten stellt einen schweren Eingriff in die Grundrechte dar. Es ist nicht verständlich, weshalb die Aufbewahrungsdauer von Daten, die kein Ergebnis erzielt haben im FPG selbst geregelt wird, die Aufbewahrungsdauer von Daten, welche aus einem Abgleich nach Art. 7 oder 9 resultieren jedoch auf Verordnungsstufe geregelt werden sollte. Ausserdem wird diese Aufbewahrungsdauer nicht einer ständigen Anpassung unterliegen, weshalb nicht klar ist, warum die Verordnungsstufe dafür ausgewählt wird. Die Aufbewahrungsdauer für Daten, die aus einem Abgleich nach den Artikeln 7 und 9 resultieren, muss im FPG selbst festgehalten werden. Eine Delegation an eine Verordnung genügt nicht.

14. Völkerrechtlicher Vertrag i.S.v. Art. 21 FPG

Gemäss Art. 3 FPG übermitteln die Luftverkehrsunternehmen die Flugpassagierdaten bei Flügen von der Schweiz ins Ausland an die am Ort der Landung zuständigen Behörde, wenn ein völkerrechtlicher Vertrag mit dem betreffenden Staat die Übermittlung und Bearbeitung der Flugpassagierdaten vorsieht. Dass der Bundesrat solche völkerrechtlichen Verträge nur mit Staaten abschliessen kann, die einen mit der Schweiz «vergleichbaren Schutz der Daten» gewährleisten (Art. 21 FPG), ist alles andere als beruhigend, da der Datenschutz im FPG nicht gewährleistet ist. So haben die Betroffenen weder ein Auskunftsrecht, noch wird die Datensicherheit bei der Übermittlung im FPG selbst geregelt (s. u. 2. und 12.).

Art. 16 Abs. 1 und 2 des neuen Datenschutzgesetzes (nDSG) regeln, dass Personendaten nur ins Ausland bekanntgegeben werden dürfen, wenn der betreffende Staat einen angemessenen oder geeigneten Datenschutz gewährleistet. Dieser

Standard des nDSG soll auch für Flugpassagierdaten gelten. In Art. 3 und Art. 21 FPG muss explizit vorgesehen werden, dass ein völkerrechtlicher Vertrag nur mit Staaten abgeschlossen werden kann, die einen angemessenen oder geeigneten Datenschutz gewährleisten, damit der Standard im nDSG nicht untergraben wird.

Schlussbemerkung

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Artikeln bedeutet keine Zustimmung der Digitalen Gesellschaft.

Freundliche Grüsse

Erik Schönenberger



LAW FIRM
ÉTUDE D'AVOCATS

Département fédéral de justice et police
DFJ
kd-rechtsabteilung@fedpol.admin.ch

Lausanne, le 29 juillet 2022

Avant-projet de Loi fédérale sur le traitement des données relatives aux passagers aériens (LDPa)

Madame la Conseillère fédérale,
Mesdames, Messieurs,

Dans le délai imparti au 31 juillet 2022, je me permets de participer spontanément à la consultation mentionnée sous rubrique et de vous transmettre quelques brèves observations en lien avec l'avant-projet mentionné en référence.

Premièrement et de manière générale, la collecte, l'analyse et la conservation systématiques des données PNR représentent une **atteinte grave** aux droits fondamentaux. Elles doivent être limitées au **strict nécessaire**.

Deuxièmement, la Cour de justice de l'Union européenne a rendu un arrêt (grande chambre) le 21 juin 2022 dans une affaire opposant la Ligue des droits humains contre le Conseil des ministres (**Affaire C-817/19**)¹ qu'il n'est pas nécessaire de paraphraser ici mais qui doit évidemment être pris en compte.

Troisièmement, la conservation pendant cinq ans des données de l'intégralité des passagers aériens est excessive. Elle représente un risque important de surveillance permanente généralisée et de profilage. La pseudonymisation (relative puisqu'elle peut être levée), n'apporte pas des garanties suffisantes.

Il faut donc **renoncer à la conservation pendant cinq ans**. En effet, la conservation n'est pas justifiable pour les données PNR de l'ensemble des passagers aériens pour lesquels ni l'évaluation préalable, ni les éventuelles vérifications effectuées au cours de la période de six mois, ni aucune autre circonstance n'ont révélé l'existence d'éléments

¹ ECLI:EU:C:2022:491.

objectifs de nature à établir un risque suffisant présentant un lien objectif, à tout le moins indirect, avec le voyage aérien effectué par ces passagers.

Au vu de l'avis de la CJUE dans l'arrêt précité ((points 251 à 258 notamment), l'absence de conservation au-delà de six mois dans la LDPa ne devrait pas poser de problème de compatibilité avec le droit de l'UE.

Quatrièmement, les restrictions prévues au **droit d'accès** sont excessives. D'une part les données pseudonymes sont des données personnelles et ne peuvent pas être soustraites au droit d'accès. D'autre part, la consultation des autorités à qui les données ont été transmises ne se justifie pas. Cela risque au contraire de créer des soupçons alors que la personne concernée ne fait que valoir un droit. La LPD ne prévoit d'ailleurs et de manière générale pas de consultation des destinataires.

Finalement, le rapport explicatif envisage largement la possibilité de ne pas communiquer les renseignements à la personne concernée. Au contraire, les informations ayant pour l'essentiel été communiquées par la personne elle-même, rien ne s'oppose à une réponse complète au droit d'accès. La seule réserve envisageable concerne les destinataires, et dans ce cas il faudrait simplement **différer** la réponse.

Je vous remercie par avance de l'attention portée à la présente et vous prie de croire, Madame la Conseillère fédérale, Mesdames, Messieurs, à l'expression de ma parfaite considération.

Sylvain Métille
Professeur ass., Dr jur, avocat
metille@hdclegal.ch

Eidgenössisches Justiz- und Polizeidepartement
Bundeshaus West
3003 Bern

Per E-Mail an: kd-rechtsabteilung@fedpol.admin.ch

22. Juli 2022

Stellungnahme des Schweizer Tourismus-Verbandes

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG)

Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, im Rahmen der Vernehmlassung zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG) Stellung nehmen zu können. Der Schweizer Tourismus-Verband STV ist die nationale tourismuspolitische Dachorganisation mit über 500 Mitgliedern, darunter rund 40 schweizerischen Branchen- und Fachverbänden des Tourismus mit insgesamt rund 30'000 touristischen Leistungserbringern. Als Vertreter des viertgrössten Exportbereichs der Schweizer Wirtschaft setzen wir uns für bessere politische Rahmenbedingungen für die Schweizer Tourismuswirtschaft ein.

Würdigung der Vorlage

Der STV begrüsst, dass der Bundesrat mit der Vorlage internationalen Verpflichtungen nachkommt und mit der vorgeschlagenen Lösung ein möglichst einfaches System zur Übermittlung der Flugpassagierdaten durch die Luftverkehrsunternehmen gewählt hat. Bei der Buchung von Flügen fallen Flugpassagierdaten ohnehin an. Es ist somit sichergestellt, dass für die Luftverkehrsunternehmen ein möglichst kleiner zusätzlicher Aufwand entsteht und bürokratische Leerläufe verhindert werden. Ausserdem ist durch die gewählte Lösung für Flugpassagiere einfach erkennbar, wofür und zu welchen Bedingungen ihre Daten staatlich bearbeitet werden dürfen und welche Rechte ihnen als Betroffene zustehen. Der Schweizer Tourismus profitiert davon, dass die Schweiz ein sicheres Reiseland ist und von terroristischen Anschlägen im Ausmass unserer Nachbarländer verschont blieb. Es ist somit auch im Interesse des Tourismussektors, dass die Schweiz alle Massnahmen ergreift, die nötig sind, um Terrorismus und andere schwere Kriminalität effektiv und effizient zu bekämpfen.

Aus den genannten Gründen unterstützt der STV die Vorlage.

PARTNERSCHAFT. POLITIK. QUALITÄT.

Für weitere Fragen stehen Ihnen zur Verfügung:



Philipp Niederberger
Direktor



Samuel Huber
Wissenschaftlicher Mitarbeiter

Sehr geehrter Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Meine Stellungnahme zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Vernehmlassung 2021/80)

Vorbemerkung

Als Rentner, der seine ganze Zeit in der Schweiz verbringt und bei Reisen zu 90% den öffentlichen Verkehr benützt, verzichte ich auf Flugreisen. Hauptsächlich wegen den massiv übertriebenen sog. Sicherheitsvorschriften, die weltweit wegen ein paar Idioten eingeführt wurden. Durch die Digitalisierung ist es jetzt viel einfacher, diese Massnahmen durch entsprechende Gesetze zu verschärfen und vor allem die lückenlose Überwachung zu vereinfachen. Während sich einige Bundesämter oder Bundesbeamte jeweils damit schwertun, das Öffentlichkeitsgesetz korrekt anzuwenden, sollen nun persönliche Daten der Bürger anlasslos an ausländische Behörden übermittelt werden.

Eine mit diesem Gesetz vorgesehene Vorratsdatenspeicherung ist nicht anderes als eine massenhafte Überwachung der Bevölkerung. Aus der Wortwahl im Einladungsschreiben lässt sich schliessen, dass eine sorgfältige Abwägung beim Eingriff in Grundrechte gar nicht vorgesehen ist.

Meine Stellungnahme zum FPG

Ohne dazu eingeladen worden zu sein nehme ich zu einigen Artikeln wie folgt Stellung:

Artikel 2

Abs. 1 sieht eine Übermittlung von Daten bei allen Flügen von und in die Schweiz vor. Wie der EuGH das Datensammeln für Flüge innerhalb der EU deutlich auf besondere Fälle eingeschränkt, sollte , um der Datensparsamkeit zu genügen, auf die Daten der meisten Flüge im Schengenraum verzichtet werden.

In Abs. 2 wird eine Übermittlung der Flugpassagierdaten 48-24 Stunden vor Abflug festgelegt. Und was passiert mit Daten von Passagieren, die den Flug gar nicht antreten? Übermittlung der Daten nach Abschluss des boardings genügt.

Für die in Abs. 3 erwähnte Löschung von besonders schützenswerten Daten fehlt eine Instanz, welche solche Löschungen kontrolliert.

Abs. 4

Die technischen Einzelheiten der Datenübermittlung dem Fedpol zu überlassen geht gar nicht. Der EDÖB, gemeinsam mit dem Fedpol legt die Modalitäten fest und entscheidet endgültig.

Artikel 5

Die Übermittlung der persönlichen Daten der Flugpassagiere muss an die Passagiere klar kommuniziert werden. Klar, verständlich, mit Nennung sämtlicher Daten (einschliesslich an wen die Daten übermittelt werden) und vor der Buchung. Die Passagiere müssen bewusst einwilligen.

Artikel 6

Hä? "Schwere Straftat"? Haben Sie jetzt selber definiert, was eine schwere Straftat ist? Bevor dieser Begriff in neuen Gesetzen genutzt wird muss die Definition für alle Gesetze eindeutig geklärt sein. «und anderen schweren Straftaten» ist zu löschen.

Absatz 6 widerspricht Art. 2 Abs. 3, welcher den Luftverkehrsunternehmen verbietet besonders schützenswerte Personendaten zu übermitteln, was biometrische Daten einschliesst, und eine sofortige

Löschung bei der PIU vorsieht. Ausserdem sind biometrische Daten im Anhang 1 "Flugpassagierdaten" (inkl. dem Verweis in Punkt 18) nicht vorgesehen und sollten somit per se nicht Teil der Daten sein.

Wie genügsam bekannt, will die US-NSA diese Daten vollumfänglich abrufen, das ist zu verhindern. Also Absatz ersatzlos streichen.

Artikel 9

Das ist ja ein ganz schrecklicher Artikel in einem Gesetzesentwurf in einem demokratischen Land. Von den unklaren Definitionen (Analysen, Risikoprofile, Beobachtungslisten) einmal abgesehen nehme ich an, dass für die «Abgleiche» künstliche Intelligenz eingesetzt werden soll. Also selbstlernende Systeme, die notorisch unzuverlässig sind. Das geht nicht. Diese «Abgleiche» müssen von Menschen gemacht und kontrolliert werden.

Technologien der künstlichen Intelligenz im Rahmen selbstlernender Systeme («machine learning») sollen explizit verboten werden.

Wenn die Präzisierung der Definitionen von Analyse, Risikoprofilen und Beobachtungslisten nicht möglich ist, den Artikel 9 ersatzlos streichen.

Artikel 10

Es wird dem NDB gefallen, Passagierdaten von allen Flugstrecken zu erhalten. Mich erschreckt das ungemein. Diese offene Formulierung geht so sicher nicht. Der NDB soll sich die gewünschten Strecken von den GPK des Parlamentes genehmigen lassen.

Es sollte auch klar in dieses Gesetz geschrieben werden, dass die übermittelten Daten direkt nach einem Abgleich gelöscht werden, wenn der Abgleich erfolglos war.

Artikel 11

Komplett und ersatzlos löschen.

Artikel 12

«oder andere schwere Straftat» löschen.

Artikel 13

Da man für die Programmierung oder den Unterhalt eines solchen Systems keine richtigen Daten benötigt, ist Abs. 2, Buchstabe b ersatzlos zu streichen

Artikel 14

Weshalb 6 Monate? Sofort nach Landung Ware angebracht.

Artikel 16

6 Monate ist noch zu lange. 24 Std. nach Landung genügt vollkommen. Und zwar kontrolliert. Falls die Löschung nicht zeitgerecht erfolgt, wird sanktioniert.

Artikel 18

Absatz 2 Die Pseudonymisierung der Daten ist eine massive Schlechterstellung aller Betroffenen. Und das, wie das ganze Gesetz, absolut ohne Grund. Da es sich immer noch um besonders schützenswerte Personendaten handelt muss man weiterhin vom Auskunftsrecht Gebrauch machen können. Falls die Daten nicht wie von mir vorgeschlagen innert 24 Stunden nach Landung gelöscht werden, müssen Betroffene auf jeden Fall über den gesamten Zeitraum der Speicherung der Daten (mit oder ohne Pseudonymisierung) von ihrem Auskunftsrecht Gebrauch machen können.

Artikel 20

Also das Gesetz empfinde sich ja schon als Ganzes völlig daneben und überflüssig. Und jetzt das noch. Aus den Diskussionen über die Zuständigkeiten des Bundes und der Kantone bei der Covid19-Pandemie scheint man beim Bund etwas unsicher zu sein und will nun komplizierte Prozesse einführen.

Artikel 21

«Vergleichbar»? Wie vergleichbar? Mein Vorschlag: "soweit ihr nationales Recht mindestens einen wie in der Schweiz vorhandenen Schutz dieser Daten gewährleistet." Damit meine ich das Datenschutzgesetz (DSG) vom 25. September 2020.

Meine Schlussfolgerung: Dieses Gesetz ist überflüssig. Hört mit dieser Panikmache endlich auf!

N.B. Als Rentner habe ich nicht genügend finanzielle Mittel, um mir teure Textbearbeitungssoftware zu kaufen. Es genügt mir schon, wenn ich dazu zu einem sehr kleinen Teil mit meinen Steuern beitrage. Ich benütze daher die kostenlose Software LibreOffice. Da kann ich die Dateien in dem von Ihnen gewünschten Format vom MS Office speichern und zudem noch als PDF-Datei.

Rudolf Sommer
Flurstrasse 6
5415 Nussbaumen AG