

## 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  
Nussbaumstrasse 29  
3003 Bern

11. Dezember 2019

**Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen-Besitzstands); Vernehmlassung**

Sehr geehrte Damen und Herren

Mit Schreiben vom 9. Oktober 2019 haben Sie uns zur Vernehmlassung des obengenannten Geschäfts eingeladen.

Wir bedanken uns für diese Gelegenheit und teilen Ihnen mit, dass wir dazu keine gegenteiligen Bemerkungen haben und den erleichterten Datenaustausch zwischen den EU-Informationssystemen beziehungsweise den Entwurf des Bundesbeschlusses über die Genehmigung und Umsetzung der Notenaustausche betreffend die Übernahme und Umsetzung der beiden genannten EU-Verordnungen begrüssen.

Wir danken Ihnen für die Berücksichtigung unserer Vernehmlassung

Freundliche Grüsse

Im Namen des Regierungsrats

Dr. Urs Hofmann  
Landammann

Vincenza Trivigno  
Staatsschreiberin

Selbes Schreiben geht an

- Staatssekretariat für Migration, Quellenweg 6, 3003 Bern

Kopie

- [simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch)
- [anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)
- [sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch)
- [helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)



## 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

An die  
Adressaten gemäss Verteiler

Appenzell, 9. Januar 2020

### **Bundesbeschluss über die Genehmigung und die Umsetzung der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität (Weiterentwicklungen des Schengen-Besitzstands) Stellungnahme Kanton Appenzell I.Rh.**

Sehr geehrte Damen und Herren

Mit Schreiben vom 9. Oktober 2019 haben Sie uns die Vernehmlassungsunterlagen zum Bundesbeschluss über die Genehmigung und die Umsetzung der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität zukommen lassen.

Die Standeskommission begrüsst die Vorlage. Allerdings wird die Umsetzung der EU-Interoperabilitätsverordnungen auch bei den Kantonen zu einem finanziellen und personellen Mehraufwand führen. Diesem Mehraufwand steht jedoch der grosse Nutzen der Interoperabilität gegenüber. Die Sicherheit im Schengen-Raum wird erhöht, was einen positiven Einfluss auf die Volkswirtschaft und die Gesellschaft erwarten lässt. Insgesamt überwiegen die positiven Aspekte deutlich, sodass die Vorlage begrüsst werden kann.

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

#### **Im Auftrage von Landammann und Standeskommission**

Der Ratschreiber-Stv.:

Michael Bühler

#### *Geht an:*

- anna.wolf@fedpol.admin.ch
- simone.rusterholz@fedpol.admin.ch
- sandrine.favre@sem.admin.ch
- helena.schaer@sem.admin.ch
- 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)



Regierungsrat, 9102 Herisau

Eidg. Justiz- und Polizeidepartement  
3003 Bern

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

Herisau, 16. Dezember 2019

**Eidg. Vernehmlassung; Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei; Stellungnahme des Regierungsrates von Appenzell Ausserrhoden**

Sehr geehrte Damen und Herren

Mit Schreiben vom 9. Oktober 2019 wurden die Kantonsregierungen vom Eidgenössischen Justiz- und Polizeidepartement (EJPD) eingeladen, zu Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei bis zum 9. Januar 2020 Stellung zu nehmen.

Der Regierungsrat von Appenzell Ausserrhoden nimmt dazu wie folgt Stellung:

Der Regierungsrat unterstützt die vorliegende Weiterentwicklung des Schengen-Besitzstandes. Zu den vorgeschlagenen Gesetzesänderungen bestehen keine Bemerkungen.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse

Im Auftrag des Regierungsrates

Roger Nobs, Ratschreiber



Regierungsrat

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

Staatskanzlei, Postfach, 3000 Bern 8

Eidgenössisches Justiz- und Polizeidepartement EJPD  
Per Mail (PDF und Word) an:  
simone.rusterholz@fedpol.admin.ch  
anna.wolf@fedpol.admin.ch  
sandrine.favre@sem.admin.ch  
helena.schaer@sem.admin.ch

Ihr Zeichen:

7. Januar 2020

Unser Zeichen: 2019.POMGS.651

- - 1 2 / 2 0 2 0

RRB Nr.:

Direktion: Sicherheitsdirektion

Klassifizierung: nicht klassifiziert

**Vernehmlassung des Bundes: Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen den EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklung des Schengen-Besitzstands)  
Stellungnahme des Kantons Bern**

Sehr geehrte Frau Bundesrätin  
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Zustellung der Unterlagen und die Gelegenheit zur Stellungnahme.

Gerne teilen wir Ihnen mit, dass wir der Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) zustimmen und keine Bemerkungen anzubringen haben.

Freundliche Grüsse

**Im Namen des Regierungsrates**

Christoph Ammann  
Regierungspräsident

Christoph Auer  
Staatsschreiber

Verteiler

- Direktion für Inneres und Justiz
- Gesundheits-, Sozial- und Integrationsdirektion
- Sicherheitsdirektion
- Justizleitung
- Datenschutzaufsichtsstelle des Kantons Bern

Regierungsrat BL, Rathausstrasse 2, 4410 Liestal

Eidgenössisches Justiz- und  
Polizeidepartement, Bern

Per E-Mail an:

[simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch)

[anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)

[sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch)

[helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

Liestal, 17. Dezember 2019

### **Vernehmlassung**

**betreffend Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen-Besitzstands)**

Sehr geehrte Frau Bundesrätin

Wir bedanken uns für die Möglichkeit zur Meinungsäusserung und teilen mit, dass wir dem unterbreiteten Vorhaben zustimmen. Einerseits müssen die beiden EU-Verordnungen als Weiterentwicklungen des Schengen-Besitzstands von der Schweiz übernommen werden. Andererseits können mit der Einführung der Interoperabilität bestehende Sicherheitslücken geschlossen werden, und sie ermöglicht auch effizientere Kontrollen an den Aussengrenzen. Wir gehen davon aus, dass sich die Sicherheit im Schengen-Raum mit der Umsetzung der EU-Verordnungen verbessern wird.

Über ein gemeinsames europäisches Suchportal (ESP) werden in Zukunft alle relevanten Informationssysteme der Grenzkontroll-, Migrations- und Strafverfolgungsbehörden mit bloss einer Abfrage konsultiert werden können. Dies verbessert den Informationsaustausch und ermöglicht eine effizientere Nutzung von vorhandenen Informationen. Wir gehen davon aus, dass die Abfragen zu mehr Treffern («Hits») führen werden. Die Stärkung des europäischen Informationsaustauschs insbesondere zur Bekämpfung des Terrorismus und anderer schwerer Straftaten wird von uns begrüsst.

Abschliessend möchten wir noch darauf hinweisen, dass es für die Umsetzung der Interoperabilität unbedingt eine nationale Abfrageplattform für die polizeilichen Informationssysteme von Bund und Kantonen braucht, auf die sowohl der Bund als auch die Kantone Zugriff haben. Dafür muss noch eine bundesgesetzliche Grundlage geschaffen werden, die auch den Datenaustausch mit den Kantonen regelt. Darüber hinaus müssen auch in den Kantonen rechtliche Grundlagen für die Anbindung an diese nationale Abfrageplattform und den Informationsaustausch darüber geschaffen werden. Aus unserer Sicht wäre es sinnvoll, als Mustervorlage für einheitliche Rechtsgrundlagen in den Kantonen die im Rahmen des Polizeikonkordats Nordwestschweiz (unter Federführung der

Polizei Basel-Landschaft) geschaffene Vorlage für den Austausch polizeilicher Daten zwischen den Kantonen zu verwenden.

Hochachtungsvoll



Isaac Reber  
Regierungspräsident



Elisabeth Heer Dietrich  
Landschreiberin



Rathaus, Marktplatz 9  
CH-4001 Basel

Tel: +41 61 267 80 54  
Fax: +41 61 267 85 72  
E-Mail: staatskanzlei@bs.ch  
www.regierungsrat.bs.ch

Eidg. Justiz- und Polizeidepartement EJPD

per E-Mail an:  
*simone.rusterholz@fedpol.admin.ch*  
*anna.wolf@fedpol.admin.ch*  
*sandrine.favre@sem.admin.ch*  
*helena.schaer@sem.admin.ch*

Basel, 8. Januar 2020

**Regierungsratsbeschluss vom 7. Januar 2020**

**Vernehmlassung zur Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen-Besitzstands);  
Stellungnahme des Kantons Basel-Stadt**

Sehr geehrte Damen und Herren

Mit Schreiben vom 9. Oktober 2019 haben Sie uns die Vernehmlassungsunterlagen zum im Be-  
treff erwähnten Geschäft zukommen lassen.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und teilen Ihnen mit, dass der Kanton  
Basel-Stadt die Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der In-  
teroperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Poli-  
zei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen-  
Besitzstands) begrüsst.

Mit freundlichen Grüssen

Im Namen des Regierungsrates des Kantons Basel-Stadt

Elisabeth Ackermann  
Präsidentin

Barbara Schüpbach-Guggenbühl  
Staatsschreiberin



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

**Transmission par mail**

*Document PDF et Word à :*

Fedpol

[simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch) et

[anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)

SEM

[sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch) et

[helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

*Fribourg, le 16 décembre 2019*

**Reprise et mise en œuvre des bases légales pour l'établissement de l'interopérabilité des systèmes d'information de l'UE dans les domaines des frontières, de la migration et de la police (règlements [UE] 2019/817 et [UE] 2019/818) (développement de l'acquis de Schengen)**

Madame, Monsieur,

Par courrier du 9 octobre dernier, vous nous avez consultés sur l'objet cité en titre et nous vous en remercions.

Indépendamment du fait que la reprise des développements de l'acquis Schengen paraît s'imposer à la Suisse sous peine de risquer une cessation de l'accord d'association à Schengen, nous approuvons sans réserve cette reprise particulière.

En effet, la mise en place de cette interopérabilité entre les différents systèmes d'information améliorera grandement le travail des différents services intéressés. Nous relevons toutefois qu'à ce stade les conséquences pour les cantons ne sont pas encore précisément chiffrables, mais devraient se limiter à certaines adaptations techniques des systèmes informatiques et à de la formation des catégories de personnel concernées.

En vous remerciant une nouvelle fois de nous avoir consultés, nous vous prions de croire, Madame, Monsieur, à nos salutations les meilleures.

**Au nom du Conseil d'Etat :**

Jean-Pierre Siggen  
Président



Danielle Gagnaux-Morel  
Chancelière d'Etat



Genève, le 15 janvier 2020

## Le Conseil d'Etat

6348-2019

Département fédéral de justice et police  
Madame Karin Keller-Sutter  
Conseillère fédérale  
Palais fédéral Ouest  
3003 Berne

**Concerne : consultation fédérale sur la reprise et la mise en œuvre des bases légales pour l'établissement de l'interopérabilité des systèmes d'information de l'UE dans les domaines des frontières, de la migration et de la police (règlements [UE] 2019/817 et [UE] 2019/818) (développement de l'acquis de Schengen)**

Madame la Conseillère fédérale,

Notre Conseil a bien reçu votre lettre du 9 octobre 2019, par laquelle vous avez invité le gouvernement cantonal à se prononcer dans le cadre de la procédure de consultation citée en marge, et il vous en remercie.

En préambule, notre Conseil salue la volonté du Département fédéral de justice et police (DFJP) de vouloir accroître la sécurité intérieure dans l'espace Schengen.

Actuellement, le système d'information Schengen (SIS), la Banque de données Eurodac et le système d'information sur les visas (VIS) ne sont pas interconnectés, ce qui se traduit par un risque de pertes d'informations, une impossibilité d'accéder à certaines informations ou de les échanger.

Il convient effectivement de ne pas reproduire ces lacunes avec le système entrée/sortie (EES), le système européen d'information et d'autorisation concernant les voyages (ETIAS) et d'autres encore.

Les projets de la Confédération qui sont en cours démontrent bien la volonté d'un développement pour s'adapter aux règlements UE et atteindre les objectifs de l'interopérabilité.

Nous avons identifié que l'atteinte de ces objectifs présuppose un portail de recherche européen (ESP), un service de partage d'établissement de correspondances biométriques (BMS), un répertoire - données biographiques et biométriques - commun de données d'identité (CIR) et un détecteur d'identités multiples (MID).

Ces propositions du règlement visent à remédier aux lacunes mises en évidence lors de crises ayant affecté l'ensemble de l'UE, plus particulièrement la mise en œuvre du principe de libre circulation inhérent au bon fonctionnement de l'espace Schengen.

Grâce à une véritable interopérabilité des systèmes d'information, aujourd'hui cloisonnés, les contrôles aux frontières extérieures de l'UE seront renforcés et la sécurité à l'intérieur de l'UE devrait s'en trouver améliorée.

Cela étant, il conviendrait que l'ordonnance fédérale, qui définira la mise en place des actes d'exécution et des actes délégués de l'UE, précise avec clarté les rôles et responsabilités des différentes autorités fédérales et cantonales compétentes.

A cet égard, nous tenons également à relever que l'état d'avancement de ce projet ne permet pas d'avoir, à ce stade, une idée claire des conséquences financières et technologiques pour notre canton.

En effet, il s'agira d'évaluer les coûts possibles, induits notamment par l'augmentation des demandes spécifiques (par exemple : demande de levée d'alerte/signalement ou de précisions complémentaires à l'autorité compétente) susceptibles d'engendrer des frais de procédure et en personnel complémentaire, ainsi que par les mesures à prendre pour identifier les systèmes informatiques adaptés et réaliser les éventuels changements.

Dès lors, si des charges supplémentaires devaient ainsi être supportées par les différentes autorités cantonales dans le cadre de cette mise en œuvre, la Confédération devrait également prévoir une indemnisation ou allouer des fonds nécessaires aux cantons.

Nous vous remercions d'ores et déjà de l'attention que vous voudrez bien prêter aux observations de notre Conseil et vous prions de croire, Madame la Conseillère fédérale, à l'assurance de notre haute considération.

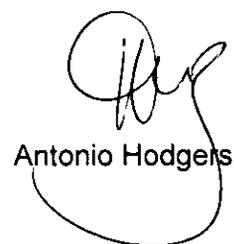
AU NOM DU CONSEIL D'ÉTAT

La chancelière :



Michele Righetti

Le président :



Antonio Hodgers

Copie à : - pour fedpol : [simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch) et [anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)  
- pour le SEM : [sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch) et [helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

**Regierungsrat**  
Rathaus  
8750 Glarus

Eidgenössisches Justiz- und  
Polizeidepartement EJPD  
Bundeshaus West  
3003 Bern

Glarus, 7. Januar 2020  
Unsere Ref: 2019-223

**Vernehmlassung zur Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818); Weiterentwicklung des Schengen-Besitzstandes**

Hochgeachtete Frau Bundesrätin  
Sehr geehrte Damen und Herren

Sie gaben uns in eingangs genannter Angelegenheit die Möglichkeit zur Stellungnahme. Dafür danken wir und teilen mit, dass die Vorlage von uns begrüsst wird. Sie ermöglicht den Einsatz von technischen Möglichkeiten, die für die Verbrechensbekämpfung und für die Eindämmung der irregulären Migration nicht nur zweckmässig, sondern auch erforderlich sind. Die Schweiz vollzieht damit eine Entwicklung nach, die in anderen Staaten bereits Realität bildet.

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

Freundliche Grüsse

**Für den Regierungsrat**

  
Dr. Andrea Bettiga  
Landammann

  
Hansjörg Dürst  
Ratsschreiber

E-Mail an: simone.rusterholz@fedpol.admin.ch; anna.wolf@fedpol.admin.ch;  
sandrine.favre@sem.admin.ch; helena.schaer@sem.admin.ch;

versandt am: **07. Jan. 2020**



Sitzung vom

10. Dezember 2019

Mitgeteilt den

11. Dezember 2019

Protokoll Nr.

902

Eidgenössisches Justiz- und  
Polizeidepartement EJPD  
Bundeshaus West  
3003 Bern

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

[simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch) und [anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)  
[sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch) und [helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

**Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen-Besitzstands)**

Sehr geehrte Frau Bundesrätin  
Sehr geehrte Damen und Herren

Mit Schreiben vom 9. Oktober 2019 erhalten die Kantone Gelegenheit, sich zu erwähntem Geschäft zu äussern. Dafür danken wir Ihnen bestens.

Die uns zugesandte Dokumentation haben wir geprüft. Die Regierung begrüsst die Vorlage zur Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818). Wir haben keine Anmerkungen.



Namens der Regierung

Der Präsident:

Dr. Jon Domenic Parolini

Der Kanzleidirektor:

i.V. lic. iur. W. Frizzoni

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

Département fédéral de justice et police (DFJP)  
A l'att. de Madame la Conseillère fédérale  
Karine 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

Transmission par courrier électronique à :

[simone.rusterholz@fedpoj.admin.ch](mailto:simone.rusterholz@fedpoj.admin.ch)

[anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)

[sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch)

[helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

Delémont, le 10 décembre 2019

**Reprise et mise en œuvre des bases légales pour l'établissement de l'interopérabilité des systèmes d'information de l'UE dans les domaines des frontières, de la migration et de la police (règlements [UE] 2019/817 et [UE] 2019/818) (développement de l'acquis de Schengen) : Ouverture de la procédure de consultation**

Madame la Conseillère fédérale,

Le Gouvernement de la République et Canton du Jura a bien reçu votre courrier du 9 octobre 2019 par lequel vous sollicitez son avis, dans le cadre de la procédure de consultation, sur le projet cité sous rubrique et son rapport explicatif.

Après avoir pris connaissance de l'ensemble des documents transmis, le Gouvernement a l'avantage de vous faire part des considérations qui suivent.

Il paraît utile en premier lieu de rappeler le cadre juridique dans lequel le présent projet intervient.

Par la signature de l'accord d'association à Schengen (AAS), la Suisse a pris l'engagement de reprendre tous les développements de l'acquis de Schengen.

En date du 20 mai 2019, le Parlement européen et le Conseil de l'Union européenne ont adopté deux règlements visant l'établissement de l'interopérabilité entre les systèmes d'information de l'UE. Il s'agit du règlement (UE) 2019/817 concernant le domaine des frontières et des visas (ci-après : règlement IOP Frontières) et le règlement (UE) 2019/818 concernant le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration (ci-après : règlement IOP Police).

Ces deux règlements ont été notifiés à la Suisse le 21 mai 2019 en tant que développements de l'acquis de Schengen.

Il est évident que si la Suisse ne mettait pas en œuvre un développement de l'acquis de Schengen, elle prendrait le risque de mettre fin à la coopération Schengen dans son ensemble et de mettre en péril la coopération Dublin.

Fort de ce constat, le Gouvernement jurassien ne peut qu'adhérer en son principe au fait que la Suisse procède aux adaptations législatives nécessaires à la reprise des développements Schengen dans le respect de ses obligations découlant de l'AAS.

Par ailleurs, il apparaît opportun de rappeler le contexte géopolitique dans lequel lesdits règlements sur l'interopérabilité ont été élaborés. Ceux-ci ont précisément été adoptés à la suite des attentats terroristes commis en 2015 dans l'espace Schengen et au regard des défis croissants dans le domaine migratoire. Avec le Conseil fédéral, le Gouvernement considère que la Suisse doit disposer des outils idoines lui permettant de lutter de manière efficace contre la criminalité et le terrorisme. Il prend ainsi bonne note que la présente reprise des développements de l'acquis de Schengen est conforme à la stratégie du Conseil fédéral dans la mesure où elle a pour finalité de pallier certains manquements existants en matière sécuritaire. Concrètement, les règlements visent l'établissement de l'interopérabilité entre les systèmes d'information de l'UE. En l'état, les différents systèmes existants ne sont pas raccordés entre eux du point de vue technique. Il existe ainsi un risque que certaines informations utiles ne soient pas décelées lorsque le système d'information dans lequel elles sont inscrites n'est pas consulté directement. Grâce à l'interopérabilité prévue, tous les systèmes d'information pourront être consultés en même temps et en une seule requête via le portail de recherche européen. En assurant ainsi une certaine connexion entre les différents systèmes d'information, les autorités de contrôle aux frontières, douanières, migratoires et de poursuite pénale gagneront indubitablement en efficacité et verront leur travail facilité, tout en améliorant la sécurité dans l'espace Schengen, ce à quoi le Gouvernement souscrit pleinement.

Le Conseil fédéral relève en outre que le présent développement de l'acquis de Schengen devrait impliquer certaines conséquences pour les autorités cantonales de police et de migration. Il précise notamment que des adaptations techniques sur les systèmes de recherche cantonale seront nécessaires, sans néanmoins en préciser les contours. Il en va de même des modifications des processus opérationnels qui pourraient être constitutifs de charge de travail supplémentaire pour les autorités cantonales concernées. Conscient des bénéfices de l'interopérabilité sur la sécurité dans l'espace Schengen, le Gouvernement aurait trouvé néanmoins opportun que le Conseil fédéral apporte des éléments plus concrets permettant de se déterminer sur l'ampleur et les coûts de la charge de travail potentielle afin de se préparer et d'anticiper au mieux les modifications législatives et techniques à venir.

Partant, au vu de l'ensemble de ce qui précède et malgré les réserves mentionnées ci-dessus, il se prononce en faveur du projet mis en consultation.

Tout en vous remerciant de l'avoir consulté, le Gouvernement vous adresse, Madame la Conseillère fédérale, l'expression de sa parfaite considération.

AU NOM DU GOUVERNEMENT DE LA  
RÉPUBLIQUE ET CANTON DU JURA

Jacques Gerber  
Président



Gladys Winkler Docourt  
Chancelière d'État



**Justiz- und Sicherheitsdepartement**

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

**Zustellung per Mail**

- Bundesamt für Polizei fedpol
- Staatssekretariat für Migration

Luzern, 17. Dezember 2019

Protokoll-Nr.: 1385

**Schengen: Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Weiterentwicklungen Schengen-Besitzstand)**

Sehr geehrte Damen und Herren

Im Namen und Auftrag des Regierungsrates teilen wir Ihnen mit, dass wir den Umsetzungs-erlass zur Interoperabilität zwischen EU-Informationssystemen begrüssen. Durch die techni-sche Verbindung der verschiedenen Systeme können Synergien genutzt werden.

Wir sind uns bewusst, dass damit mehr Kosten und Personalaufwand auf den Kanton Luzern zukommen werden. Angesichts der neuen Möglichkeiten und der Verbesserung des Informa-tionsflusses gehen wir jedoch davon aus, dass der Mehrwert diesen Aufwand rechtfertigt.

Freundliche Grüsse

Paul Winiker  
Regierungsrat



## LE CONSEIL D'ÉTAT

DE LA RÉPUBLIQUE ET  
CANTON DE NEUCHÂTEL

Département fédéral de justice et police  
Bundesrain 20  
3003 Berne

### **Reprise et mise en œuvre des bases légales pour l'établissement de l'interopérabilité des systèmes d'information de l'UE dans les domaines des frontières, de la migration et de la police (Règlements UE 2019/817 et UE 2019 /818) – Développement de l'Acquis de Schengen**

Madame, Monsieur,

Donnant suite à la procédure de consultation du 9 octobre dernier relative à l'objet susmentionné, nous vous prions de bien vouloir trouver, ci-après, la prise de position du Canton de Neuchâtel.

Au vu du sujet concerné, le service des migrations et la police neuchâteloise ont été sollicités afin d'avoir une prise de position concrète des utilisateurs des systèmes d'information de Schengen (notamment SIS et VIS).

Les principaux intéressés saluent l'amélioration envisagée des échanges d'informations qui seront rendus plus efficaces et efficaces par l'accroissement de l'interopérabilité des systèmes d'information de l'UE. Les services consultés espèrent toutefois que la Confédération développera une interface aisée et intuitive pour les utilisateurs de terrain, afin d'en faciliter le travail tant au niveau de la consultation qu'en cas de résultat positif suite à une recherche.

Bien évidemment, les applications informatiques cantonales connectées à celles de la Confédération devront être adaptées. Il est néanmoins malheureusement impossible, pour l'heure, d'évaluer la charge de travail que cela représentera.

En vous remerciant de nous avoir associés à cette procédure de consultation, nous vous prions de croire, Madame, Monsieur, à l'assurance de notre parfaite considération.

Neuchâtel, le 18 décembre 2019

Au nom du Conseil d'État :

Le président,  
A. RIBAUX

La chancelière,  
S. DESPLAND



NE



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

**PER E-MAIL**

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

Telefon 041 618 79 02  
[staatskanzlei@nw.ch](mailto:staatskanzlei@nw.ch)  
Stans, 14. Januar 2020

**Vernehmlassung in Sachen Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Weiterentwicklung des Schengen-Besitzstandes). Stellungnahme**

Sehr geehrte Frau Bundesrätin  
Sehr geehrte Damen und Herren

Mit Schreiben vom 9. Oktober 2019 haben Sie den Kanton Nidwalden in der erwähnten Angelegenheit zur Stellungnahme eingeladen. Für diese Möglichkeit zur Mitwirkung möchten wir uns bedanken. Wir vernehmen uns binnen der uns gewährten Erstreckung der Vernehmlassungsfrist.

Vorab halten wir fest, dass die Schweiz sich grundsätzlich verpflichtet hat, die Anpassungen des Schengen-Besitzstands zu übernehmen. Mit den jetzt geplanten Verknüpfungen zwischen den einzelnen Datenbanksystemen ist es zukünftig möglich, mit einer elektronischen Abfrage eine Übersicht der vorhandenen Daten zu einer bestimmten Person zu erhalten. Dies wirkt sich nicht nur positiv auf die Effizienz, sondern auch auf die Sicherheit aus, da damit das Risiko, dass wichtige Personeninformationen unerkannt bleiben oder erst verzögert zur Kenntnis kommen, verringert werden kann. Die erfragten Informationen können so schneller, effizienter und wirksamer genutzt werden. Dies ist für die involvierten Behörden zweifellos ein Mehrwert.

Die Interoperabilität sieht auch den automatisierten Abgleich biometrischer Daten einer Person vor, ermöglicht die Sammlung der biographischen und biometrischen Daten von Drittstaatsangehörigen in einem gemeinsamen Speicher und schafft neue Möglichkeiten, die wahre Identität von Personen aufzudecken, die in mehreren Informationssystemen unter falschen Identitäten oder Mehrfachidentitäten registriert sind.

Die Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei benötigt auf kantonaler Ebene Gesetzesanpassungen. Diesbezüglich hat die KKPKS bereits mit Schreiben vom 6. November 2019 an die KKJPD reagiert und eine gemeinsame, schweizerische Lösung vorgeschlagen. Dieses Vorgehen wird auch durch den Kanton Nidwalden unterstützt.

Aufgrund dieser Überlegungen befürworten wir die Vorlage. Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme bei Ihren weiteren Arbeiten.

Freundliche Grüsse  
NAMENS DES REGIERUNGSRATES



Alfred Bossard  
Landammann



lic. iur. Hugo Murer  
Landschreiber

Geht an:

- [simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch)
- [anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)
- [sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch)
- [helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)



CH-6061 Sarnen, Postfach 1561, SJD

**Per E-Mail an:**

Eidgenössisches Justiz-  
und Polizeidepartement EJPD  
3003 Bern

[simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch)  
[anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)  
[sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch)  
[helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

Referenz/Aktenzeichen: OWSTK.3622  
Unser Zeichen: fu

Sarnen, 7. Januar 2020

**Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen-Besitzstands); Stellungnahme**

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

Für die Gelegenheit der Stellungnahme zur Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei danken wir Ihnen.

Wir unterstützen grundsätzlich die Gesetzesanpassungen für die Herstellung der Interoperabilität der betroffenen Informationssysteme. Durch einen besseren und automatisierten Datenabgleich wird die Qualität der Kontrolle der Schengenaussengrenze und die Sicherheit im Schengenraum unzweifelhaft zunehmen.

Jedoch ist zu beachten, dass die neue Interoperabilität zu Mehraufwänden bei den involvierten kantonalen Behörden führen wird. Durch die neue Vernetzung der Systeme ist eine erhöhte Trefferwahrscheinlichkeit und damit letztlich auch ein erhöhter Bearbeitungsaufwand zu erwarten. Zudem müssen auch allfällige Kosten für die Anpassung der bisherigen kantonalen Datenbanken und Systeme berücksichtigt werden.

Wir bitten Sie diese Tatsache insbesondere bei den zu erwartenden Anpassungen auf Verordnungsebene zu berücksichtigen und die Kantone bei der Anpassung der Systeme finanziell zu unterstützen.

Wir danken Ihnen, sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren, für die Berücksichtigung unserer Ausführungen

Freundliche Grüsse



Christoph Amstad  
Regierungsrat

Kopie an:

- Kantonale Mitglieder der Bundesversammlung
- Volkswirtschaftsdepartement
- InformatikLeistungsZentrum Obwalden-Nidwalden
- Kantonspolizei
- Amt für Justiz
- Staatskanzlei (Kommunikation)



Regierung des Kantons St.Gallen, Regierungsgebäude, 9001 St.Gallen

Eidgenössisches Justiz-  
und Polizeidepartement  
Bundeshaus West  
3003 Bern

Regierung des Kantons St.Gallen  
Regierungsgebäude  
9001 St.Gallen  
T +41 58 229 32 60  
F +41 58 229 38 96

St.Gallen, 17. Dezember 2019

**Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen-Besitzstands); Vernehmlassungsantwort**

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 9. Oktober 2019 haben Sie uns die Übernahme und Umsetzung der EU-Verordnungen 2019/817 und 2019/818 betreffend die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei zur Vernehmlassung unterbreitet. Dafür danken wir Ihnen bestens.

Gerne teilen wir Ihnen mit, dass wir die Übernahme und Umsetzung der erwähnten EU-Verordnungen begrüßen und keine Bemerkungen haben.

Im Namen der Regierung

Heidi Hanselmann  
Präsidentin

Canisius Braun  
Staatssekretär



**Zustellung auch per E-Mail (pdf- und Word-Version) an:**  
simone.rusterholz@fedpol.admin.ch; anna.wolf@fedpol.admin.ch;  
sandrine.favre@sem.admin.ch; helena.schaer@sem.admin.ch

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

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



Regierungsrat

---

Eidgenössisches Justiz- und  
Polizeidepartement EJPD

**per E-Mail:**

simone.rusterholz@fedpol.admin.ch  
anna.wolf@fedpol.admin.ch  
sandrine.favre@sem.admin.ch  
helena.schaer@sem.admin.ch

Schaffhausen, 10. Dez. 2019

**Vernehmlassung betreffend Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen Besitzstands); Stellungnahme**

Sehr geehrte Frau Bundesrätin  
Sehr geehrte Damen und Herren

Mit Schreiben vom 9. Oktober 2019 haben Sie uns eingeladen, in vorerwähnter Angelegenheit Stellung zu nehmen. Wir danken Ihnen für diese Gelegenheit.

Der Regierungsrat begrüsst die vorgesehenen Änderungen grundsätzlich, da sie die Interoperabilität der nationalen und kantonalen Informationssysteme in der Schweiz verbessern und zu mehr Sicherheit im Schengen-Raum führen werden.

Sie gehen gemäss dem Erläuternden Bericht davon aus, dass die beantragte Neuregelung für die kantonalen Verwaltungen technische Anpassungen und neue Aufgaben mit sich bringen, die zu einem Mehraufwand führen. Diesbezüglich ersuchen wir Sie, den Kantonen zur Anpassung der kantonalen Anwendungen entsprechende technische Plattformen zur Verfügung zu stellen und die mit der beantragten Neuregelung einhergehenden Prozesse und die Schnittstellen so auszugestalten, dass die technischen, administrativen und finanziellen Aufwände für die Kantone möglichst eingegrenzt werden.

Wir danken Ihnen für die Kenntnisnahme und Berücksichtigung unserer Stellungnahme.



Freundliche Grüsse

Im Namen des Regierungsrates

Der Präsident:

A handwritten signature in blue ink, appearing to be "Ernst Landolt", written over a large, stylized blue scribble.

*Ernst Landolt*

Der Staatsschreiber:

A handwritten signature in blue ink, appearing to be "Dr. Stefan Bilger", written in a cursive style.

*Dr. Stefan Bilger*

## **Regierungsrat**

Rathaus / Barfüssergasse 24  
4509 Solothurn  
www.so.ch

Eidgenössisches Justiz- und Poli-  
zeidepartement EJPD  
3003 Bern

17. Dezember 2019

### **Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen-Besitzstands); Vernehmlassung**

Sehr geehrte Frau Bundesrätin  
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf Ihr Schreiben vom 9. Oktober 2019 in oben genannter Angelegenheit und danken Ihnen für die Gelegenheit zur Stellungnahme. Gerne äussern wir uns wie folgt:

#### A. Zweck und Inhalt der EU-Interoperabilitätsverordnungen sowie Auswirkungen auf die Sicherheit in der Schweiz

Wir unterstützen den Zweck der beiden EU-Interoperabilitätsverordnungen, den Informationsaustausch der EU-Informationssysteme in den Bereichen Grenze, Migration und Polizei zu verbessern. Das öffentliche Interesse an einer entsprechenden Optimierung ist unbestritten. Allerdings entstehen dadurch auch neue Datenschutzrisiken. Diese müssen im Auge behalten werden, die vorgesehenen Datenschutzvorgaben müssen konsequent umgesetzt werden.

Das geltende Recht erteilt den Grenzkontroll-, Migrations- und Strafverfolgungsbehörden die Zugriffsberechtigung auf verschiedene Informationssysteme der Europäischen Union. Bislang sind die verschiedenen Systeme technisch nicht miteinander verknüpft. Zur Überprüfung im konkreten Einzelfall hat die Behörde nach Massgabe ihrer Zugriffsrechte die Abfrage in jedem System einzeln vorzunehmen und gestützt auf die abgerufenen Informationen die angemessene Massnahme anzuordnen. Das Vorgehen ist ineffizient und gerade bei Gefahr in Verzug besteht das Risiko, eine Massnahme gestützt auf unvollständige Informationen anzuordnen.

Die vorgeschlagene Interoperabilität führt zur technischen Vernetzung der bestehenden EU-Informationssysteme. Der Zugriff erfolgt über ein gemeinsames Europäisches Suchportal (ESP). Die Behörde erhält mit einer Abfrage alle in den miteinander verknüpften Systemen vorhandenen Informationen. Behördliche Fehlentscheidungen aufgrund einer unvollständigen Sachverhaltsabklärung dürften dadurch vermieden werden. Auch die weiteren Massnahmen begrüessen wir (Schaffung eines gemeinsamen Dienstes zum Abgleich biometrischer Daten, eines gemeinsamen Speichers für Identitätsdaten von Drittstaatenangehörigen (CIR) sowie eines Detektors für Mehrfachidentitäten zur Bekämpfung von Identitätsbetrug).

Zum Ausgleich der weggefallenen systematischen Grenzkontrollen sieht das Schengen- Assoziierungsabkommen (SAA) verschiedene Massnahmen vor (insbesondere das Schengener-Informationssystem SIS). Die Interoperabilität und die weiteren Vorschläge stellen im Sinne zusätzlicher Kompensationsmassnahmen sachgerechte Weiterentwicklungen des Schengen-Besitzstandes dar. Im Rahmen der sicherheits- und gerichtspolizeilichen Aufgabenerfüllung zur Verhütung, Feststellung und Verfolgung von schweren Straftaten oder Terrorismus stellt das Abrufverfahren einen erheblichen Mehrwert dar. Die Optimierung des Informationsaustausches ist zur effektiven und effizienten Aufgabenerfüllung der Behörden in den Bereichen Grenze, Migration und Polizei nötig. Die einzelnen Massnahmen erachten wir als geeignet und angemessen, um Kontrollen an den Aussengrenzen effizienter auszugestalten, die irreguläre Migration gezielt zu bekämpfen und somit einen wesentlichen Beitrag zur Sicherheit im Schengen-Raum zu leisten. Die Rechte überprüfter Personen erachten wir als gewahrt.

Von der Umsetzung der EU- Interoperabilitätsverordnungen sind positive Auswirkungen auf die Sicherheit im Schengen-Raum und somit in der Schweiz zu erwarten.

#### B. Weitere Auswirkungen der Umsetzung der EU- Interoperabilitätsverordnungen

Für Bund und Kantone ist die Umsetzung der EU-Interoperabilitätsverordnungen mit finanziellem und personellem Aufwand verbunden. Aufgrund der Neuerungen der Interoperabilität ist mit Anpassungen verschiedener kantonaler Anwendungen zu rechnen. Insbesondere die Anbindung der Schweizer Systeme an das ESP macht technische Anpassungen bei den kantonalen Abfragesystemen nötig. Ein weiterer Anpassungsbedarf ist möglich, kann zum jetzigen Zeitpunkt allerdings nicht genau benannt werden.

Auch die operationellen Prozesse sind anzupassen. Bei den Grenzkontrollen an den Schengen-Aussengrenzen beispielsweise ist das ESP zwingend abzurufen, weshalb der Bundesrat mit einem entsprechend grösseren Aufwand der Grenzkontrollbehörden rechnet. An der Schengen-Aussengrenze am Flughafen Grenchen ist die Polizei Kanton Solothurn für die Durchführung der Grenzkontrollen verantwortlich. Die neu zugewiesenen Kontrollaufgaben werden bei der Polizei zu einem entsprechenden Mehraufwand führen. Da mehr Informationssysteme als früher gleichzeitig abgefragt werden, ist ausserdem - durchaus gewollt - die Chance auf einen Treffer grösser. Auch für die daraus resultierenden Folgeaufgaben ist in der Regel die Polizei zuständig. Der erläuternde Bericht geht von weiteren Prozessabläufen aus, die neu zu definieren und zu einem Mehraufwand der kantonalen Behörden führen werden. Aus verschiedenen Gründen sind momentan keine Schätzungen möglich.

In diesem Zusammenhang ersuchen wir um eine frühzeitige Einbindung der Kantone in die technischen und operationellen Anpassungsarbeiten.

Wir weisen zudem darauf hin, dass auch den Datenschutzaufsichtsbehörden zusätzliche Aufgaben zugewiesen werden und der Bund und die Kantone dafür zu sorgen haben, dass die Datenschutzaufsichtsbehörden mit den erforderlichen Ressourcen ausgestattet werden. Die Umsetzung der EU-Interoperabilitätsverordnungen hat auch in diesem Bereich finanzielle Auswirkungen.

#### C. Bemerkungen zum Projekt "Nationale Abfrageplattform NAP"

Gleichzeitig mit der Umsetzung der EU- Interoperabilitätsverordnungen soll die Interoperabilität der nationalen und kantonalen Polizeisysteme verbessert werden. Beim Projekt "Nationale Abfrageplattform NAP" handelt es sich um ein berechtigtes Anliegen der Konferenz der Kantonalen Polizeidirektoren (KKPKS), welches wir unterstützen. Die geltenden Zugriffsrechte der Behörden bleiben unverändert.

Auch die effiziente und zügige Umsetzung der NAP bedingt eine technisch und rechtlich enge Zusammenarbeit, sowohl der Kantone untereinander als auch mit dem Bund.

Abschliessend weisen wir auf den gesetzgeberischen Handlungsbedarf hin: Gemeinsam betriebene Plattformen und Abrufverfahren auf kantonale Systeme bedürfen einer Rechtsgrundlage im jeweiligen kantonalen Recht. Das gilt gleichermaßen für das ESP wie für die NAP. Ein entsprechender Koordinations- und Harmonisierungsbedarf erscheint offensichtlich. Für die angestrebte Verbesserung des Informationsaustausches stellen unterschiedliche rechtliche Regelungen ein erhebliches Risiko dar.

Aus diesen Gründen weist die KPKKS in ihrer Stellungnahme vom 6. November 2019 zur Übernahme und Umsetzung der beiden EU-Interoperabilitätsverordnungen, gerichtet an die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren der Schweiz (KKJPD), auf den Nutzen einer kantonal harmonisierten Rechtsgrundlage hin. Konkret beantragt die KPKKS, den Kantonen eine geeignete Mustervorlage für die kantonalen Gesetzesanpassungen zur Verfügung zu stellen. Zur spürbaren Optimierung des Informationsaustausches innerhalb der Schweiz und des Schengen-Raumes dürfte es sich dabei um eine unverzichtbare Voraussetzung handeln.

Gerne hoffen wir auf Berücksichtigung unserer Überlegungen.

IM NAMEN DES REGIERUNGSRATES

sig.  
Roland FÜRST  
Landammann

sig.  
Andreas Eng  
Staatschreiber

Regierungsrat des Kantons Schwyz



6431 Schwyz, Postfach 1260

**per E-Mail**

Eidgenössisches Justiz- und Polizeidepartement (EJPD)

elektronisch an fedpol: [simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch) und [anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)

elektronisch an SEM: [sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch) und [helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

Schwyz, 10. Dezember 2019

**Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) – Weiterentwicklungen des Schengen-Besitzstands**  
Vernehmlassung

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 9. Oktober 2019 haben Sie die Kantonsregierungen eingeladen, in der rubrizierten Angelegenheit bis 9. Januar 2020 Stellung zu nehmen.

Für diese Einladungen danken wir Ihnen bestens, indes verzichtet der Kanton Schwyz auf die Einreichung einer Vernehmlassung.

Im Namen des Regierungsrates:

Dr. Mathias E. Brun  
Staatsschreiber



Kopie z.K. an:

– Schwyzer Mitglieder der Bundesversammlung.

Staatskanzlei, Regierungsgebäude, 8510 Frauenfeld

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

Frauenfeld, 7. Januar 2020

## Übernahme und Umsetzung der Rechtsgrundlage für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei

### Vernehmlassung

Sehr geehrte Frau Bundesrätin

Wir danken Ihnen für die Möglichkeit zur Abgabe einer Stellungnahme zum Entwurf für einen Bundesbeschluss über die Genehmigung und die Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend Übernahme der Verordnungen (EU) 2019/817 und 2019/818 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen sowie zu den damit verbundenen Anpassungen des Ausländer- und Integrationsgesetzes (AIG; SR 142.20), des Bundesgesetzes über das Informationssystem für den Ausländer- und den Asylbereich (BGIAA; SR 142.51), des Verantwortlichkeitsgesetzes (VG; SR 170.32) und des Bundesgesetzes über die polizeilichen Informationssysteme des Bundes (BPI; SR 361) und teilen Ihnen mit, dass wir mit diesen Entwürfen grundsätzlich einverstanden sind. Für die weiteren Gesetzgebungsarbeiten bitten wir Sie indessen um nochmalige Überprüfung des vorgeschlagenen Art. 19b VG: In Abs. 1 Satz 1 wird festgehalten, dass der Bund gegenüber geschädigten Drittpersonen **ohne Nachweis einer Widerrechtlichkeit** haftet, lit. a sieht jedoch vor, dass für die Haftung eine **unrechtmässige** Speicherung erforderlich ist. Damit ist nicht klar, ob es sich bei dieser Bestimmung um eine Kausalhaftungsnorm handelt, oder ob für eine Haftung dennoch Widerrechtlichkeit vorliegen muss.

Aus datenschutzrechtlicher Sicht ist zudem zu beachten, dass einfache Gesamtabfragen erst dann ermöglicht werden, wenn ein gemeinsamer, grosser Speicher für alle Identitätsdaten erstellt wird (CIR). Dieser wird zwangsläufig sehr umfassend ausfallen. Damit ergibt sich indessen auch eine erhöhte Gefahr für den Missbrauch sowohl durch Privatpersonen wie auch durch fremde Staaten. Es ist daher angezeigt, die staatlichen

2/2

Kontrollpflichten umfassend zu regeln, damit dem Datenschutz und der Datensicherheit ein angemessener Stellenwert zukommt. So sollte in jedem einzelnen Land gewährleistet werden, dass die Daten nur zweckgebunden verwendet werden und diese nicht unrechtmässig an Dritte gelangen.

Mit freundlichen Grüssen

Der Präsident des Regierungsrates



Der Staatsschreiber

i.V.



numero			Bellinzona
11	cl	0	7 gennaio 2020
Repubblica e Cantone Ticino Consiglio di Stato Piazza Governo 6 Casella postale 2170 6501 Bellinzona telefono +41 91 814 43 20 fax +41 91 814 44 35 e-mail can-sc@ti.ch			Repubblica e Cantone Ticino

## Il Consiglio di Stato

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

anticipata per email: [simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch),  
[anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch), [sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch),  
[helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

### **Procedura di consultazione concernente il recepimento e trasposizione nel diritto svizzero delle basi legali concernenti la realizzazione dell'interoperabilità tra i sistemi d'informazione dell'UE nel settore delle frontiere, della migrazione e della polizia (regolamenti [UE] 2019/817 e [UE] 20189/818 (Sviluppi dell'acquis di Schengen)**

Gentili signore,  
Egredi signori,

abbiamo ricevuto la vostra lettera del 9 ottobre 2019 in merito alla summenzionata procedura di consultazione. L'avamprogetto del decreto federale, unitamente al relativo rapporto esplicativo sul recepimento e la trasposizione nel diritto svizzero delle basi legali concernenti la realizzazione dell'interoperabilità tra i sistemi d'informazione dell'UE nel settore delle frontiere, della migrazione e della polizia, è stato da noi esaminato in collaborazione con i servizi di polizia interessati e l'Ufficio cantonale della migrazione.

Nella fase di allestimento della risposta è stato consultato anche l'Incaricato cantonale per la protezione dei dati, che ha formulato osservazioni che divergono da quelle presentate in questo scritto. Ci permettiamo pertanto di allegare alla presente la sua presa di posizione del 12 dicembre 2019.

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

#### **1. Considerazioni generali**

In generale, l'Esecutivo cantonale accoglie favorevolmente la realizzazione dell'interoperabilità tra i vari sistemi d'informazione UE ritenuto che tale principio di interconnessione dei sistemi d'informazione centrali non può che portare indubbi vantaggi anche agli Uffici cantonali della migrazione e alle Polizie cantonali. Infatti essa permette la condivisione tempestiva e completa delle informazioni rilevanti atte alle gestioni della migrazione e alla prevenzione della migrazione irregolare, così da poter comparare in maniera intelligente ed efficiente una serie d'informazioni

utili all'attività corrente. Ad esempio è indubbia l'utilità del rilevatore delle identità multiple (MID) per scovare se una persona tenta di ottenere un permesso o un visto d'entrata, per accedere sul nostro territorio sotto false generalità, grazie alla comparazione di dati presenti nei diversi sistemi d'informazione UE. In precedenza ciò non era possibile poiché tra questi sistemi non vi era scambio d'informazioni e ciò permetteva ai malintenzionati di accedere illecitamente con un'identità di un'altra persona allo Spazio Schengen sfruttando queste lacune.

Anche per quel che concerne l'ambito di polizia, le modifiche proposte non possono che venire accolte positivamente, in quanto le stesse permettono di prevenire in modo più efficiente la violenza, la criminalità e il terrorismo e di combatterli efficacemente, colmando le attuali lacune in materia di sicurezza e consentendo l'esecuzione di controlli più efficaci alle frontiere esterne.

## **2. Considerazioni sugli articoli delle Leggi oggetto di modifica**

### **2.1 Legge federale del 16 dicembre 2005 sugli stranieri e la loro integrazione (LStrI)**

#### **Ad art. 110c cpv. 1 lett. c (Consultazione del CIR a fini di individuazione di identità multiple)**

Accogliamo favorevolmente il fatto che i Servizi cantonali della migrazione competenti in materia di visti siano contemplati tra le Autorità che possono accedere ai dati e ai riferimenti conservati nel Registro delle identità comuni (CIR), banca dati comune che raccoglie i dati inerenti all'identità dei cittadini di Stati terzi, al fine di individuare le identità multiple. Ciò contribuirà in maniera efficace e tempestiva ad evitare abusi nell'ambito del rilascio dei visti, a persone che richiedono il visto con una falsa identità con secondi fini, quali quello di giungere nel nostro Paese per compiere atti illeciti oppure per aggirare un divieto d'entrata in corso di validità.

#### **Ad art. 120d (trattamento indebito di dati personali nei sistemi d'informazione)**

Per quanto attiene alla punibilità dei funzionari con una multa fino a CHF 10'000.--, in caso di trattamento indebito dei dati personali presenti nei sistemi d'informazione UE (ORBIS, C-VIS, EES, ETIAS e CIR), non abbiamo nulla da osservare ritenuto che si tratta di un'estensione ai fini dell'interoperabilità.

### **2.2 Legge federale del 20 giugno 2003 sul sistema d'informazione per il settore degli stranieri e dell'asilo (LSISA)**

A tal proposito, lo scrivente Esecutivo cantonale saluta positivamente le modifiche e non ha particolari osservazioni da formulare.

### **2.3 Legge del 14 marzo 1958 sulla responsabilità**

Considerato come questo dispositivo di legge trovi applicazione unicamente per persone cui è conferita una carica pubblica della Confederazione, lo scrivente Consiglio non ha osservazioni da formulare in proposito.

### **2.4 Legge federale del 13 giugno 2008 sui sistemi d'informazione di polizia della Confederazione**

Come indicato in entrata, l'Autorità di polizia accoglie favorevolmente l'interoperabilità tra i sistemi d'informazione. Tale principio permette infatti di migliorare la celerità e la qualità della consultazione delle banche dati, agevolando non solo lo snellimento della procedura soprattutto ai servizi di polizia che sono tenuti a consultare le stesse diverse volte al giorno al fine di rispondere alle richieste dei colleghi della Confederazione e delle Autorità estere, ma altresì adattamenti necessari al fine di combattere efficacemente la criminalità internazionale di ogni tipo.

Si ritiene inoltre fondamentale il collegamento tra la Polizia cantonale e le Autorità preposte della migrazione, considerato come quest'ultima funga spesso da vettore di individui legati al terrorismo, in particolare di matrice islamica.

### 3. Conclusioni

Si rinnovano i ringraziamenti per averci dato la possibilità di prendere posizione nell'ambito della procedura in consultazione in parola.

Dal lato finanziario rileviamo che i Cantoni non dovrebbero venir toccati in maniera rilevante poiché il grosso dei costi informatici e di gestione sarà a carico dell'Ufficio federale di polizia (fedpol) e della Segreteria di Stato della migrazione (SEM). I costi dei Cantoni saranno limitati alle modifiche informatiche per aggiornare i vari applicativi che consentono l'accesso alle menzionate banche dati UE. Il collegamento dei sistemi svizzeri al portale di ricerca ESP richiederà ad esempio modifiche tecniche dei sistemi cantonali d'interrogazione. Dal rapporto esplicativo i costi a carico dei Cantoni al momento attuale non sono ancora quantificabili. Non è infatti ancora possibile valutare in quale misura i Cantoni saranno coinvolti, ad esempio nelle verifiche operate mediante il rilevatore delle identità multiple (MID), ritenuto che i processi concreti per la verifica dei collegamenti di questa componente centrale devono ancora essere definiti (cfr. pto. 6.3 rapporto esplicativo, pag. 60).

In questo contesto di incertezza circa l'impatto finanziario e i possibili oneri supplementari, benché compensati dai vantaggi l'introduzione del concetto di interoperabilità comporterà, lo scrivente Consiglio di Stato non può nascondere delle legittime preoccupazioni. Sarebbe infatti auspicabile una maggiore chiarezza e trasparenza in questo ambito da parte delle Autorità federali, in modo tale che i Cantoni abbiano concretamente la possibilità di valutare la portata di un simile progetto in termini economici e anche organizzativi. Ciò che attualmente non ci è possibile.

Vogliate gradire, gentili Signore ed egregi Signori, l'espressione della nostra stima.

PER IL CONSIGLIO DI STATO

Il Presidente:

  
Christian Vitta

Il Cancelliere:

  
Arnoldo Coduri

#### Allegato:

- Osservazioni del 12 dicembre 2019 dell'Incaricato cantonale della protezione dei dati.

#### Copia per conoscenza a:

- Dipartimento delle istituzioni ([di-dir@ti.ch](mailto:di-dir@ti.ch));
- Segreteria generale del Dipartimento delle istituzioni ([di-sg.ap@ti.ch](mailto:di-sg.ap@ti.ch));
- Sezione della popolazione ([di-sp.direzione@ti.ch](mailto:di-sp.direzione@ti.ch));
- Comando della Polizia cantonale ([servizio.giuridico@polca.ti.ch](mailto:servizio.giuridico@polca.ti.ch));
- Deputazione ticinese alle Camere federali ([can-relazioniesterne@ti.ch](mailto:can-relazioniesterne@ti.ch));
- Pubblicazione in Internet.



2019.286

sviluppo, il sistema di ingressi/uscite (EES, *Entry-Exit System*), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e il sistema europeo di informazione sui casellari giudiziari riguardo ai cittadini di paesi terzi (sistema ECRIS-TCN); la banca dati Interpol sui documenti di viaggio rubati o smarriti (SLTD) e i dati Europol.

### **Contenuto dei principali sistemi informatici da interconnettere**

I tre sistemi d'informazione già esistenti sono complementari e, ad eccezione del SIS, riguardano essenzialmente i cittadini di paesi terzi. Essi servono principalmente alla gestione delle frontiere, ad eccezione del SIS che ha anche accessoriamente delle funzioni di contrasto della criminalità.

Il SIS è la più grande e più diffusa piattaforma di scambio di informazioni sull'immigrazione e il contrasto della criminalità. Esso è consultato dalle autorità di polizia, di controllo delle frontiere e della immigrazione. Contiene le cartelle dei cittadini di paesi terzi cui è fatto divieto di entrare o di soggiornare nello spazio Schengen, dei cittadini dell'UE e di paesi terzi che sono scomparsi o ricercati (minori compresi) e degli oggetti ricercati (armi da fuoco, veicoli, documenti d'identità, attrezzature industriali, ecc.).

Il sistema europeo di dattiloscopia, EURODAC, contiene le impronte digitali dei richiedenti asilo e dei cittadini di paesi terzi che attraversano irregolarmente le frontiere esterne di Schengen.

Il VIS è un sistema centralizzato per lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata. Elabora i dati e le decisioni inerenti alle domande di visto per soggiorni di breve durata, a fini di visita o di transito attraverso l'area Schengen.

L'EES (Entry-Exit System) è un sistema centralizzato di gestione delle frontiere, anch'esso riguardante i cittadini di paesi terzi.

L'ECRIS è un sistema elettronico per lo scambio di informazioni sulle condanne pronunciate a carico di una determinata persona dagli organi giurisdizionali penali all'interno dell'UE. I sistemi ECRIS e Europol sono principalmente dei sistemi di contrasto della criminalità.

2019.286

**Modalità dell'interoperabilità**

L'interoperabilità tra tali sistemi avrà quattro componenti ossia, un portale di ricerca europeo («ESP»), un servizio comune di confronto biometrico («BMS comune»), un archivio comune di dati di identità («CIR») e un rilevatore di identità multiple («MID»).

L'ESP ha lo scopo di offrire un'interfaccia semplificata che fornisca risultati dell'interrogazione rapidi in modo trasparente. Ciò permetterebbe l'interrogazione simultanea dei diversi sistemi sulla base dei dati di identità (sia anagrafici sia biometrici). In altre parole, l'utente finale potrebbe effettuare un'unica ricerca e ottenere risultati da tutti i sistemi cui è autorizzato ad accedere invece di interrogare ogni sistema singolarmente.

Il BMS comune sarà uno strumento tecnico per facilitare l'identificazione di una persona che può essere registrata in più banche dati. Conserverebbe i modelli dei dati biometrici (impronte digitali e immagini del volto) contenuti nei sistemi di informazione centralizzati dell'UE (vale a dire il SIS, il sistema Eurodac, l'EES, il VIS e il sistema ECRIS-TCN). Permetterebbe, da un lato, di ricercare simultaneamente i dati biometrici conservati nei diversi sistemi e, dall'altro lato, di confrontarli.

IL CIR faciliterebbe l'identificazione delle persone anche nel territorio degli Stati membri e contribuirebbe altresì a semplificare l'accesso delle autorità di contrasto della criminalità a sistemi di informazione estranei al settore del contrasto. Il CIR conserverebbe dati anagrafici e biometrici registrati nel VIS, nel sistema ECRIS-TCN, nell'EES, nel sistema Eurodac e nell'ETIAS. I dati sarebbero conservati, logicamente separati, in base al sistema da cui provengono.

Il MID sarebbe uno strumento che permetterebbe di collegare le identità presenti nel CIR e nel SIS e conserverebbe i collegamenti tra le registrazioni. Conserverebbe i collegamenti che forniscono informazioni laddove una o più corrispondenze definite o possibili siano rilevate o qualora si utilizzi un'identità fraudolenta. Verificherebbe se i dati oggetto dell'interrogazione o i dati di partenza sono presenti in più di uno dei sistemi per individuare identità multiple (vale a dire stessa serie di dati biometrici collegati a dati anagrafici diversi o stessa/analogica serie di dati anagrafici collegati a dati biometrici diversi). Il MID evidenzierebbe le registrazioni di identità anagrafica per le quali esiste un collegamento in sistemi diversi.

## Osservazioni generali

Stante i regolamenti, le quattro componenti dell'interoperabilità mirano a fornire agli utenti autorizzati un accesso rapido, continuato, sistematico e controllato ai sistemi di informazione pertinenti, agevolare, nel territorio degli Stati membri, le verifiche di identità dei cittadini di paesi terzi, rilevare le identità multiple collegate alla stessa serie di dati e semplificare l'accesso delle autorità di contrasto a sistemi di informazione estranei al settore del contrasto. Inoltre, istituirebbero un archivio centrale di relazioni e statistiche («CRRS») e il formato universale dei messaggi («UMF») e introdurrebbero meccanismi automatizzati di controllo della qualità dei dati.

Sebbene il progetto dia l'impressione che l'interoperabilità sia la componente finale di sistemi di informazione già interamente funzionanti (o quanto meno di sistemi i cui atti giuridici istitutivi siano già «stabili» e nelle fasi finali del processo legislativo), va sottolineato che ciò non è il caso. Di fatto, come già detto sopra, tre dei sei sistemi di informazione dell'UE che i regolamenti tentano di mettere in interconnessione non sono al momento esistenti (ETIAS, ECRIS-TCN ed EES), due sono attualmente in revisione (SIS ed Eurodac) e uno sarà oggetto di revisione nel corso dell'anno (VIS). Ne consegue che, allo stato attuale, è pressoché impossibile valutare le implicazioni esatte per la protezione della vita privata e dei dati di un sistema così complesso e con così tanti «elementi mobili». Per tali motivi le modalità di salvaguardia dei diritti fondamentali in tale contesto, dovranno essere rivalutate mano a mano che i diversi strumenti giuridici interconnessi progrediranno nel corso dei processi legislativi.

Si può tuttavia già dire che, in termini sia legali sia tecnici, le proposte contenute nei regolamenti aggiungono un ulteriore livello di complessità ai sistemi esistenti nonché a quelli ancora in fase di elaborazione, le cui esatte implicazioni sono difficilmente valutabili in questa fase. Tale complessità avrà implicazioni non solo per la protezione dei dati, ma anche per la governance e la supervisione dei sistemi.

L'Incaricato riconosce che l'interoperabilità, purché attuata in modo ponderato e nel pieno rispetto dei diritti fondamentali, compresi i diritti alla vita privata e alla protezione dei dati, potrebbe rivelarsi uno strumento utile per soddisfare le necessità legittime delle autorità competenti, utilizzando sistemi di informazione su larga scala, e per contribuire allo sviluppo di una condivisione efficace ed efficiente delle informazioni.

2019.286

Preme tuttavia rilevare che l'interoperabilità non è esclusivamente o prevalentemente una scelta tecnica, ma piuttosto una scelta politica, tale da avere profonde conseguenze giuridiche e sociali, che non possono essere nascoste dietro presunte modifiche tecniche.

La decisione del legislatore dell'UE di realizzare sistemi di informazione su larga scala interoperabili mostra la tendenza a unire la normativa e gli obiettivi politici diversi dell'UE (vale a dire controlli alle frontiere, asilo e immigrazione, cooperazione di polizia e ora anche cooperazione giudiziaria in materia penale) nonché a concedere l'accesso alle banche dati del settore di contrasto della criminalità e di gestione delle frontiere ad autorità estranee a questi settori. Ciò non avrà soltanto conseguenze permanenti e profonde sulla struttura dei sistemi di informazione e sul loro modo di funzionamento, bensì cambierà altresì il modo in cui i principi giuridici in questo settore sono stati tradizionalmente interpretati, segnando pertanto un «punto di non ritorno».

Si può citare come esempio l'uso di ECRIS-TCN. Di fatto, il suo utilizzo a fini di gestione delle frontiere implicherebbe inevitabilmente l'ulteriore trattamento dei dati conservati in ECRIS-TCN per scopi diversi da quelli inizialmente previsti dall'accordo politico su ECRIS-TCN. Infatti, il sistema centrale ETIAS sarebbe in grado di interrogare i dati ECRIS-TCN per verificare se il richiedente ETIAS è una persona i cui dati sono registrati in ECRIS-TCN per reati di terrorismo e altri reati gravi. Questo uso consentirebbe inoltre a una nuova categoria di autorità competenti per la gestione delle frontiere di accedere ai dati personali contenuti nell'ECRIS-TCN. Né il regolamento ETIAS né l'accordo politico sul regolamento ECRIS-TCN (come concordato) prevedono l'uso di ECRIS-TCN ai fini della gestione delle frontiere. L'utilizzo dei dati conservati in ECRIS-TCN per la gestione delle frontiere andrebbe ben oltre le finalità definite per ECRIS-TCN nel suo atto giuridico (nella sua versione attuale). Pertanto non si può ritenere che l'estensione del campo di applicazione di ECRIS-TCN, una banca dati centralizzata contenente informazioni molto sensibili sulle persone, sia un mero adeguamento tecnico. Ciò potrebbe persino essere un esempio di "uso improprio", cioè una graduale espansione dell'uso di un sistema o database al di là dello scopo originario. Facilitare l'accesso delle autorità di contrasto della criminalità e di gestione delle frontiere a sistemi estranei al loro settore, anche se in misura limitata, ha implicazioni tutt'altro che insignificanti in termini

2019.286

di diritti fondamentali. L'accesso di routine potrebbe, a parer nostro, rappresentare una violazione del principio di limitazione delle finalità.

### **Conclusione**

Benché l'interoperabilità possa essere vista inizialmente soltanto come uno strumento per facilitare l'uso dei sistemi, le proposte introdurrebbero nuove possibilità di accesso e uso dei dati archiviati nei diversi sistemi, al fine di combattere la frode di identità, agevolare i controlli di identità nonché semplificare l'accesso delle autorità di contrasto della criminalità a sistemi di informazione estranei al settore del contrasto. In particolare, le proposte creano una nuova banca dati centralizzata che conterrebbe informazioni su milioni di cittadini di paesi terzi, compresi i loro dati biometrici. In ragione della scala della banca dati e della natura dei dati da conservarvi, le conseguenze di una violazione dei dati potrebbero danneggiare gravemente un numero potenzialmente molto elevato di persone. Qualora tali informazioni cadessero nelle mani sbagliate o fossero utilizzate in modo sbagliato, la banca dati potrebbe diventare uno strumento pericoloso per i diritti fondamentali.

Si teme in particolare che il progetto in questione porti le autorità a credere che, poiché i dati sono già registrati in un sistema, questi possono essere utilizzati regolarmente e con la stessa facilità per scopi diversi rispetto a quelli per i quali sono stati originariamente raccolti, senza esplicita giustificazione o discussione trasparente, malgrado il rischio di un maggiore impatto sulla vita delle persone. In merito si ricorda che il trattamento dei dati, anche se considerato proporzionato ad una finalità specifica, può diventare inadeguato o eccessivo quando gli stessi dati sono ulteriormente trattati per finalità aggiuntive. Inoltre, è importante ricordare che i dati personali relativi alle condanne penali sono considerati più sensibili e soggetti a speciali garanzie previste dalla legislazione sulla protezione dei dati. Pertanto, le estensioni dell'uso dei sistemi di informazione sono possibili unicamente se sono conciliabili con il principio di limitazione delle finalità, uno dei principi fondamentali della legislazione in materia di protezione dei dati. Eccezioni a questo principio sono possibili, ma solo nel rispetto di rigorose condizioni, in particolare che il trattamento dei dati per un'altra finalità sia previsto da una base legale chiara e che ciò sia necessario e proporzionato.

Trattandosi di un'acquis di Schengen le norme in questione vengono recepite senza che vi sia stato un vero e proprio dibattito in merito alla portata del problema che si in-

2019.286

tende risolvere con l'interoperabilità dei sistemi informatici a livello Svizzero, onde garantire che le misure proposte siano adeguate e proporzionate.

Pertanto è essenziale non solo incorporare garanzie legali e tecniche ma sarà fondamentale accrescere la formazione degli utenti finali in merito al corretto utilizzo dei sistemi a loro disposizione e adottare delle rigorose misure organizzative. È altresì necessario prestare particolare attenzione alla definizione delle finalità della banca dati e delle relative condizioni e modalità d'uso.

L'Incaricato desidera richiamare l'attenzione sull'attuale tendenza a confondere le diverse finalità della migrazione e della gestione delle frontiere, della sicurezza interna e della cooperazione giudiziaria in materia penale. In merito si osserva che, sebbene sia possibile realizzare sinergie tra questi settori, si tratta di settori politici diversi, con obiettivi diversi e attori chiave distinti. Pertanto, l'analisi della necessità e della proporzionalità di cui sopra dovrebbe tener conto anche dei settori d'intervento in cui le misure proposte sarebbero applicate e dei rispettivi ruoli e missioni dei principali attori coinvolti in questi settori.

Si ricorda inoltre che le nuove norme federali e cantonali in materia di protezione dei dati impongono al responsabile del trattamento di effettuare, prima del trattamento, una valutazione d'impatto sulla protezione dei dati per tutte le operazioni di trattamento che possono presentare un rischio elevato per i diritti e le libertà delle persone interessate (conformemente ai principi della protezione dei dati fin dalla fase di progettazione e della protezione dei dati per difetto). Il sistema d'informazione ETIAS e l'ECRIS-TCN comportano l'uso di queste operazioni di trattamento che possono generare un rischio elevato e richiederanno pertanto valutazioni d'impatto sulla protezione dei dati prima del trattamento. Ciò porterà alla definizione di controlli supplementari da attuare o alla modifica dei controlli esistenti sia internamente sia da parte dell'Incaricato.

Rimaniamo a disposizione per ulteriori approfondimenti e le trasmettiamo i nostri cordiali saluti.

Carine Anato



## Landammann und Regierungsrat des Kantons Uri

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

**Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen-Besitzstands); Vernehmlassung**

Sehr geehrte Frau Bundesrätin  
Sehr geehrte Damen und Herren

Mit Schreiben vom 9. Oktober 2019 laden Sie den Regierungsrat des Kantons Uri ein, zur Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) Stellung zu nehmen.

Bei der Vorlage handelt es sich um eine Übernahme einer Weiterentwicklung des Schengen-Besitzstands. Diese Übernahme und die Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen der EU und den involvierten Behörden (Grenze, Migration und Polizei) ist daher aus Sicht des Regierungsrats zu begrüßen. Die Identifizierung und Suche einer Person erfolgt heute über verschiedene Systeme/Kanäle. Eine entsprechende Zusammenlegung bzw. koordinierte sowie gezielte und effiziente Abfrage über ein europäisches Suchportal ist ebenfalls zu begrüßen und dient schliesslich der Bekämpfung der irregulären Migration. Die damit gewonnenen Synergieeffekte werden einen Beitrag für mehr Sicherheit im Schengen-Raum leisten.

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren, wir bedanken uns für die Möglichkeit zur Stellungnahme und grüssen Sie freundlich.

Altdorf, 20. Dezember 2019



Im Namen des Regierungsrats

Der Landammann

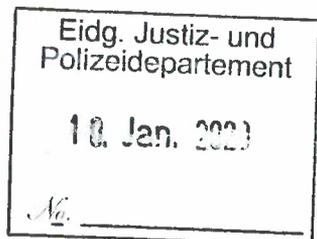
Der Kanzleidirektor

Roger Nager

Roman Balli

CONSEIL D'ETAT

Château cantonal  
1014 Lausanne



Eingang

10. Jan. 2020

fedpol Rechtsabteilung

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

Réf. : MFP/15026144

Lausanne, le 18 décembre 2019

**Consultation fédérale – Reprise et mise en œuvre des bases légales pour l'établissement de l'interopérabilité des systèmes d'information de l'EU dans le domaine des frontières, de la migration et de la police (Règlement (EU) 2019/817 et (EU) 2019/818. Développement de l'acquis Schengen - Réponse du Conseil d'Etat vaudois**

Madame la Conseillère fédérale,

Le Conseil d'Etat du Canton de Vaud vous remercie de l'avoir associé à la consultation citée en titre. Vous trouverez ci-dessous la détermination du Gouvernement vaudois à ce sujet.

Le Conseil d'Etat n'a pas de remarques particulières à formuler, dans la mesure où cette révision n'a aucune incidence directe sur la législation vaudoise. Il prend note que les adaptations légales proposées s'inscrivent dans l'échange de notes entre la Suisse et l'UE, ainsi que dans les accords d'association Schengen et Dublin du 26 octobre 2004. Il souhaite toutefois que les autorités cantonales en charge de la migration puissent également accéder pleinement à ces nouvelles banques de données.

Nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de nos sentiments les meilleurs.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE

Nuria Gorrite

LE CHANCELIER

Vincent Grandjean

**Copies**

- Mme la Conseillère d'Etat Béatrice Métraux, cheffe du DIS
- M. Stève Maucci, chef du SPOP
- M. Jacques Antenen, commandant de la Police cantonale



Département fédéral de justice et police  
Madame Karin Keller-Suter  
Conseillère fédérale  
Bundesgasse 1  
3001 Berne

Références C-39906 / CV  
Date - 4 DEC. 2019

**Procédure de consultation**

**Reprise et mise en œuvre des bases légales pour l'établissement de l'interopérabilité des systèmes d'information de l'UE dans les domaines des frontières, de la migration et de la police (règlements [UE] 2019/817 et [UE] 2019/818) (développement de l'acquis de Schengen)**

Madame la Conseillère fédérale,

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

Les règlements proposés permettront d'améliorer l'échange d'informations et participeront au maintien de la sécurité en Suisse.

Nous prenons note que les coûts des adaptations techniques nécessaires seront à la charge de l'Administration fédérale des douanes.

Pour le Valais, les contrôles aux frontières extérieures de Schengen se déroulent à l'aéroport de Sion uniquement.

Les charges de travail supplémentaires devraient être compensées par les avantages de l'interopérabilité des systèmes d'information.

Nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de nos sentiments les meilleurs.

Au nom du Conseil d'Etat

Le président

  
**Roberto Schmidt**



Le chancelier

  
**Philipp Spörri**



Sicherheitsdirektion, Postfach, 6301 Zug

**Nur per E-Mail**

Eidgenössisches Justiz- und  
Polizeidepartement EJPD  
Bundeshaus West  
3003 Bern

T direkt +41 41 728 50 33  
carmen.lingg@zg.ch  
Zug, 6. Dezember 2019 LIRM  
SD SDS 7.11 / 251

**Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818; Weiterentwicklungen des Schengen-Besitzstands)**

**Stellungnahme**

Sehr geehrte Frau Bundesrätin  
Sehr geehrte Damen und Herren

Mit Schreiben vom 9. Oktober 2019 haben Sie die Kantonsregierungen eingeladen, sich bis am 9. Januar 2020 zur obgenannten Vorlage vernehmen zu lassen. Der Regierungsrat des Kantons Zug hat die Sicherheitsdirektion mit der direkten Erledigung der Vernehmlassung beauftragt. Nach Rücksprache mit der Finanzdirektion, der Zuger Polizei, dem Amt für Migration, der Datenschutzstelle sowie dem Obergericht (inkl. Staatsanwaltschaft und Strafgericht) nehmen wir im Namen der Zuger Regierung gerne zur Vorlage Stellung.

Wir begrüssen die Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei ausdrücklich und verzichten auf Anträge.

Im Allgemeinen erlauben wir uns folgende Bemerkungen: Die zur Übernahme anstehenden EU-Verordnungen sind rechtsverbindlich. Über ein gemeinsames europäisches Suchportal (ESP) sollen inskünftig alle relevanten Informationssysteme (der Grenzkontroll-, Migrations- und Strafverfolgungsbehörden) mit bloss einer Abfrage konsultiert werden können. Dadurch wird der Informationsaustausch verbessert, vorhandene Informationen können effizienter genutzt werden und das Risiko, dass Daten bzw. Personen unerkannt bleiben, wird reduziert. Die Abfragen dürften zu mehr Treffern bzw. «Hits» führen. Die Einführung der Interoperabilität führt somit zu einer Schliessung von bestehenden Sicherheitslücken und ermöglicht effizientere Kontrollen an den Aussengrenzen. Wir gehen davon aus, dass sich die Sicherheit im Schengen-Raum mit der Umsetzung der Vorlage verbessern wird. Allerdings ist damit auch von ei-

nem gewissen Mehraufwand für die kantonalen Polizeibehörden auszugehen, nachdem diese noch enger mit den Bundesbehörden, insbesondere dem fedpol, zusammenarbeiten werden.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse  
Sicherheitsdirektion

A handwritten signature in blue ink, appearing to read 'Villiger', with a stylized flourish at the end.

Beat Villiger  
Regierungsrat

Kopie per E-Mail an:

- Fedpol (simone.rusterholz@fedpol.admin.ch und anna.wolf@fedpol.admin.ch; als PDF-Version und als Word-Version)
- SEM (sandrine.favre@sem.admin.ch und helena.schaer@sem.admin.ch; als PDF-Version und als Word-Version)
- Obergericht des Kantons Zug (felix.ulrich@zg.ch)
- Datenschutzbeauftragte (yvonne.joehri@zg.ch)
- Sicherheitsdirektion (info.sd@zg.ch)
- Zuger Polizei (kommandooffice.polizei@zg.ch)
- Amt für Migration (info.afm@zg.ch)
- Finanzdirektion (info.fd@zg.ch)
- Elisabeth Käppeli (elisabeth.kaeppli@zg.ch; zur Aufschaltung der Vernehmlassungsantwort im Internet)



Eidgenössisches Justiz- und Polizeidepartement  
3003 Bern

4. Dezember 2019 (RRB Nr. 1153/2019)

**Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818), Weiterentwicklungen des Schengen-Besitzstands; Vernehmlassung**

Sehr geehrte Frau Bundesrätin

Am 9. Oktober 2019 haben Sie uns eingeladen, zur Übernahme und Umsetzung der Verordnungen (EU) 2019/817 und (EU) 2019/818 Stellung zu nehmen.

Wir begrüssen den angestrebten verbesserten Informationsaustausch innerhalb der Informationssysteme der EU und die Möglichkeit, biometrische Daten effizienter abzugleichen. Die Schaffung eines europäischen Suchportals trägt zur Schliessung von Informationslücken und damit zu einer weiteren Qualitätssteigerung bei grenzpolizeilichen Kontrollen an den Schengen-Aussengrenzen, namentlich am Flughafen Zürich, bei. Begrüssenswert ist auch der Zugriff durch die Polizeistellen und Migrationsbehörden. Dadurch können auch Personen, die sich schon im Schengen-Raum befinden, einfacher identifiziert werden. Dies ist wichtig im Zusammenhang mit der Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten.

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

Im Namen des Regierungsrates

Die Präsidentin:

Die Staatsschreiberin:

Carmen Walker Späh

Dr. Kathrin Arioli



Eidgenössisches Polizei- und Justizdepartement  
*Sem und Fedpol*

Bern, 10.01.2020/TH/YB  
VL Interoperabilität EU

Per Mail an:

- [simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch)
- [anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)
- [sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch)
- [helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

**Bundesbeschluss über die Genehmigung und die Umsetzung der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität (Weiterentwicklungen des Schengen-Besitzstands)  
Vernehmlassungsantwort der FDP.Die Liberalen**

Sehr geehrte Damen und Herren

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

FDP.Die Liberalen begrüsst grundsätzlich die Weiterentwicklung des Schengen-Besitzstandes zur Herstellung von Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei. Den Herausforderungen im Sicherheits- und Asylbereich kann nur in Zusammenarbeit auf europäischem Niveau begegnet werden. Die Assoziierung an Schengen/Dublin ist für die Schweiz deshalb von herausragender Bedeutung. Schengen/Dublin deckt die Schweizer sicherheits- und migrationspolitischen Interessen ab und bringt klare volkswirtschaftliche und finanzielle Vorteile.

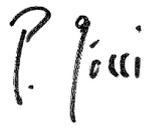
Die Herstellung von Interoperabilität zwischen verschiedenen EU-Informationssystemen (und deren Anbindung an die Schweizer Systeme) verspricht einen besseren und effizienteren Informationsaustausch in den Bereichen Grenze, Migration und Polizei. Damit werden im Schengen-Raum die Sicherheit erhöht, effizientere Grenzkontrollen ermöglicht und die Migrationssteuerung erleichtert. Die Schweiz hat gegenwärtig noch nicht zu allen EU-Informationssystemen, die mit dieser Vorlage miteinander verbunden werden sollen, Zugang. Die FDP begrüsst daher das Bestreben, Zugang zu weiteren Informationssystemen (z.B. Europol-Informationssystem) zu erhalten, damit auch die Schweizer Behörden vollständig von der Interoperabilität profitieren können. Das Kernstück dieser Schengen-Weiterentwicklung bildet das gemeinsame Suchportal (ESP) für die verschiedenen Systeme. Dieses wird es künftig erlauben, mit einer Abfrage mehrere Informationssysteme gleichzeitig zu durchsuchen. Via Suchportal können beispielsweise Migrationsbehörden in Zukunft ohne grossen Aufwand die im Visa-Informationssystem (VIS) gespeicherten Fingerabdruckdaten mit denjenigen im Schengener-Informationssystem (SIS) abgleichen. Wenn in Zukunft zum Beispiel eine kriminelle Person, deren Fingerabdrücke im SIS registriert sind, ein Visum unter falscher Identität beantragt, können die Migrationsbehörden dank dem Abgleich der Fingerabdrücke die Einreise verhindern.

Den unbestrittenen Vorteilen einer besseren Vernetzung stehen derzeit noch unklare Kosten gegenüber. Die Vorlage führt zu einem finanziellen und personellen Mehraufwand bei verschiedenen Behörden auf nationaler und kantonaler Ebene. Dieser kann aber noch nicht genau beziffert werden, da gegenwärtig noch keine technischen Spezifikationen von Seiten der EU vorliegen. Genauere Angaben zu Machbarkeit, Umsetzung und Finanzierung sind daher wünschenswert. Wir erwarten daher hierzu noch konkretere Angaben für die parlamentarische Beratung. Ferner unterstreicht die FDP die Bedeutung des Persönlichkeits- und Datenschutzes, zumal es sich bei den im Schengen-Kontext verarbeiteten Daten regelmässig um sehr sensible Personendaten handelt. Die Herstellung von Interoperabilität bedeutet nicht, dass alle Behörden Zugang zu allen Informationssystemen erhalten. Die in der Vorlage verankerten Zuständigkeitsregeln sind einzuhalten und Massnahmen gegen Missbräuche zu ergreifen. Ebenfalls erachten wir die in Kapitel 3.2 des erläuternden Berichts erwähnten Datenschutzbestimmungen als wichtig, um Missbräuchen bei der Verarbeitung von sensiblen Personendaten zu verhindern. Der Schutz sensibler Personendaten ist darüber hinaus im Verbund mit dem von den eidgenössischen Räten am 28. September 2018 verabschiedeten Schengen-Datenschutzgesetz sicherzustellen.

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

Freundliche Grüsse

FDP.Die Liberalen  
Die Präsidentin

Handwritten signature of Petra Güssi in black ink.

Petra Güssi  
Nationalrätin

Der Generalsekretär

Handwritten signature of Samuel Lanz in black ink.

Samuel Lanz



EJPD  
Staatssekretariat für Migration SEM  
[sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch)  
[helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)  
fedpol  
[simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch)  
[anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)

Sozialdemokratische Partei  
der Schweiz

Theaterplatz 4  
Postfach · 3001 Bern

Telefon 031 329 69 69  
Telefax 031 329 69 70

[info@spschweiz.ch](mailto:info@spschweiz.ch)  
[www.spschweiz.ch](http://www.spschweiz.ch)

Bern, 9. Januar 2020

## **Stellungnahme zum Bundesbeschluss über die Genehmigung und die Umsetzung der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität (Weiterentwicklungen des Schengen-Besitzstands)**

Sehr geehrte Frau Bundesrätin  
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Zustellung der Vernehmlassungsunterlagen zum Bundesbeschluss über die Genehmigung und die Umsetzung der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität. Gerne nehmen wir dazu Stellung.

**Zusammenfassung:** Die SP unterstützt die Übernahme der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität, fordert in der Umsetzung aber deutliche Nachbesserungen: Grundrechts- und Datenschutz müssen gestärkt, die Normendichte erhöht und zum Schutz der Freiheitsrechte eine unabhängige und ausreichend dotierte Aufsichtsbehörde eingerichtet werden. Zudem sind mit der EU gleichwertige Verfahren zu den Qualitätssicherungs- und Evaluationsprozessen vorzusehen.

Für die SP ist es inakzeptabel, dass der Bundesrat den objektiv vorhandenen grossen Spielraum der Schweiz zur Umsetzung von Schengen-Recht einmal mehr einseitig zugunsten der «Festung Europa», des repressiven Überwachungsstaates und zulasten der Freiheit der Bürger und Bürgerinnen wahrnimmt. Die Tatsache, dass bei einer Ablehnung einer Schengen-Vorlage durch die Schweiz sehr viel auf dem Spiel stehen würde, darf nicht dazu missbraucht werden, dass der Bundesrat mittels eines schwer verständlichen, spröde-juristischen Sachzwangdiskurses eine offene politische Debatte über Spielräume zugunsten einer Grundrechts-schonenden Umsetzung zu vermeiden versucht.

### **Die vorgesehene Interoperabilität birgt bedeutende Risiken**

Ziel der Vorlage besteht darin, die Schweiz an eine im Aufbau begriffene Infrastruktur gewaltiger Mengen höchst sensibler Daten anzudocken. Rechtliche Grundlage bilden zwei Verordnungen, die Rat und Parlament der EU im Mai 2019 nach dreijähriger Vorbereitung verabschiedet haben. Ihr Ziel ist es, die Interoperabilität zwischen neun Datenbanken aufzubauen: zu drei bestehenden und drei im Aufbau befindlichen Informationssystemen der EU im Bereich Asyl, Migration und Sicherheit sowie zu Europol-Daten und zwei Interpol-Datenbanken. Die beiden EU-Verordnungen sind fast identisch. Eine getrennte Regelung «Grenze» bzw. «Polizei» war nötig, weil nicht alle Informationssysteme auf Schengen-Recht beruhen und je unterschiedliche Staatengruppen daran teilnehmen.

**Kaum abschätzbare Folgen:** Weil bestehende Informationssysteme weiterentwickelt und andere erst neu aufgebaut werden, werden viele technische Normen und Folgeerlasse erst in den nächsten Jahren erarbeitet. Die Interoperabilität erfordert zudem den Aufbau vier so genannter «Komponenten». Die Auswirkungen des Gesamtsystems lassen sich entsprechend noch kaum abschätzen. Umso wichtiger ist die Einrichtung begleitender Evaluierungsverfahren. Die vier neuen «Komponenten» bilden ihrerseits vier gigantische, neu aufzubauende Datenbanken bzw. Plattformen:

1. Das *Europäische Suchportal* (European Search Portal, ESP) ermöglicht mit einer Abfrage die gleichzeitige Suche in neun Informationssystemen: In sechs EU-Datenbanken (Schengener Informationssystem SIS, Visa-Informationssystem VIS, Fingerabdruck Datenbank von Asylsuchenden Eurodac, Einreise/Ausreisesystem EES, Reiseinformations- und -genehmigungssystem ETIAS und Strafregisterinformationssystem für Drittstaatsangehörige ECRIS-TCN) sowie den Europol-Daten und zwei Interpol-Datenbanken. Die Schweiz hat momentan Zugang zu den fünf erstgenannten EU-Datenbanken, aber noch nicht direkt zum ECRIS-TCN und den Europol/Interpol-Daten. Dies wird zurzeit geprüft bzw. angestrebt. Die Inbetriebnahme des ESP ist auf 2023 geplant.
2. Der *Gemeinsame Dienst für den Abgleich biometrischer Daten* (Biometric Matching Service, BMS) speichert systematisch die mathematischen Abbilder («templates») aller biometrischen Daten aus dem SIS, VIS, Eurodac und EES. Mittels eines biometrischen Datensatzes können so mit einer einzigen Anfrage gleichzeitig alle vier Datenbanken durchsucht werden (in Betrieb 2021).
3. Der *Gemeinsame Speicher für Identitätsdaten* (Common Identity Repository, CIR). Alle Identitätsdaten aus VIS, Eurodac, EES, ETIAS und ECRIS-TCN werden im CIR gespeichert einschliesslich Daten zu Reisedokumenten und biometrische Daten von Drittstaatenangehörigen (in Betrieb 2022).
4. Der *Detektor für Mehrfachidentitäten* (Multiple Identity Detector, MID). Der MID ist erforderlich, weil polizeiliche Identitätsdaten aus dem SIS aus rechtlichen Gründen nicht in den CIR aufgenommen werden können (SIS ist strafrechtlich, CIR nicht). MID deckt Zusammenhänge zwischen neuen und bestehenden Identitätsdaten in allen EU-Informationssystemen auf (in Betrieb 2023).

Zusätzlich wird ein *Zentraler Speicher für Berichte und Statistiken* (Central Repository for Reporting and Statistics, CRRS) eingerichtet. Dieser wird aus allen genannten Datenbanken systematisch gefüttert. Er speichert also gigantische Mengen höchst sensibler Daten, freilich allein zu Statistikzwecken.

Der Europäische Datenschutzbeauftragte wies in seiner Stellungnahme<sup>1</sup> auf folgende Risiken hin:

**Immenses Schadenpotenzial:** Aufgrund der Grösse der zentralen Datenbanken CIR und BMS und der hochsensiblen Art der darin gespeicherten Daten kann jeder Verstoss gegen Datenschutzvorschriften einen immensen Schaden zufügen, und zwar potenziell für Millionen von Menschen.

**Erhöhte Vulnerabilität:** Je grösser Datenbanken, desto attraktiver werden sie für Hackerangriffe und Geheimdienste beispielsweise aus den USA, Russland, China oder Nordkorea.

**Unverhältnismässiges Misstrauen gegen Drittstaatsangehörige:** Die EU-Verordnungen gehen davon aus, dass Drittstaatsangehörige die Sicherheit a priori bedrohen und Identitätsbetrug weit verbreitet sei. Die mitwirkenden Staaten speichern in den Systemen konsequent sämtliche Daten von Drittstaatsangehörigen, unabhängig davon, ob es sich um blosser Reisende wie Touristen und Geschäftsleuten handelt. Um die Verhältnismässigkeit der Massnahme zu überprüfen, forderte der Europäische Datenschutzbeauftragte, zunächst das Ausmass von Identitätsbetrug unter Drittstaatsangehörigen abzuklären. Diese Zahlen sind nie vorgelegt worden und fehlen auch im erläuternden Bericht.

**Verstoss gegen den Grundsatz der Zweckbindung:** Laut Artikel 20 sind Abfragen im zentralen Speicher für Identitätsdaten CIR bereits erlaubt, «wenn Zweifel an den von einer Person vorgelegten Identitätsdaten bestehen». Derart vage Kriterien könnten, so der Datenschutzbeauftragte, zu einem routinemässigen Abruf der Daten führen, was gegen den Grundsatz der Zweckbindung verstosse.

---

<sup>1</sup> Europäischer Datenschutzbeauftragter, Stellungnahme 04/2018 zu den Vorschlägen für zwei Verordnungen über die Einrichtung eines Rahmens für die Interoperabilität von IT-Grosssystemen der EU  
[https://edps.europa.eu/sites/edp/files/publication/18-04-16\\_edps-opinion-on-interoperability\\_de.pdf](https://edps.europa.eu/sites/edp/files/publication/18-04-16_edps-opinion-on-interoperability_de.pdf)

**Aushebelung von rechtsstaatlichen Grundsätzen der Strafverfolgung:** Artikel 22 erleichtert den Strafverfolgungsbehörden den Zugriff auf Systeme, die nichts mit Strafverfolgung zu tun haben. Strafverfolgungsbehörden aus über dreissig Staaten könnten so Zugriff auf Millionen von Identitätsdaten irgendwelcher Personen erhalten, die allein eine Reise gemacht haben.

**Gegenseitige Vertrauensbasis ist brüchig geworden:** Die Interoperabilität und der erleichterte Austausch sehr grosser Mengen an hoch sensiblen Daten beruht auf dem Grundsatz des gegenseitigen Vertrauens, einem tragenden Pfeiler der europäischen Zusammenarbeit. Dieses Vertrauen ist aktuell aber erheblich erschüttert, wenn wir an Korruption in höchsten Regierungskreisen<sup>2</sup>, Mängel bei der Rechtsstaatlichkeit<sup>3</sup> und der Unabhängigkeit der Justiz<sup>4</sup> in einzelnen Mitgliedstaaten denken. Umso wichtiger sind Sicherungsmassnahmen in der nationalen Umsetzungsgesetzgebung der Schweiz.

### **Wer das Schengen-Recht einseitig umsetzt, gefährdet die Assoziation an Schengen**

**JA zur Übernahme der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität:** Würde die Schweiz die beiden Interoperabilität-Verordnungen «Grenze» bzw. «Polizei» nicht übernehmen, so würde dies die Schweizer Assoziation an Schengen in höchstem Masse gefährden. Es müsste ein in den Verträgen nicht vorgesehenes Wunder passieren, damit die Assoziation der Schweiz an Schengen nicht nach Ablauf von sechs Monaten automatisch erlöschen würde. Es wäre nicht einmal eine Kündigung erforderlich. Ohne Schengen fiel aber die grossartige Errungenschaft der europaweiten Reisefreiheit dahin. Und ohne Zugriff auf die erwähnten Datenbanken hätte die Schweiz rasch sehr grosse Probleme mit der Sicherheit, der Ein- und Ausreise, der Migration und dem Asylwesen.

**NEIN zu einer einseitigen Umsetzung zugunsten der «Festung Europa», des repressiven Überwachungsstaates und zulasten der Freiheit der Bürger und Bürgerinnen:** Trotz der erwähnten (und weiteren) Risiken der Interoperabilität-Verordnungen tritt die SP deshalb für ein Andocken der Schweiz an die vier «Komponenten» ein, welche die Interoperabilität gewährleisten. Für die SP ist es aber inakzeptabel, dass der Bundesrat den objektiv vorhandenen grossen Spielraum der Schweiz zur Umsetzung von Schengen-Recht einseitig umsetzt

- **zugunsten der «Festung Europa»:** Identifizierende biometrische Daten von Drittstaatsangehörigen werden ohne jeden Anfangsverdacht gegen eine bestimmte Person bei jeder Ein- und Ausreise systematisch erfasst, unbeschränkt lange gespeichert und aufgrund der neuen Interoperabilitätskomponenten in einem Hit/No-Hit-Verfahren erleichtert routinemässig systematisch abgefragt. Namentlich der systematische Gebrauch biometrischer Daten von Drittstaatsangehörigen bedeutet für diese eine deutliche Schlechterstellung gegenüber EU/EFTA-Bürger und Bürgerinnen.
- **zugunsten des repressiven Überwachungsstaates:** die Effizienz der Instrumente von Grenzschutzbehörden, Justiz, Polizei und Nachrichtendiensten wird durch die neue Interoperabilität deutlich erhöht. Der Vernehmlassungsentwurf ignoriert aber im EU-Recht ebenfalls enthaltene Vorgaben für eine Stärkung der Datenschutzbehörden, die Einrichtung einer unabhängigen Aufsichtsbehörde sowie Qualitätssicherungs- und Evaluationsmechanismen systematisch.

---

<sup>2</sup> Joseph Muscat, Premierminister von Malta, musste aufgrund schwerer Korruptionsvorwürfe im Gefolge der Ermordung der Journalistin Daphne Caruana Galizia seinen Rücktritt per 18. Januar 2020 bekanntgeben. Der ehemalige slowakische Staatspräsident der Slowakei, Andrej Kiska, bezeichnete sein Land im Sommer 2019 als «Mafia-Staat», nachdem bekannt wurde, dass Premierminister Robert Fico in die Ermordung des Journalisten Ján Kuciak und seine Verlobte Martina Kusnirova verwickelt war und deswegen zurücktreten musste. Der ehemalige rumänische Premierminister Liviu Dragnea ist zweifach rechtskräftig wegen Korruption verurteilt worden und sitzt jetzt im Gefängnis. Dennoch wurde die vorgängige Entlassung von Laura Kövesi als Leiterin der obersten Korruptionsbekämpfungsbehörde sowie die von Dragnea veranlassten weiteren massiven Erschwerungen zur Korruptionsbekämpfung bisher nicht rückgängig gemacht. Die Vorstellung, dass die Behörden von Malta, Polen oder der Slowakei noch einfacheren Zugriff auf Daten aus der Schweiz zugreifen könnten, trägt nicht wirklich zur Stärkung des Vertrauens und des Sicherheitsgefühls bei.

<sup>3</sup> Vgl. Vertragsverletzungsverfahren gegen Polen, EuGH, Rs. C-619/18, Kommission/Polen, [ECLI:EU:C:2019: 531](#); Kommission eröffnet Debatte zur Stärkung der Rechtsstaatlichkeit in der EU, [Medienmitteilung](#), 3.4.2019.

<sup>4</sup> Die Grosse Kammer des Europäischen Gerichtshofs EuGH urteilte am 27. Mai 2019 in einem Vorabentscheidungsverfahren, die deutschen Staatsanwaltschaften böten keine hinreichende Gewähr für Unabhängigkeit gegenüber der Exekutive, um zur Ausstellung eines Europäischen Haftbefehls befugt zu sein. Es bestehe die strukturelle Gefahr, dass Entscheide der Staatsanwaltschaft durch Anordnungen der Exekutive beeinflusst werden könnten ([Urteil vom 27.05.2019, Az. C-508/18](#)).

- **zulasten der Freiheit der Bürgerinnen und Bürger**: es fehlen planmässige und konsequente Vorkehrungen, um die Grundrechte der Bürgerinnen und Bürger im Gegenzug zur Stärkung der polizeilich-repressiven Instrumente zu schützen und so das Gleichgewicht zwischen Freiheit und Sicherheit zu wahren.

Für die SP ist klar: Die Tatsache, dass bei einer Ablehnung einer Schengen-Vorlage durch die Schweiz sehr viel auf dem Spiel stehen würde, darf nicht dazu missbraucht werden, dass mittels eines schwer verständlichen, spröde-juristischen Sachzwangdiskurses versucht wird, eine offene politische Debatte über die vorhandenen grossen Spielräume zugunsten einer Grundrechts-schonenden Umsetzung zu vermeiden. Es gibt bei der Umsetzung von Schengen-Recht Grenzen, die aus Sicht der SP nicht überschritten werden dürfen.

### **Ungenügende Verfassungsgrundlage, unklare Zuständigkeiten und Rechtsgrundlagen**

**Ungenügende materielle Verfassungsgrundlage**: Gemäss Kapitel 7.1 des erläuternden Berichtes stützt sich die Übernahme der Rechtsgrundlagen zur Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei auf Artikel 54 Absatz 1 der Bundesverfassung (BV) (die auswärtigen Angelegenheiten sind Sache des Bundes), auf Artikel 184 Absatz 2 BV (der Bundesrat unterzeichnet und ratifiziert völkerrechtliche Verträge) und Artikel 166 Absatz 2 BV (die Bundesversammlung ist für die Genehmigung völkerrechtlicher Verträge zuständig). Die Umsetzung der EU-Verordnungen geht aber weit über Aussenpolitik hinaus. Die materielle Verfassungsgrundlage bleibt im erläuternden Bericht ungeklärt.

**Weit mehr als Aussenpolitik**: Es geht beim Anschluss der Schweiz an die EU-Informationssysteme um weit mehr als um Aussenpolitik. Es geht um grundlegende Weichenstellungen, wie die Schweiz ihre Politik im Bereich Asyl, Migration und Sicherheit gestaltet. Diese Bereiche greifen tief in die Funktionsweise der Gesellschaft ein, die teilweise europäisiert wird. Es gibt kein lupenreines „Drinnein“ und „Draussen“, wie die Verfassungsartikel über die Zuständigkeiten zur Gestaltung der Aussenpolitik nahelegen. Vielmehr gibt es nur noch einen einzigen europaweiten Raum der Freiheit, der Sicherheit und des Rechts sowie die Tendenz, den repressiv-polizeilichen Schutz der Aussengrenzen massiv auszubauen. Je stärker die Schweiz in diesen Raum eingebunden ist, desto schwerer wiegt das demokratiepolitische Defizit, so lange dessen Gestaltung allein unter dem Titel „Aussenpolitik“ abgehandelt wird. Dieses Defizit würde sich im Falle eines EU-Beitritts der Schweiz deutlich verkleinern, denn dann könnten Schweizer EU-Parlamentsmitglieder, die solchen Verordnungen zustimmen, gewählt oder abgewählt werden. Solange dies nicht der Fall ist, sollte zumindest bei der Umsetzung von Schengen-Recht alles daran gesetzt werden, keine zusätzlichen demokratiepolitischen Probleme zu schaffen. Auch dazu könnte eine materielle Verfassungsgrundlage beitragen.

**Ungeklärtes Verhältnis Bund-Kantone**: Eine direkte Folge der ungenügenden Klärung der Zuständigkeiten auf Verfassungsebene besteht in einer ungeklärten Ausscheidung von Rechten und Pflichten zwischen Bund und Kantonen. Obschon die Kantone im Bereich der öffentlichen Sicherheit und der Migration bedeutende Zuständigkeiten haben, sieht der Bundesrat nach aktueller Planung eine einseitige Überwälzung der hohen Investitionskosten an den Bund vor. Salami-Taktik<sup>5</sup>, Vermeidung von ordentlichen Vernehmlassungsverfahren mit luftigen Begründungen<sup>6</sup> und fehlende explizite Klärung der Kostenausscheidung dürften alle dem Ziel dienen, kritische Rückfragen und eine politische Diskussion aus dem Weg zu gehen: solange der Bund einfach bezahlt, schweigen die Kantone. All dies geht zulasten der demokratischen Legitimität des Vorhabens, was grosse politische Risiken birgt.

<sup>5</sup> Im vorliegenden Erläuternden Bericht werden allein Kosten von 21.6 Millionen Franken ausgewiesen. In seiner Botschaft zu einem Verpflichtungskredit zur Weiterentwicklung des Schengen/ Dublin-Besitzstands vom 4. September 2019 ([19.049](#)) beantragt der Bundesrat aber einen Verpflichtungskredit von 98.7 Millionen Franken und betont, weitere 23 Millionen würden aus Eigenmitteln finanziert. Dies bedeutet in der Summe **Schengen-Informatik-Investitionen von 122 Millionen Franken**.

<sup>6</sup> Beim Verpflichtungskredit von 98.7 Millionen Franken bzw. geplanten Informatik-Investitionen von 122 Millionen Franken handelt es sich laut Bundesrat „nicht um ein Vorhaben von grosser finanzieller Tragweite“. Es könne deshalb auf „die Durchführung einer Vernehmlassung ... verzichtet werden“. Siehe Botschaft [19.049](#), Kapitel 2, Seite 6198.

**Unklarheit über das anwendbare Recht:** Übernimmt die Schweiz eine EU-Richtlinie oder eine EU-Verordnung, so wird diese in der Schweiz zum direkt anwendbaren Recht. Nach einem fast nicht nachvollziehbaren Filter werden einzelne Bestimmungen des EU-Rechts in einem Schweizer Bundesgesetz wiederholt, andere nicht. Im Vernehmlassungsentwurf ausführlich wiederholt wird etwa im neuen 14b. Kapitel des Ausländer- und Integrationsgesetzes (AIG), auf welcher Grundlage und mit welcher Funktion die vier neuen europäischen Datenbanken bzw. Plattformen ESP, BMS, CIR und MID errichtet werden. Dies wird selbst dann umschrieben, wenn das gleiche bereits in den beiden EU-Verordnungen zur Interoperabilität geregelt ist. Bedeutende Bestimmungen dieser Verordnungen über Grundrechte, Datenschutz, Aufsichtsbehörden, Evaluations- und Qualitätssicherungsmaßnahmen usw. werden aber nirgends wiederholt. Sind sie deswegen in der Schweiz nicht anwendbar, obschon es sich bei den EU-Verordnungen um direkt anwendbares Recht handelt? Wie werden diese Bestimmungen in der Schweiz angewendet, wenn der Bundesrat darauf verzichtet zu klären, welche Behörden für deren Umsetzung zuständig sind? Warum schaffen es alle Bestimmungen mit repressivem Inhalt systematisch in die Schweizer Gesetzgebung und alle Bestimmungen über den Grundrechts- und Menschenrechtsschutz nicht? Diese Problematik wird verschärft, indem die Vernehmlassungsentwurf an mehreren Stellen eine Delegationskompetenz an den Bundesrat vorsieht (siehe erläuternder Bericht, Kapitel 7.4 unter Verweis auf Art. 110h AIG und Art. 22 BPI; weiter hinten findet sich freilich kein Art. 22 BPI: der aktuelle Art. 22 BPI regelt dessen Inkrafttreten) bzw. in Kapitel 4.3.1 wird betont: «Zahlreiche Neuerungen haben demgegenüber nur Auswirkungen auf das später zu erlassende Verordnungsrecht und bleiben im Folgenden unberücksichtigt». Es wird also angekündigt, dass «zahlreiche» Bestimmungen aus den EU-Verordnungen direkt im Schweizer Verordnungsrecht umgesetzt werden. Auch dies entzieht sie einer politischen Diskussion im Schweizer Parlament.

### **Interne Kontrollstelle für Datenschutz einrichten (AIG Art. 101)**

Auch in anderen Gesetzen ging es darum, zwischen Sicherheitsanforderungen und dem Schutz der Freiheit der Bürgerinnen und Bürger eine ausgewogene Balance zu wahren. Diese Herausforderung wird im Nachrichtendienstgesetz (u.a. in Art. 45) sowie Ziffer 73 im erwähnten Bericht des Europäischen Datenschutzbeauftragten darin gesucht, dass starke institutionelle Mechanismen der Qualitätskontrolle geschaffen werden. Entsprechend regt die SP an, den Datenschutzartikel E-AIG Art. 101 um einen neuen Absatz 3 und 4 wie folgt zu ergänzen:

#### **AIG Art. 101 Datenschutz**

<sup>3</sup> Die für die Bearbeitung der Daten zuständige Behörde setzt eine interne Kontrollstelle ein. Sie wacht über

- a. für die Einhaltung hoher Qualitätsstandards;
- b. ein umfassendes Risikomanagement für Informationssicherheit;
- c. die Rechtmässigkeit, Zweckmässigkeit, Wirksamkeit und Richtigkeit der Datenbearbeitungen und überprüft stichprobenweise die Protokolle über die Nutzung der Schengen-Dublin-Informationssysteme und die Einhaltung des Datenschutzgesetzes.

<sup>4</sup> Die interne Kontrollstelle erstellt jährlich Bericht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

### **Normendichte für Abfragen des CIR zwecks Identifikation erhöhen (E-AIG Art. 110b)**

Aus Sicht des Datenschutzes gilt es namentlich zu vermeiden, dass es zu routinemässige Abfragen des CIR zwecks Identifikation kommt. Solche Abfragen müssen auf begründete Fälle beschränkt werden. Ein Grundsatz des Datenschutzes besteht darin, dass in heiklen Fragen des Datenschutzes eine ausreichende Normendichte erforderlich ist, um Fragen der Verhältnismässigkeit und Angemessenheit des Grundrechtseingriffes zu klären. Die SP erachtet die Normendichte in den sehr allgemeinen Formulierungen von Art. 110b E-AIG als zu klein und schlägt in Anlehnung an die Ziffern 48 und 83 der Empfehlungen des Europäischen Datenschutzbeauftragten folgende Ergänzung vor:

### **Art. 101b E-AIG      Abfrage des CIR zwecks Identifikation**

<sup>2</sup> ...sowie des Schutzes der inneren Sicherheit. Die Abfrage des CIR erfolgt grundsätzlich in Anwesenheit der Person, und

- a. wenn die Person zur Kooperation nicht in der Lage ist und kein Dokument vorlegen kann, aus dem ihre Identität hervorgeht, oder
- b. wenn sie die Kooperation verweigert, oder
- c. wenn der berechtigte und begründete Verdacht besteht, dass vorgelegte Dokumente falsch sind oder dass die Person über ihre Identität nicht die Wahrheit sagt.

<sup>2bis</sup> Eine Duplizierung personenbezogener Daten aus dem CIR ist untersagt.

### **Beschleunigungsgebot für die manuelle Verifizierung von Verknüpfungen im MID**

Der Europäische Datenschutzbeauftragte empfiehlt in Ziffer 92 seines Berichtes die Einführung eines festen Zeitrahmens mit konkreten Fristen und die Festlegung eines klaren Verfahrens, das eine rechtzeitige Verifizierung von Verknüpfungen im MID gewährleistet. Ungeklärte Verknüpfungen können für die betreffende Person nachteilige Folgen nach sich ziehen. Die SP regt deshalb an, im MID-Artikel 18d in einem neuen Absatz 3bis vorzusehen, dass ungeklärte Verknüpfungen innert nützlicher Frist verifiziert werden und die betreffende Person entsprechend informiert wird.

### **E-AIG Art. 18d      Manuelle Verifizierung von Verknüpfungen im MID**

<sup>3bis</sup> Die manuelle Verifizierung verschiedener Identitäten erfolgt wenn immer möglich innerhalb von zwölf Stunden nach der Feststellung und Meldung einer ungeklärten Verknüpfung. Die betreffende Person wird umgehend informiert, sofern einer solchen Mitteilung keine überwiegenden Sicherheitsinteressen entgegenstehen.

### **Schnittstellen zum Europäischen Datenschutzbeauftragten und der nationalen unabhängigen Aufsichtsbehörde klären**

Die Interoperabilitäts-Verordnungen fordern in Artikel 53 im Rahmen ihrer jeweiligen Zuständigkeiten eine aktive Zusammenarbeit zwischen den nationalen Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten, dies im Sinne einer koordinierten Aufsicht über die Nutzung der Interoperabilitätskomponenten und der Anwendung anderer Bestimmungen dieser Verordnung. Auch wenn der Europäische Datenschutzbeauftragte oder eine Aufsichtsbehörde grössere Diskrepanzen zwischen den Verfahrensweisen der Mitgliedstaaten feststellen oder unrechtmässige Übermittlungen über die Kommunikationskanäle der Interoperabilitätskomponenten bemerken, soll diese koordinierte Aufsicht einschreiten. Erstmals bis zum 12. Juni 2021 und danach alle zwei Jahre übermittelt der Europäische Datenschutzausschuss zudem einen gemeinsamen Bericht über seine Tätigkeiten bezüglich der Interoperabilitäts-Verordnungen an das Europäische Parlament, den Rat, die Kommission, Europol, die Europäische Agentur für die Grenz- und Küstenwache und eu-LISA. «Dieser Bericht enthält für jeden Mitgliedstaat ein Kapitel, das von der Aufsichtsbehörde des betreffenden Mitgliedstaats erstellt wird.», schreibt Artikel 53 der EU-Verordnungen vor. Es muss sichergestellt werden, dass dieser Bericht auch von den Schweizer Behörden und dem Schweizer Parlament zur Kenntnis genommen wird und die Schweiz ihrerseits zu diesem Bericht angemessen beiträgt.

Für die SP ist es unverständlich, weshalb diese zentrale Vorgabe der Interoperabilitäts-Verordnungen im Entwurf nicht umgesetzt wird. Namentlich ist zu klären, wer als nationale Aufsichtsbehörde die geforderte Zusammenarbeit mit dem Europäischen Datenschutzbeauftragten wahrnimmt und worin dessen Kompetenzen und Aufgaben bestehen. U.a. ist zu klären, wer zuhanden des erwähnten periodischen EU-Rechenschaftsberichtes das Schweizer Kapitel verfasst und wer den Gesamt-Bericht in der Schweiz anschliessend in welcher Form zur Kenntnis nimmt.

Diese Frage ist umso dringender, als auch innerhalb der Schweiz die Vorarbeiten zur Schaffung einer nationalen Abfrageplattform zur Verbesserung des nationalen polizeilichen Informationsaustauschs

weit vorangeschritten sind (siehe Motion [18.3592](#)). Dies wirft auch auf nationaler Ebene die Frage auf, wie angesichts der fortschreitenden Interoperabilität von polizeilichen und anderen Informationssystemen innerhalb der Schweiz und im Verkehr mit den Schengen-Dublin-Informationssystemen eine gleichmässige Kontrolle der Verarbeitung personenbezogener Daten sichergestellt werden kann.

Der Europäische Datenschutzbeauftragte hat seine rechtliche Grundlage in Artikel 75 Absatz 1 der *Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten*<sup>7</sup>. Gleichzeitig hat diese Datenschutz-Grundverordnung in Artikel 51 Absatz 1 auch die Mitgliedstaaten zur Errichtung nationaler Aufsichtsbehörden verpflichtet. Allerdings hat die Schweiz diese Verordnung nie übernommen, sondern allein die gleichzeitig erlassene *Richtlinie (EU) 2016/ 680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts*<sup>8</sup>. Dies erfolgte im Rahmen der «Schengen-Revision des Datenschutzgesetzes» ([17.059](#)).

Weil die Schweiz die EU-Datenschutz-Grundverordnung nicht übernahm, blieb ungeklärt, wer die nationale Aufsichtsbehörde im Sinne des EU-Rechts sei und ob die sanfte Stärkung des EDÖB in Ziffer 1 des Bundesgesetzes über die Umsetzung der Richtlinie (EU) 2016/680<sup>9</sup> ausreichend sei, um in der Schweiz ein mit der EU gleichwertiges, «angemessenes Datenschutzniveau» zu schaffen.

Erschwerend kommt hinzu, dass sich die Stärkung des EDÖB im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 allein auf Daten zum Aufdecken und Verfolgen von Straftaten bezog, nicht aber in Bezug auf alle weiteren Dublin-Schengen-Informationssysteme, die mit Strafverfolgung nichts zu tun haben. Diese Frage spitzte sich anlässlich des Beitritts der Schweiz zum Ein- und Ausreisensystem EES im Jahre 2018 zu.<sup>10</sup> Die SP forderte deshalb bereits damals in ihrer Stellungnahme zum EES-Vernehmlassungsentwurf die Aufwertung des EDÖB zu einer eigentlichen unabhängigen Aufsichtsbehörde, die auf Augenhöhe mit ihren Schwesterbehörden in den EU Mitgliedstaaten sowie mit dem Europäischen Datenschutzbeauftragten kommunizieren kann.<sup>11</sup>

Mit der hier vorliegenden weiteren massiven Ausweitung der Schengen-Dublin-Informationssysteme sowie der parallelen Errichtung einer nationalen Abfrageplattform für den polizeilichen Informationsaustausch wird eine solche Aufsichtsbehörde noch dringender. Ein Präzedenzfall bildet die Umsetzung der EU-VIS-Verordnung 767/2008<sup>12</sup>, die dannzumal eine «nationale Kontrollstelle» verlangte. Diese wurde gestützt auf [Art. 109e Bst. f, g und i AIG](#) in [Art. 37 Abs. 3 VISA-Informationssystem-Verordnung](#) umgesetzt, indem der EDÖB als solche bezeichnet wurde.

Aus Sicht der SP sollte eine so wichtige Frage allerdings auf Gesetzesstufe geregelt werden. Neben der Interoperabilitäts- und VIS-Verordnungen fordern auch das EES und das ETIAS eine Benennung einer Aufsichtsbehörde. Die Regelung allein auf Stufe verstreuter Einzel-Verordnungen ist der Transparenz nicht förderlich und kann dazu verleiten, den damit verbunden zusätzlichen Ressourcenbedarf beim EDÖB nicht ausreichend zu erkennen. Eine einheitliche Regelung dieser Frage für sämtliche Schengen-Dublin-Informationssysteme erleichtert zudem die Umsetzung der Berichterstattungspflichten an den Europäischen Datenschutzbeauftragten (Interoperabilitäts-Verordnung Art. 53 Abs. 3) und eine – bis heute fehlende – parallele Rechenschaftsablage an das Schweizer Parlament. Während in der EU ein mehrstufiges Aufsichts- und Oberaufsichtssystem unter Einbezug des Parlamentes besteht, fehlt in der Schweiz eine solche Aufsicht/Oberaufsicht über die Nutzung von Schengen-Dublin-Informationssystemen weitestgehend, obschon deren Risikopotenzial riesig ist.

<sup>7</sup> <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679>

<sup>8</sup> [https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AAOJ.L\\_.2016.119.01.0089.01.DEU](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AAOJ.L_.2016.119.01.0089.01.DEU)

<sup>9</sup> Bundesgesetz über die Umsetzung der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (Weiterentwicklung des Schengen-Besitzstands) vom 28. September 2018, <https://www.admin.ch/opc/de/official-compilation/2019/625.pdf>

<sup>10</sup> Bundesgesetz zur Genehmigung und Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Rechtsgrundlagen zur Errichtung und Nutzung des Einreise- und Ausreisensystems (EES) (Verordnungen [EU] 2017/2226 und 2017/2225

<sup>11</sup> [https://www.sp-ps.ch/sites/default/files/documents/18-418\\_einreise\\_ausreise-system\\_sp.pdf](https://www.sp-ps.ch/sites/default/files/documents/18-418_einreise_ausreise-system_sp.pdf)

<sup>12</sup> EU-VIS-Verordnung Art. 41, <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32008R0767>

Die SP fordert gestützt auf diese Überlegungen folgende Ergänzung:

E-AIG Art. 111k (neu) Nationale Aufsichtsbehörde und Berichterstattung

- <sup>1</sup> Nationale Aufsichtsbehörde gemäss Artikel 51 Absatz 1 der Datenschutz-Grundverordnung (EU) 2016/679 ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB).
- <sup>2</sup> Er ist im Rahmen seiner Zuständigkeiten gegenüber den Behörden weisungsberechtigt, die in der Schweiz für die Bearbeitung der Daten in den Schengen-Dublin-Informationssystemen zuständig sind.
- <sup>3</sup> Er veröffentlicht jährlich die Zahl der Anträge auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung personenbezogener Daten, die getroffenen Folgemaassnahmen und die Zahl der Berichtigungen, Löschungen und Einschränkungen der Verarbeitung, die auf Antrag der betroffenen Personen vorgenommen wurden (Artikel 51 Absatz 2 der Verordnungen (EU) 2019/8177 und (EU) 2019/8187).
- <sup>4</sup> Er arbeitet mit dem Europäischen Datenschutzbeauftragten und den übrigen nationalen Aufsichtsbehörden zusammen. Er erstattet diesen Bericht, falls er grössere Diskrepanzen zwischen den Verfahrensweisen der Mitgliedstaaten oder unrechtmässige Übermittlungen über die Kommunikationskanäle der Interoperabilitätskomponenten feststellt und zieht Schlussfolgerungen für die Schweiz aus dem Evaluierungsbericht, den die Europäische Kommission jedes Jahr zur Umsetzung der Datenqualität durch die Mitgliedstaaten erstellt (Artikel 37 Absatz 5 der Verordnungen (EU) 2019/8177 und (EU) 2019/8187).
- <sup>5</sup> Der EDÖB erstattet dem Schweizer Parlament und dem Europäischen Datenschutzbeauftragten alle zwei Jahre über die Bearbeitung der Daten in den Schengen-Dublin-Informationssystemen Bericht.
- <sup>6</sup> Er wacht im Bereich seiner Zuständigkeiten über die Umsetzung der EU-Empfehlungen über die Evaluation der Umsetzung und Anwendung des Schengen-Rechts in der Schweiz.
- <sup>7</sup> Der Bundesrat stellt sicher, dass der EDÖB als nationale Aufsichtsbehörde über ausreichende Ressourcen und Fachkenntnisse zur Wahrnehmung der Aufgaben verfügt, die ihm hier übertragen werden (Artikel 51 Absatz 4 der Verordnungen (EU) 2019/8177 und (EU) 2019/8187).

Der Europäische Datenschutzbeauftragte misst der Forderung in Absatz 7 in seinem Bericht (Ziffer 23) besondere Bedeutung zu. In Ziffer 141 betont er erneut, «dass eine Aufsicht nur wirksam sein kann, wenn für sie angemessene Ressourcen bereitstehen». Auch Artikel 51 Absatz 4 der Interoperabilitäts-Verordnungen schreibt allen mitwirkenden Staaten – also auch der Schweiz – vor, dass die nationalen Aufsichtsbehörden über ausreichende Ressourcen zur Wahrnehmung ihrer Aufgaben verfügen sollten, die ihnen gemäss dieser Verordnung übertragen werden. Der Europäische Datenschutzbeauftragte empfiehlt in Ziffer 137 ausdrücklich, eine entsprechende Bestimmung ins nationale Recht aufzunehmen. Auch dieser wichtige Passus über eine angemessene Ressourcenausstattung wird im vorliegenden Vernehmlassungsentwurf einfach ignoriert. Die SP fordert, diese Lücke zu schliessen.

Wir danken Ihnen, geschätzte Damen und Herren, für die Berücksichtigung unserer Anliegen und verbleiben mit freundlichen Grüssen

Sozialdemokratische Partei der Schweiz



Christian Levrat  
Präsident



Peter Hug  
Politischer Fachsekretär

---

## Eidgenössisches Justiz- und Polizeidepartement EJPD

Elektronisch (pdf und Word) an:

Für fedpol: simone.rusterholz@fedpol.admin.ch und anna.wolf@fedpol.admin.ch

Für SEM: sandrine.favre@sem.admin.ch und helena.schaer@sem.admin.ch

Bern, 6. Januar 2020

## Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen-Besitzstands)

### Vernehmlassungsantwort der Schweizerischen Volkspartei (SVP)

---

Sehr geehrte Damen und Herren

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

**Die SVP ist nach wie vor überzeugt, dass ihre Forderung nach systematischen Grenzkontrollen richtig ist und der blosser Nachvollzug von EU-Verordnungen im Rahmen der Schengen-Mitgliedschaft in vielerlei Hinsicht problematisch ist. Dennoch ist sie bereit, die vorliegende Weiterentwicklung des Schengen-Besitzstands und den damit verbundenen Mehraufwand mitzutragen, sofern der verbesserte Informationsaustausch zwischen den EU-Informationssystemen den versprochenen Sicherheitsgewinn tatsächlich zu erzielen vermag.**

#### Bestehende Daten besser nutzen

Trotz ihrer grundlegenden Vorbehalte gegenüber der Schweizer Schengen-Mitgliedschaft unterstützt die SVP die Einführung eines europäischen Suchportals, um die bereits vorhandenen Daten besser nutzbar zu machen und so u.a. effektiver gegen illegale Migration, Verstösse gegen Aufenthaltsauflagen, Identitätsmissbrauch etc. innerhalb des Schengen-Raums vorgehen zu können. Positiv erachtet die SVP die Schaffung eines nationalen Abfrageinstruments zur Vereinfachung der interkantonalen Polizeizusammenarbeit, womit wohl auch die von beiden Räten diskussionslos angenommene Motion Eichenberger (18.3592) umgesetzt wird. Entsprechend ist die SVP mit dem Bundesbeschluss und der damit einhergehenden Änderungen von Bundesgesetzen einverstanden. Hinsichtlich Datenschutz erachtet die SVP die Vorlage als wenig problematisch, da keine zusätzlichen Daten erhoben werden und an den Zugriffsrechten auf die einzelnen Datenbanken im Grundsatz nichts ändert. Ohnehin sind in den Datenbanken mit Ausnahme der Fahndungen im Schengener Informationssystem (SIS) sowie der Datenbanken von Europol und Interpol lediglich Angehörige von Drittstaaten verzeichnet und keine Schweizer Bürger.

### **Mehrwert nicht nur für grenzpolizeiliche Aufgaben**

Neben einer zu erwartenden Effektivitätssteigerung der Kontrollen an den Schengen-Aussengrenzen, namentlich den Schweizer Flughäfen, nimmt die SVP den geplanten Zugriff durch die Polizei- und Migrationsbehörden positiv zur Kenntnis. Dadurch können auch Personen, die sich schon im Schengen-Raum befinden, einfacher hinsichtlich der Person und des Aufenthaltsstatus identifiziert werden.

### **Mehraufwand klar ausweisen**

Die kompletten Kostenfolgen bzw. der insgesamt zu erwartende Mehraufwand durch die Bundesbehörden können zurzeit nur näherungsweise angegeben werden, solange die technischen Spezifikationen seitens der EU nicht bekannt sind. Aus Sicht der SVP ist die Erläuterung des Bundes zwar nachvollziehbar, aber umso mehr wirft das Vorgehen der EU und damit der Prozess der Rechtsübernahme im Rahmen der Schengen-Mitgliedschaft der Schweiz Fragen auf, wenn Kostenfolgen im Rahmen des Genehmigungsprozesses nur unzureichend abgeschätzt werden können. Aus diesem Grund fordert die SVP, dass der Zusatzaufwand der Weiterentwicklung fortlaufend dokumentiert wird, damit dieser bei einer Evaluation dem versprochenen Zusatznutzen klar gegenübergestellt werden kann bzw. bei einer Projektverzögerung allenfalls eine Neubeurteilung vorgenommen werden kann.

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

### **SCHWEIZERISCHE VOLKSPARTEI**

Der Parteipräsident

Der Generalsekretär



Albert Rösti  
Nationalrat



Emanuel Waeber



Die Präsidentenkonferenz

Postfach, 9023 St. Gallen  
Telefon +41 58 465 27 27  
Registrierungsnummer: 024.1  
Geschäfts-Nr. 2019-090

A-Post

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

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

simone.rusterholz@fedpol.admin.ch  
anna.wolf@fedpol.admin.ch  
sandrine.favre@sem.admin.ch  
helena.schaer@sem.admin.ch

St. Gallen, 17. Dezember 2019 / rmh

**Vernehmlassung: Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklung des Schengen-Besitzstandes)**

Sehr geehrte Frau Bundesrätin

Für Ihre Einladung vom 9. Oktober 2019 zur Stellungnahme im oben erwähnten Vernehmlassungsverfahren danken wir Ihnen bestens. Wir haben den Entwurf mit Interesse zur Kenntnis genommen.

In der vorliegenden Angelegenheit verzichtet das Bundesverwaltungsgericht auf eine Stellungnahme. Wir bitten Sie, bei der Auswertung der Vernehmlassung die Antwort des Bundesverwaltungsgerichts als Enthaltung und nicht als Zustimmung auszuweisen.

Mit vorzüglicher Hochachtung

Die Vorsitzende der  
Präsidentenkonferenz

Nina Spälti Giannakitsas



Der stellvertretende  
Generalsekretär

Bernhard Fasel

Kopie an:

- Bundesgericht
- Bundesstrafgericht
- Bundespatentgericht



Frau Anna Wolf  
Eidgenössisches Justiz- und Polizeidepartement EJPD  
Abteilung Internationale Beziehungen, EU und Stab  
Büro G1A-E/F-04.247  
Guisanplatz 1a, 3003 Bern

Bern, 28. Oktober 2019

### **Verzicht Stellungnahme**

Sehr geehrte Frau Wolf

Wir danken Ihnen für die Möglichkeit zur Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) Stellung zu nehmen.

Der VSAA verzichtet auf eine Stellungnahme.

Besten Dank für die Kenntnisnahme  
Freundliche Grüsse

### **Verband Schweizerischer Arbeitsmarktbehörden VSAA**

Peter Kalbermatten  
Vize-Präsident

Ursula Kraft  
Direktorin

Bundesamt für Justiz  
Sekretariat für Migration  
Quellenweg 6  
3003 Bern

E-Mail:

[simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch)

[anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)

[sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch)

[helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

Bern, 9. Januar 2020

**Vernehmlassungsantwort zur Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklung des Schengen-Besitzstands)**

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

Wir danken Ihnen für die Möglichkeit, zur Übernahme und Umsetzung der oben genannten EU-Rechtsgrundlagen Stellung nehmen zu können. Es geht dabei um eine Weiterentwicklung des Schengen-Besitzstands, die bezweckt, die EU-Informationssysteme so miteinander zu vernetzen, dass vorhandene Informationen besser genutzt werden können. Die Schweiz ist als Schengen-Mitglied zur Übernahme der EU-Verordnungen 2019/817 und 2019/818 verpflichtet.

Der Schweizerische Gewerkschaftsbund SGB hat sich bisher immer hinter das Schengen-Abkommen gestellt und respektiert die Notwendigkeit der Übernahme der genannten Verordnungen. Der unterbreiteten Vorlage steht er jedoch kritisch gegenüber. Die zugrundeliegende Sammlung, Bearbeitung, Speicherung und Weitergabe sensibler Daten in diesem Umfang ist problematisch. Wir fordern deshalb, bei der Umsetzung den Grundsatz der Verhältnismässigkeit zu wahren und dem Schutz der Daten von Betroffenen genügend Rechnung zu tragen. Es sollen nur Regelungen eingeführt werden, die vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) geprüft, beurteilt und gutgeheissen wurden.

Die den beiden EU-Verordnungen zu Grunde liegende Tendenz, Migration hauptsächlich unter dem Aspekt der inneren Sicherheit zu betrachten, erachtet der SGB als höchst problematisch. Dabei werden Migrationskontrolle und die Bekämpfung von Kriminalität und Terrorismus begrifflich gleichgesetzt. Drittstaatsangehörige erscheinen so ohne jeden empirischen Nachweis per se als Sicherheitsrisiko, was eine nicht zu rechtfertigende Diskriminierung darstellt.

Der SGB unterstützt deshalb die Stellungnahme der Schweizerischen Flüchtlingshilfe SFH und fordert bei der Umsetzung insbesondere folgende Nachbesserungen und Präzisierungen:

- Explizit festzuhalten ist, dass eine Behörde, die eine Abfrage über den gemeinsamen Dienst für den Abgleich biometrischer Daten (sBMS) einleitet, nur die Verweise auf jene EU-Informationssysteme sieht, zu deren Zugang sie berechtigt ist.

- Es ist eine präzisere und genau abgegrenzte Definition der Zwecke vorzunehmen, für die eine Abfrage des gemeinsamen Speichers für Identitätsdaten (CIR) zulässig ist, damit die Erfordernisse der Notwendigkeit und der Verhältnismässigkeit erfüllt sind.
- Es ist ein ergänzender Verweis auf die Anforderungen zur Vermeidung jeder Form von Diskriminierung explizit ins Gesetz aufzunehmen.
- Die Garantien zum Schutz des Grundrechts auf Achtung des Privat- und Familienlebens und des Grundrechts auf Schutz personenbezogener Daten ist soweit als möglich zu gewährleisten und im Gesetz entsprechend zu präzisieren.
- Auf Gesetzesstufe ist zu präzisieren, dass es sich bei «sonstigen schweren Straftaten» im Sinne von Art. 110d Abs. 1 E-AIG um Straftaten mit einer Mindestfreiheitsstrafe von 3 Jahren handeln muss.
- Die nationale Polizeibehörde eines Herkunftslandes darf unter keinen Umständen Informationen darüber erhalten, dass ihre Datenbanken über das Europäische Suchportal (ESP) abgefragt wurden – insbesondere nicht im Falle anerkannter Flüchtlinge und jener Personen, die in Eurodac als Asylsuchende registriert sind.
- Die Schnittstellen zur europäischen und zur nationalen Aufsichtsbehörde sowie zum neuen Schengen-Datenschutzgesetz muss auf Gesetzesstufe geklärt und geregelt werden, um dem Datenschutz und der Datensicherheit die nötige Nachachtung zu verschaffen.
- Die nationale Aufsichtsbehörde bzw. der EDÖB sollte mit den erforderlichen (zusätzlichen) Ressourcen ausgestattet werden, damit die Aufsichtsfunktion auch angemessen wahrgenommen werden kann.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen bei Fragen gern zur Verfügung.

Freundliche Grüsse

**SCHWEIZERISCHER GEWERKSCHAFTSBUND**



Pierre-Yves Maillard  
Präsident



Regula Bühlmann  
Zentralsekretärin

AsyLex  
Gotthardstrasse 52  
8002 Zürich  
info@asylex.ch

Frau Bundesrätin  
Karin Keller-Sutter  
Vorsteherin des Eidgenössischen  
Justiz- und Polizeidepartements EJPD  
Bundeshaus West  
CH- 3003 Bern

simone.rusterholz@fedpol.admin.ch  
anna.wolf@fedpol.admin.ch  
sandrine.favre@sem.admin.ch  
helena.schaer@sem.admin.ch

Zürich, den 9. Januar 2020

**Vernehmlassung zum «Bundesbeschluss über die Genehmigung und die Umsetzung der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität (Weiterentwicklung des Schengen-Besitzstandes)»**

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

Im Namen des Vereins AsyLex bedanken wir uns für die Möglichkeit zur Stellungnahme zum Bundesbeschluss über die Genehmigung und die Umsetzung der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität (Weiterentwicklung des Schengen-Besitzstandes). Nachfolgend finden Sie unsere Stellungnahme.

Mit freundlichen Grüssen



Théoda Woeffray  
Public Relations AsyLex

## 1. Das Wichtigste in Kürze

- **Generell nehmen wir der durch die Verordnungen [EU] 2019/817 und [EU] 2019/818 eingeführte Interoperabilität eine kritische Haltung ein.** Die Interoperabilität ist aus unserer Sicht ein weiterer Schritt in Richtung des «gläsernen Bürgers», beziehungsweise gläsernen Migranten. Diese Entwicklung verlangt nach einer Stärkung und Konkretisierung der Massnahmen im Bereich des Datenschutzes, welche wir in der Vorlage grossteils vermissen.
- Wir befürchten in Bezug auf die Interoperabilität unter anderem ein **vergrössertes Missbrauchsrisiko** in Bezug auf Datenschutzrechte und dem dringendst notwendigen Persönlichkeitsschutz. Dies leiten wir von der Untergrabung des Grundsatzes der Zweckbindung ab.
- Der **Detektor für Mehrfachidentitäten** ist unseres Erachtens aus Datenschutzgründen besonders heikel und birgt ein erhöhtes Fehlerrisiko. Eine derartige Anwendung kann den datenschutzrechtlichen Anforderungen nicht gerecht werden und insbesondere vor dem Hintergrund der Verhältnismässigkeit einer Prüfung nicht standhalten.
- Die vorgesehenen Änderungen haben überdies eine weitere **Diskriminierung und Stigmatisierung von Drittstaatenangehörigen** zur Folge. Das gesamte Gesetzespaket geht von der Grundannahme aus, dass Drittstaatenangehörige als Gefahr für Europa, und insbesondere die Schweiz, zu qualifizieren sind. Die daraus resultierende Diskriminierung ist nicht hinnehmbar und folglich zu verhindern.
- Die durch die Interoperabilität vorgesehene Konsolidierung der Daten birgt ein **erhöhtes Risiko in Sachen Datenmissbrauch durch Dritte** (Hacking). In Anbetracht dessen, dass es sich um teils höchst sensible Daten von Menschen handelt, die teils aus autoritären Staaten flüchten mussten, ist dies höchstproblematisch.
- Die in der Vorlage vorgesehenen **Vorkehrung zur Wahrung des Datenschutzes** sind unzureichend und müssen zwingend im Gesetz festgehalten werden.
- Die für Datenschutzverletzungen **vorgesehenen Sanktionen** sind als unverhältnismässig tief zu beurteilen. In Anbetracht des zu schützenden Rechtsguts ist eine Busse als Strafdrohung schlicht bei Weitem nicht ausreichend.

## 2. Generelle Gründe

**Generell nehmen wir der durch die Verordnungen [EU] 2019/817 und [EU] 2019/818 eingeführte Interoperabilität eine kritische Haltung ein.** Breits in der Vergangenheit haben wir uns des Öfteren kritisch zu den verschiedenen Informationssystemen wie dem SIS und ETIAS, insbesondere hinsichtlich der Verknüpfung dieser, geäussert<sup>1</sup>. Die Interoperabilität ist aus unserer Sicht ein weiterer Schritt in Richtung des «gläsernen Bürgers», beziehungsweise gläsernen Migranten. Dies ist sehr bedauernswert, da Asylsuchende und Flüchtlinge besonders verwundbar sind und eine verstärkte «Durchleuchtung» dieser Personen, die Verwundbarkeit zusätzlich verstärkt. Diese Entwicklung verlangt aus diesen Gründen nach einer Stärkung und Konkretisierung der Massnahmen im Bereich des Datenschutzes, welche wir in der Vorlage grossteils vermissen. Dieser Ausgleich in Bezug auf den Datenschutz erscheint uns demzufolge als unabdingbar.

## 3. Konkrete Gründe

### 3.1. Vergrössertes Missbrauchsrisiko in Bezug auf Datenschutzrechte

Zudem befürchten wir in Bezug auf die Interoperabilität unter anderem ein vergrössertes Missbrauchsrisiko in Bezug auf Datenschutzrechte und dem dringendst notwendigen Persönlichkeitsschutz. Die Verknüpfung verschiedener Datensysteme (SIS, VIS, Eurodac, ETIAS, EES, etc.) bedeutet, dass die Zweckbestimmung der verschiedenen Systeme entfällt. Jede dieser EU-Datenbanken wurde für jeweils ganz spezifische Zwecke eingerichtet. Die in der Vorlage dargelegte Interoperabilität ermöglicht es, Daten neu für Zwecke zu nutzen, die ursprünglich nie vorgesehen waren. Dies ist sehr bedauernswert und widerspricht dem Grundrecht auf Schutz der persönlichen Daten, beziehungsweise ist diesbezüglich als unverhältnismässig zu qualifizieren. Der Zugang auf sensible persönliche Daten immer weiter auszuweiten fördert demzufolge den Missbrauch und widerspricht dem dringendst notwendigen Persönlichkeitsschutz, den insbesondere geflüchtete Menschen bedürfen.

In diesem Kontext birgt auch das europäische Suchportal (ESP) als Suchschnittstelle ein erhöhtes Missbrauchsrisiko. Das ESP kann beispielsweise zur Abfrage zweier

---

<sup>1</sup> Vgl. «Vernehmlassungsantwort – Übernahme und Umsetzung der Verordnung (EU) 2018/1240 über die Einrichtung eines Europäischen Reiseinformations- und genehmigungssystems (ETIAS) (Weiterentwicklung des Schengen-Besitzstands) und Änderung des Ausländer- und Integrationsgesetzes (AIG)» vom 19. Mai 2019 und «Vernehmlassungsantwort - Übernahme und Umsetzung der Rechtsgrundlagen zur Nutzung des Schengener Informationssystems (SIS) (Verordnungen [EU] 2018/1862, [EU] 2018/1861 und [EU] 2018/1860) (Weiterentwicklungen des Schengen-Besitzstands); und Änderung des BGIAA zur Registrierung der Landesverweisung im ZEMIS sowie zur Verbesserung der Statistik über Rückkehrentscheidungen» vom 19. Mai 2019.

Interpol-Datenbanken, wie der Datenbank für gestohlene und verlorene Reisedokumente («Stolen and Lost Travel Documents», SLTD) und der Datenbank «Travel Documents Associated with Notices» (TDAWN) eingesetzt werden. Da diese Datenbanken mit den Informationen der nationalen Polizeibehörden in den 194 Mitgliedsländern gespiesen werden, besteht die Möglichkeit, dass die nationalen Behörden, welche die Ausschreibung eingegeben haben, bei einem Treffer über den Zeitpunkt sowie den Ort der Abfrage informiert werden. Wurde beispielsweise ein Reisedokument eines Asylsuchenden oder eines Flüchtlings durch die Behörden im Herkunftsstaat in einer Interpol-Datenbank ausgeschrieben, besteht die Möglichkeit, dass letztere Informationen über den Aufenthaltsort des Asylsuchenden oder Flüchtlings preisgegeben werden können. Dies hat möglicherweise nicht nur für die betroffene Person schwerwiegende Konsequenzen, aber setzt auch deren Familienangehörige einer erhöhten Gefahr aus. Aus diesem Grund ist es aus unserer Sicht unerlässlich, dass einerseits der Dateneigentümer (in diesem Fall die nationale Behörde des Herkunftslandes) unter keinen Umständen Informationen darüber erhalten, dass seine Datenbanken über das ESP abgefragt wurden. Andererseits ist aus diesen Gründen auch verstärkt darauf zu achten, dass Behörden jeweils nur Zugriff auf die für sie vorgesehenen Daten erhalten können.

### **3.2. Detektor für Mehrfachidentitäten**

Der Detektor für Mehrfachidentitäten ist unseres Erachtens aus Datenschutzgründen besonders heikel. Basierend auf minimalsten Hinweisen können so Personen zueinander in Verbindung gebracht werden, welche faktisch nichts miteinander zu tun haben. Insbesondere Personen mit gebräuchlichen Namen könnten davon überproportional stark betroffen sein. Unklar in der Verordnung bleibt zudem, wie mit Personen, welche rechtmässig mehrere Identitäten haben (Personen, welche nach einer Eheschliessung den Namen des Ehepartners angenommen haben, DoppelbürgerInnen), umgegangen werden muss. Die Fehlerquote bei derartigen Applikationen ist erwiesenermassen im heutigen Zeitpunkt noch sehr hoch, sodass eine derartige Anwendung den datenschutzrechtlichen Anforderungen nicht gerecht werden kann und insbesondere vor dem Hintergrund der Verhältnismässigkeit einer Prüfung nicht standhalten kann.

### **3.3. Diskriminierung von Drittstaatenangehörigen**

Wie wir bereits in unseren Stellungnahmen zu ETIAS und dem SIS betont haben, empfinden wir diese Informationssysteme, und nun vor allem auch deren Verknüpfung als Instrument der Festigung der europäischen Aussengrenze. Die Idee, dass die europäische Aussengrenze gefestigt werden muss, verfestigt die Annahme, dass sich Europa und die Schweiz vor Drittstaatenangehörigen verstärkt schützen muss. Die vorgesehenen Änderungen haben dadurch eine weitere Diskriminierung und Stigmatisierung von Drittstaatenangehörigen zur Folge. Das gesamte Gesetzespaket

geht von der Grundannahme aus, dass Drittstaatenangehörige als Gefahr für Europa, und insbesondere die Schweiz, zu qualifizieren sind. Während deren Daten quer durch ganz Europa mit völlig unzureichenden Datenschutzvorkehrungen herumgereicht werden dürfen, bleibt der Datenschutz für EU-Bürger und Bürgerinnen, inkl. Schweizer Bürger und Bürgerinnen, weitgehend gewahrt. Selbstverständlich ist Letzteres zu begrüßen, die eklatante Diskriminierung von Drittstaatenangehörigen hingegen ist nicht hinnehmbar und folglich zu verhindern.

### **3.4. Erhöhung der Risiken in Bezug auf Datenmissbrauch durch Dritte**

Es ist zudem zu beachten, dass eine derartige Konsolidierung der Daten eine erhebliche Erhöhung der Risiken in Sachen Datenmissbrauch durch Dritte, zum Beispiel Hacking, impliziert. Aus der Vorlage ist nicht ersichtlich, wie mit diesem erhöhten Risiko umgegangen wird. In Anbetracht dessen, dass es sich um teils höchst sensible Daten handelt (zu denken ist insbesondere an persönliche Daten von Menschen, welche aus einem autoritären Staat flüchten mussten), ist es unabdingbar, dass klare Notfallszenarien im Falle eines Hacker-Angriffs vorhanden sind. Diese Szenarien müssen sorgfältig und detailliert durchdacht und so gut wie möglich vorhergesehen werden.

### **3.5. Mangelnde Vorkehrungen in Bezug auf Datenschutz**

Gemäss Vernehmlassungsentwurf übernimmt und setzt die Schweiz den Auf- und Ausbau der EU-Informationssysteme vollumfänglich um. In Bezug auf den Datenschutz werden jedoch kaum gleichwertige Vorkehrungen getroffen. Im Kapitel zum Datenschutz fehlen zentrale Bestimmungen. Es kann auch nicht hingenommen werden, dass im erläuternden Bericht hierzu lediglich auf die künftigen Verordnungen verwiesen wird. Derartig starke Eingriffe in die höchstpersönlichen Rechte bzw. die Verpflichtungen der Behörden, ein Minimum an Datenschutz zu gewährleisten, müssen zwingend auf gesetzlicher Ebene festgelegt werden. Aus diesem Grund sollten unserer Ansicht nach zumindest die Grundzüge des Datenschutzes ins Gesetz aufgenommen werden.

### **3.6. Unzureichende Sanktionen bei Datenschutzverletzungen**

Die für Datenschutzverletzungen vorgesehenen Sanktionen sind als unverhältnismässig tief zu beurteilen. In Anbetracht des zu schützenden Rechtsguts ist eine Busse als Strafdrohung nicht ausreichend. In Anbetracht der Konsequenzen, welche ein Asylsuchender oder eine Asylsuchende im Falle eines Datenmissbrauchs (z.B. Informationenerhalt des autoritären Heimatstaates) zu ertragen hat, erscheint eine Haftung als wenig wirksam, verhältnismässig und abschreckend. Die Möglichkeit eines höheren Strafmasses muss gesetzlich definiert und festgehalten werden.



Secrétariat général

[simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch)  
[anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)

[sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch)  
[helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

Département fédéral de Justice et Police

A l'att. de Madame Karin Keller-Sutter,  
Conseillère fédérale

Genève, le 07 janvier 2020  
3414/KE - FER N°01-2020

**Reprise et mise en œuvre des bases légales pour l'établissement de l'interopérabilité des systèmes d'information de l'UE dans les domaines des frontières, de la migration et de la police (règlements [UE] 2019/817 et [UE] 2019/818) (développement de l'acquis de Schengen)**

Madame la Conseillère fédérale,

La Fédération des Entreprises Romandes (FER) vous remercie de l'avoir consultée et vous fait part de sa prise de position d'ordre général.

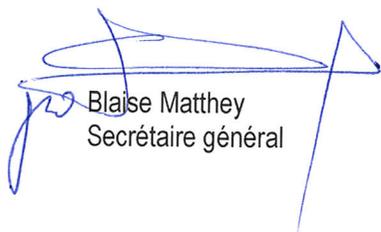
En préambule, nous tenons à rappeler notre soutien en faveur des accords bilatéraux. En tant qu'organisation économique avec plus de 45'000 membres en Suisse romande, nous défendons un accès privilégié au marché intérieur de l'Union européenne (UE), notre premier client, et le développement de relations étroites avec l'UE. Dans ce contexte, l'association de la Suisse à Schengen représente, d'une part, un intérêt économique réel et, d'autre part, une importance considérable en termes de sécurité intérieure.

En signant l'accord d'association à Schengen, la Suisse s'est engagée à reprendre les développements de l'acquis de Schengen, ce qui lui permet de maintenir les avantages de la coopération Schengen.

De plus, la reprise des deux règlements de l'UE sur l'interopérabilité représente un intérêt intrinsèque. Permettre l'interopérabilité signifie relier les systèmes d'informations de l'UE entre eux pour mieux utiliser les informations qui y figurent. Cet échange de données facilité dans les domaines des frontières, de la migration et de la police améliorera la sécurité dans l'espace Schengen et permettra de combler des lacunes existantes en la matière.

Nous apportons dès lors notre appui à la reprise et à la mise en œuvre des bases légales pour l'établissement de l'interopérabilité des systèmes d'information de l'UE dans les domaines des frontières, de la migration et de la police.

En vous remerciant par avance de l'intérêt portée à ces lignes, nous vous prions de recevoir, Madame la Conseillère fédérale, l'expression de notre haute considération.



Blaise Matthey  
Secrétaire général



Catherine Lance Pasquier  
Directrice adj. Politique générale  
FER Genève

#### **La Fédération des Entreprises Romandes en bref**

Fondée le 30 juillet 1947 à Morat, son siège est à Genève. Elle réunit six associations patronales interprofessionnelles cantonales (GE, FR, NE, JU, VS), représentant la quasi-totalité des cantons romands. La FER comprend plus de 45'000 membres.



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

Per Mail an:

Für fedpol:

[simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch)

[anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)

Für SEM:

[sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch)

[helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

Bern, 9. Januar 2020

14.02.01/hof

## **Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei**

Sehr geehrte Frau Bundesrätin  
Sehr geehrte Damen und Herren

Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) dankt Ihnen für die Möglichkeit zur Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) Stellung nehmen zu können.

Die KKJPD stimmt dem vorliegenden Entwurf des Bundesbeschlusses über die Genehmigung und Umsetzung der Notenaustausche zur Übernahme und Umsetzung der EU-Verordnungen zu. Die Weiterentwicklung und der Ausbau der IT-Struktur der EU werden als zentrale Elemente zur Verbesserung der Sicherheit im Schengen-Raum angesehen. Zudem verweisen wir auf die Stellungnahmen der Vereinigung der kantonalen Migrationsämter (VKM) vom 19. Dezember 2019 und der Konferenz der kantonalen Polizeikommandanten (KKPKS) vom 5. Dezember 2019. Wir bitten Sie, die Stellungnahmen der beiden Fachkonferenzen bei den weiteren Arbeiten zu berücksichtigen.

Freundliche Grüsse

Urs Hofmann  
Präsident



KONFERENZ DER KANTONALEN POLIZEIKOMMANDANTEN

Der Präsident

Per E-Mail an

[simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch)

[anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)

[sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch)

[helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

Bern, 5. Dezember 2019 / pyke

**Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen-Besitzstands): Stellungnahme der KKPKS**

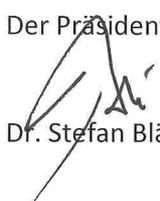
Sehr geehrte Frau Bundesrätin  
Sehr geehrte Damen und Herren

Die Konferenz der Kantonalen Polizeikommandanten der Schweiz KKPKS bedankt sich bestens für die Möglichkeit, zur Übernahme und Umsetzung der beiden im Betreff erwähnten EU-Verordnungen Stellung nehmen zu können.

Die KKPKS stimmt den geplanten für die Übernahme und Umsetzung nötigen rechtlichen Massnahmen vorbehaltlos zu und hat demzufolge keine Anmerkungen anzubringen.

Freundliche Grüsse

Der Präsident

  
Dr. Stefan Blättler

Per E-Mail an:  
[simone.rusterholz@fedpol.admin.ch](mailto:simone.rusterholz@fedpol.admin.ch)  
[anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)  
[sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch)  
[helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch)

Basel, 9. Januar 2020

**Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen-Besitzstands)**

Sehr geehrte Damen

Das vorliegende Geschäft weist einen direkten Bezug zum Thema Datenschutz auf, weshalb sich privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, zu den interessierten Kreisen zählt und wie folgt Stellung nimmt:

Im Erläuternden Bericht (S. 29) wird zu Recht auf folgende Verpflichtung der Schweiz hingewiesen: «Die Schengen-Staaten haben dafür zu sorgen, dass die Aufsichtsbehörden die Rechtmässigkeit der Datenverarbeitung unabhängig überwachen können. Dazu müssen sie die Aufsichtsbehörden mit ausreichenden Ressourcen und Fachkenntnissen ausstatten und die für die Überwachung nötigen Informationen zur Verfügung stellen. Die Aufsichtsbehörden müssen jährlich die Anzahl Anfragen auf Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten sowie die getroffenen Folgemaassnahmen veröffentlichen. Mindestens alle vier Jahre müssen sie die Datenverarbeitungsvorgänge nach einschlägigen internationalen Standards prüfen».

Die im Jahr 2018 von den zuständigen Organen der EU durchgeführte Evaluation der Anwendung des Schengen-Besitzstands im Bereich Datenschutz durch die Schweiz ergab, dass die personelle und finanzielle Ressourcenausstattung sowohl des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) als auch der geprüften kantonalen Aufsichtsstelle nicht ausreicht, um alle Aufgaben im Rahmen des Schengen-Besitzstands zu erfüllen (Durchführungsbeschluss 7281/19 des Rates der EU vom 8. März 2019). In den meisten anderen Kantonen verhält es sich genau gleich, und mit den neuen Abfragemöglichkeiten und entsprechend erhöhtem Kontrollbedarf wird sich die Situation weiter verschärfen.

Vor diesem Hintergrund ist der Bedarf der Datenschutzaufsichtsstellen nach ausreichenden – d.h. gegenüber heute erhöhten – Ressourcen nicht nur unter den materiellen Erläuterungen zu den EU-Verordnungen anzusprechen, sondern auch unter Ziff. 6.3 (Auswirkungen auf Kantone und Gemeinden) auszuweisen.

Wir danken Ihnen für die Berücksichtigung unseres Anliegens. Für Rückfragen stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Freundliche Grüsse



Beat Rudin  
Präsident privatim

# **Bundesbeschluss über die Genehmigung und die Umsetzung der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität (Weiterentwicklungen des Schengen- Besitzstands)**

Vernehmlassungsantwort der Schweizerischen  
Flüchtlingshilfe

Bern, 9. Januar 2020

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung .....</b>	<b>3</b>
<b>2</b>	<b>Das Wichtigste in Kürze .....</b>	<b>4</b>
<b>3</b>	<b>Kommentar zu den wichtigsten Bestimmungen.....</b>	<b>5</b>
3.1	Grundsätzliche Anmerkungen .....	5
3.2	Umsetzung EU-Verordnungen «IOP Grenzen» und «IOP Polizei» .....	7
3.2.1	Gemeinsamer Dienst für den Abgleich biometrischer Daten (sBMS) (Art. 110 E-AIG; Art. 18a E-BPI).....	7
3.2.2	Gemeinsamer Speicher für Identitätsdaten (CIR) (Art. 110a ff. E-AIG) .....	8
3.2.3	Europäisches Suchportal (ESP) (Art. 110e E-AIG; Art. 18b E-BPI).....	11
3.2.4	Detektor für Mehrfachidentitäten (MID) (Art. 110f und 110g E-AIG; Art. 18c und 18d E-BPI).....	11
3.2.5	Datenschutz und Datensicherheit.....	12

## Impressum

Herausgeberin  
Schweizerische Flüchtlingshilfe SFH  
Postfach, 3001 Bern  
Tel. 031 370 75 75  
Fax 031 370 75 00  
E-Mail: [info@fluechtlingshilfe.ch](mailto:info@fluechtlingshilfe.ch)  
Internet: [www.fluechtlingshilfe.ch](http://www.fluechtlingshilfe.ch)  
Spendenkonto: PC 30-1085-7

Sprachversionen  
Deutsch

COPYRIGHT  
© 2020 Schweizerische Flüchtlingshilfe SFH, Bern  
Kopieren und Abdruck unter Quellenangabe erlaubt.

# 1 Einleitung

Die Schweizerische Flüchtlingshilfe (SFH) bedankt sich für die Gelegenheit zur Antwort auf die Vernehmlassung zum «Bundesbeschluss über die Genehmigung und die Umsetzung der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität (Weiterentwicklungen des Schengen-Besitzstandes)». Sie nimmt im Folgenden zu den für sie wichtigsten Punkten Stellung. Wird zu einem Punkt nicht Stellung genommen, so ist dies nicht als Zustimmung zu werten.

Die EU forciert seit 2016 mit Hochdruck die Einrichtung intelligenter Grenzen (*smart borders*) sowie den Auf- und Ausbau von Datenbanken zur Strafverfolgung und Migrationskontrolle. Dabei demonstrieren die Schengen/Dublin-Mitgliedstaaten hier umso stärker ihren gemeinsamen Handlungswillen, je mehr es in der europäischen Asyl- und Migrationspolitik an Solidarität mangelt. Im Eiltempo werden daher in der europäischen Gesetzgebung die Rechtsgrundlagen dafür geschaffen, die die Schweiz nun Schritt für Schritt nachvollzieht. Die zwei EU-Verordnungen 2019/817<sup>1</sup> (Verordnung «IOP Grenzen») und 2019/818<sup>2</sup> (Verordnung «IOP Polizei») bilden gewissermassen das Herzstück dieser Entwicklung. Mit ihnen wird der Rechtsrahmen für die Interoperabilität der EU-Informationssysteme und damit für die systematische Verknüpfung aller EU-Datenbanken geschaffen – namentlich des Schengener Informationssystems (SIS), des Visa-Informationssystems (VIS) und Eurodac sowie des Entry/Exit-Systems (EES), des Europäischen Strafregisterinformationssystems für Drittstaatenangehörige (ECRIS-TCN) und des Europäischen Reiseinformations- und -genehmigungssystems (ETIAS). Während SIS, VIS und Eurodac bereits seit Jahren und mit Schweizer Beteiligung existieren, sind EES, ECRIS-TCN und ETIAS noch nicht eingerichtet bzw. in Betrieb.

Das Parlament hat die Schweizer Teilnahme am EES und den freiwilligen Aufbau eines nationalen Erleichterungsprogramms (*National Facilitation Programme*, NFP) bereits verabschiedet. Für die Übernahme und Umsetzung von ETIAS ist die Vernehmlassung abgeschlossen, den direkten Zugang zu ECRIS-TCN prüft die Schweiz zurzeit.<sup>3</sup> Zugleich strebt die Schweiz den direkten Zugang zu Europol-Daten und Interpol-Datenbanken an und will 2020 einen Grundsatzentscheid fällen zur Teilnahme am PNR-System (*Passenger Name Record*) der EU.<sup>4</sup> Bereits ausgehandelt ist eine Zusatzvereinbarung zur Beteiligung der Schweiz an eu-LISA, der Europäischen Agentur für das Betriebsmanagement von IT-Grosssystemen. Diese ist nicht nur zuständig für das Betriebsmanagement und die Sicherheit der bestehenden und geplanten Informationssysteme, sondern auch für die Umsetzung der Interoperabilität. Insgesamt will die Schweiz in den kommenden Jahren rund 100 Millionen Franken ausgeben, um den Anschluss der Schweiz an die EU-Datensysteme sicherzustellen.<sup>5</sup>

Die SFH befürwortet die Übernahme der beiden EU-Verordnungen unter der Prämisse der grundsätzlichen Weiterführung des Schengen/Dublin-Abkommens. Trotzdem steht sie der unterbreiteten Vorlage kritisch gegenüber. Die SFH erachtet die zugrundeliegende Sammlung, Bearbeitung, Speicherung und Weitergabe sensibler Daten in immensum Umfang als problematisch. Sie fordert deshalb, bei der innerstaatlichen Umsetzung den Grundsatz der Verhältnismässigkeit zu wahren und dem Schutz der Daten von Betroffenen genügend Rechnung zu tragen. Es sollen nur Regelungen eingeführt werden, die vom Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) geprüft, beurteilt und gutgeheissen wurden.

<sup>1</sup> Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates, ABl. L 135 vom 22.5.2019, S. 27-84.

<sup>2</sup> Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816, ABl. L 135 vom 22.5.2019, S. 85-135.

<sup>3</sup> Vgl. Erläuternder Bericht zur Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818).

<sup>4</sup> Vgl. Ziele des Bundesrates 2020, Bd. II, S. 15.

<sup>5</sup> Vgl. Botschaft zu einem Verpflichtungskredit zur Weiterentwicklung des Schengen/Dublin-Besitzstandes, BBl 2019 S. 6189-6224.

## 2 Das Wichtigste in Kürze

Die mit den beiden Verordnungen [EU] 2019/817 und [EU] 2019/818 eingeführte Interoperabilität soll den Informationsaustausch zwischen den bestehenden und zukünftigen IT-Grosssystemen der EU ermöglichen. Grenzkontroll-, Migrations- und Strafverfolgungsbehörden erhalten damit zur Überprüfung von Personen Zugang zu umfassenden Informationen und sensitiven Daten, wobei die Grundrechte der Betroffenen vollumfänglich gewahrt werden sollen. Vorgesehen ist insbesondere der Aufbau einer neuen zentralen Datenbank, in der Informationen über Millionen von Drittstaatsangehörigen samt ihrer biometrischen Daten gespeichert werden.

Die SFH befürwortet grundsätzlich die Übernahme und Umsetzung der EU-Verordnungen, da die Schengen-Assoziierung der Schweiz nicht aufs Spiel gesetzt werden sollte. Sie steht der vorgesehenen Interoperabilität aber kritisch gegenüber, zumal diese aus grundrechtlicher Perspektive erhebliche Gefahren und Probleme mit sich bringt. Besonders kritisch zu betrachten ist die Fokussierung auf die innere Sicherheit und damit einhergehend die Konzentration auf Drittstaatsangehörige. **Die Sammlung und Speicherung von immer mehr Daten von Drittstaatsangehörigen wird mit der pauschalen Unterstellung ihrer besonderen Gefährlichkeit gerechtfertigt, was faktisch eine Ungleichbehandlung und Diskriminierung bedeutet.** Zugleich untergraben die vorgelegten neuen Regeln für Interoperabilität eines der zentralen Datenschutzprinzipien: den Grundsatz der Zweckbindung. Problematisch ist zudem, dass der Zugang von Strafverfolgungsbehörden zu Daten anderer Behörden erleichtert wird.

**Aus Sicht der SFH ist es bedenklich, wenn die Schweiz gemäss Vernehmlassungsentwurf zwar den Auf- und Ausbau der EU-Informationssysteme vollumfänglich übernimmt und umsetzt, beim Datenschutz aber zugleich kaum gleichwertige Vorkehrungen trifft.** Das ist umso problematischer, als die komplexen IT-Grosssysteme der EU und deren Interoperabilität gewaltige Auswirkungen auf die Grundrechte natürlicher Personen haben und im Zusammenhang mit migrationsrechtlichen Bestimmungen ein besonderes Bedürfnis nach Datenschutz besteht.

Angesichts dessen fordert die SFH bei der Umsetzung insbesondere folgende Nachbesserungen und Präzisierungen:

- Explizit festzuhalten ist, dass eine Behörde, die eine Abfrage über den gemeinsamen Dienst für den Abgleich biometrischer Daten (sBMS) einleitet, nur die Verweise auf jene EU-Informationssysteme sieht, zu deren Zugang sie berechtigt ist.
- Es ist eine präzisere und genau abgegrenzte Definition der Zwecke vorzunehmen, für die eine Abfrage des gemeinsamen Speichers für Identitätsdaten (CIR) zulässig ist, damit die Erfordernisse der Notwendigkeit und der Verhältnismässigkeit erfüllt sind.
- Es ist ein ergänzender Verweis auf die Anforderungen zur Vermeidung jeder Form von Diskriminierung explizit ins Gesetz aufzunehmen.
- Die Garantien zum Schutz des Grundrechts auf Achtung des Privat- und Familienlebens und des Grundrechts auf Schutz personenbezogener Daten ist soweit als möglich zu gewährleisten und im Gesetz entsprechend zu präzisieren.
- Auf Gesetzesstufe ist zu präzisieren, dass es sich bei «sonstigen schweren Straftaten» im Sinne von Art. 110d Abs. 1 E-AIG um Straftaten mit einer Mindestfreiheitsstrafe von 3 Jahren handeln muss.
- Die nationale Polizeibehörde eines Herkunftslandes darf unter keinen Umständen Informationen darüber erhalten, dass ihre Datenbanken über das Europäische Suchportal (ESP) abgefragt wurden – insbesondere nicht im Falle anerkannter Flüchtlinge und jener Personen, die in Eurodac als Asylsuchende registriert sind.
- Die Schnittstellen zur europäischen und zur nationalen Aufsichtsbehörde sowie zum neuen Schengen-Datenschutzgesetz muss auf Gesetzesstufe geklärt und geregelt werden, um dem Datenschutz und der Datensicherheit die nötige Nachachtung zu verschaffen.
- Die nationale Aufsichtsbehörde bzw. der EDÖB sollte mit den erforderlichen (zusätzlichen) Ressourcen ausgestattet werden, damit die Aufsichtsfunktion auch angemessen wahrgenommen werden kann.

## 3 Kommentar zu den wichtigsten Bestimmungen

Die Verordnungen «IOP Grenzen» und «IOP Polizei» enthalten sowohl direkt anwendbare Bestimmungen als auch solche, die im nationalen Recht konkretisiert werden müssen. Die SFH nimmt im Folgenden Stellung zu einigen grundsätzlichen Aspekten der EU-Interoperabilitätsverordnungen sowie zu den geplanten Anpassungen im Ausländer- und Integrationsgesetz (AIG) und im Bundesgesetz über polizeiliche Informationssysteme des Bundes (BPI) – namentlich zu den vier Hauptkomponenten der Interoperabilität: Gemeinsamer Dienst für den Abgleich biometrischer Daten (sBMS; Kap. 3.2.1), gemeinsamer Speicher für Identitätsdaten (CIR; Kap. 3.2.2), europäisches Suchportal (ESP; Kap. 3.2.3) und Detektor für Mehrfachidentitäten (MID; Kap. 3.2.4).

### 3.1 Grundsätzliche Anmerkungen

Die neuen Regeln für die Interoperabilität sollen den Informationsaustausch erleichtern und die Sicherheit in der EU erheblich verbessern, effizientere Kontrollen an den Aussengrenzen ermöglichen, die Erkennung von Mehrfachidentitäten verbessern und zur Verhinderung und Bekämpfung der illegalen Migration beitragen, ohne dass die Grundrechte angetastet werden.<sup>6</sup> Ob dies eingehalten werden kann, ist aus Sicht der SFH fraglich. Die Interoperabilität steht und fällt mit der Zuverlässigkeit, Vertrauenswürdigkeit und Korrektheit der Daten in den verknüpften Datenbanken. Die Erfahrung zeigt jedoch, dass dies nicht gewährleistet ist: Die IT-Systeme der EU enthalten vielmehr eine beträchtliche Menge ungenauer Daten, wie etwa Evaluationen von SIS und VIS durch die EU-Kommission, den EU-Datenschutzbeauftragten (EDSB) und die Hochrangige Expertengruppe für Informationssysteme und Interoperabilität zeigen und Untersuchungen der EU-Agentur für Grundrechte (FRA) bestätigen.<sup>7</sup> Angesichts der Grösse der verknüpften EU-Datenbanken, des Ausmasses ihrer vorgesehenen Nutzung und der Anzahl angeschlossener Staaten besteht ein enormes Risiko, dass sich fehlerhafte Informationen in einer der Datenbanken in anderen EU-Datenbanken sowie auf nationaler Ebene vervielfachen. Das wiederum führt bei der Abfrage der interoperablen Systeme zwangsläufig zu einer markanten Zunahme falscher Übereinstimmungen und falscher Treffer. Die Folgen werden den Schutz der Grundrechte massiv beeinträchtigen und auch die angestrebte Wirksamkeit der Interoperabilität behindern.

Die Interoperabilität der EU-Datenbanken beruht auf dem Grundsatz des gegenseitigen Vertrauens – Vertrauen in die Rechtmässigkeit der Datenerhebungs- und Entscheidungsprozesse sowie in die Arbeit der Behörden, die Zugang zu den Datenbanken haben. Mit Blick auf den Grundrechtsschutz ist das aus Sicht der SFH hoch problematisch. Insbesondere dann, wenn es dazu führt, dass sich die nationalen Behörden auf die in den EU-Datensystemen gespeicherten Daten verlassen, anstatt jeden einzelnen Fall sorgfältig zu prüfen. Für Betroffene wird es schwierig bis unmöglich sein, sich gegen Entscheidungen auf der Grundlage falscher Daten zu wehren, wenn die Quelle oder der Verfasser dieser Informationen unbekannt ist.<sup>8</sup>

<sup>6</sup> Vgl. Verordnungen «IOP Grenzen» (Fn1) und «IOP Polizei» (Fn 2): jeweils Erwägungsgrund 9; Erläuternder Bericht (Fn 3): S. 8.

<sup>7</sup> Vgl. European Commission, [Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System \(SIS II\) in accordance with art. 24 \(5\), 43 \(3\) and 50 \(5\) of Regulation \(EC\) No 1987/2006 and art. 59 \(3\) and 66 \(5\) of Decision 2007/533/JHA](#), COM/2016/0880 final, Brussels, 21.12.2016; European Commission, [Report from the Commission to the European Parliament and the Council on the implementation of Regulation \(EC\) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System \(VIS\), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation](#), COM/2016/655, Brussels, 14.10.2016; European Data Protection Supervisor, [Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation \(EC\) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States](#), OJ 2008/C 200/01; High Level Expert Group on Informations Systems and Interoperability, [Register of Commission Expert Groups](#); European Union Agency for Fundamental Rights, [Under watchful eyes – biometrics, EU IT-systems and fundamental rights](#), Luxembourg 2018; European Union Agency for Fundamental Rights: [Fundamental rights and the interoperability of EU information systems: borders and security](#), Luxembourg 2017.

<sup>8</sup> Vgl. hierzu etwa Brouwer, Evelien: [Interoperability of Databases and Interstate Trust: a Perilous Combination for Fundamental Rights](#), *VerfBlog*, 2019/5/25; Progin-Theuerkauf, Sarah, Zoetewijj-Turhan, Margaritha, Turhan, Ozan: Interoperabilität der Informationssysteme im Migrationsbereich - digitale Grenzkontrollen 2019. In: Jahrbuch für Migrationsrecht 2018/2019, Bern 2019, S. 3-41.

Die beiden EU-Verordnungen «IOP Grenzen» und IOP Polizei» folgen der nicht nur in Europa beobachtbaren Tendenz, Migration zunehmend ausschliesslich unter dem Aspekt der inneren Sicherheit zu betrachten. Sie verknüpfen Datensysteme und Instrumente in den Bereichen Grenzkontrollen, Asyl und Einwanderung, Strafverfolgung sowie polizeiliche und justizielle Zusammenarbeit. Dabei werden Migrationskontrolle und die Bekämpfung von Kriminalität und Terrorismus begrifflich gleichgesetzt. Drittstaatsangehörige erscheinen so ohne jeden empirischen Nachweis per se als Sicherheitsrisiko. Die pauschale Annahme der Gefährlichkeit von Drittstaatsangehörigen bedeutet eine Diskriminierung, die sich nicht rechtfertigen lässt.

Mit den beiden EU-Verordnungen «IOP Grenzen» und IOP Polizei» wird eine neue zentrale Datenbank mit Informationen über Millionen von Drittstaatsangehörigen samt ihrer biometrischen Daten geschaffen.<sup>9</sup> Die Operationalisierung der Interoperabilität und deren Auswirkungen treffen denn auch in erster Linie Drittstaatsangehörige, was aus Sicht der SFH faktisch eine nicht gerechtfertigte Ungleichbehandlung darstellt. Namentlich die Folgen einer Datenverletzung könnten einer potenziell sehr grossen Zahl von Drittstaatsangehörigen ernsthaften Schaden zufügen. Die SFH teilt die Befürchtung des EDSB, wonach die Interoperabilität der EU-Datenbanken «zu einem gefährlichen, gegen die Grundrechte gerichteten Werkzeug werden» könnte, zumal eine zentrale Datenbank – im Gegensatz zu dezentralen Datenbanken – «implizit die Gefahr des Missbrauchs» birgt und eher den Wunsch weckt «nach einer Nutzung des Systems über die Zwecke hinaus, für die sie eigentlich gedacht war.»<sup>10</sup> Die Gefahr des Datenmissbrauchs ist eine Gefahr, die den Kern des Rechts auf Privatleben und Datenschutz betrifft, das in Artikel 8 EMRK sowie Artikel 13 BV geschützt ist.

Die beiden EU-Verordnungen «IOP Grenzen» und IOP Polizei» wie der erläuternde Bericht des Bundesrates postulieren, dass mithilfe der Interoperationalität bzw. intelligenten Grenzen die irreguläre Zuwanderung verhindert werden könne.<sup>11</sup> Studien belegen indes, dass die Aufrüstung von Grenzschutzmassnahmen bis hin zu intelligenten Grenzen die irreguläre Migration nicht massgeblich verringert.<sup>12</sup> Es bewirkt vielmehr, dass sich die Migration auf immer riskantere Reisewege verlagert und verstärkt die Dienste von kriminellen Schleusern in Anspruch genommen werden. Auch zwischen intelligenten Grenzen und der Sekundärmigration von Asylsuchenden innerhalb Europas besteht kein nachgewiesener Zusammenhang. Das primäre Defizit des Dublin-Systems besteht nicht darin, dass Asylsuchende an den Schengen-Aussengrenzen lückenhaft registriert würden. Das Hauptproblem ist vielmehr die nicht gewährleistete Gleichwertigkeit von Aufnahme Standards und Asylverfahren in allen Mitgliedstaaten.<sup>13</sup>

Der erläuternde Bericht des Bundesrates betont: «Mit der Interoperabilität werden keine neuen Daten erhoben, sondern lediglich zusätzliche Funktionen für die bestehenden und zukünftigen Informationssysteme geschaffen. Für die Behörden ändert sich dadurch nichts an den bestehenden Zugriffsrechten für die zugrundeliegenden Systeme.»<sup>14</sup>

Damit wird dreierlei verschleiert:

1. der Fakt, dass mit dem CIR und dem MID neue Datenbanken geschaffen werden (siehe Kap. 3.2.2 und 3.2.4);
2. der Umstand, dass der Zugang der Strafverfolgungsbehörden zu Daten anderer Behörden erleichtert wird (siehe Kap 3.2.2); und
3. die Tatsache, dass die zugrundeliegenden EU-Datenbanken für jeweils ganz spezifische Zwecke eingerichtet wurden und dass die dort erfassten Daten nun mit der Interoperabilität

<sup>9</sup> Europäischer Datenschutzbeauftragter (EDSB): Stellungnahme 4/2018 zu den Vorschlägen für zwei Verordnungen über die Einrichtung eines Rahmens für die Interoperabilität von IT-Grosssystemen der EU, Wie, 16.4.2018. S. 3.

<sup>10</sup> Ebd. S. 12

<sup>11</sup> Vgl. Verordnung „IOP Grenzen“ (Fn 1): Erwägungsgrund 9 sowie Erläuternder Bericht (Fn 3): S. 8.

<sup>12</sup> Vgl. etwa Douglas S. Massey/Jorge Durand/Karen A. Pren, »Why Border Enforcement Backfired«, in: American Journal of Sociology, 121 (2016) 5, S. 1557–1600; Amthias Czaika/ Hein de Haas, »The Effect of Visas on Migration Processes«, in: International Migration Review, 51 (2016) 4, S. 893–926.

<sup>13</sup> Raphael Bossung: Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit der EU. Umsetzungsrisiken und rechtsstaatliche Anforderungen, SWP Studie 4, April 2018, S. 21.

<sup>14</sup> Erläuternder Bericht (Fn 3): S. 7f.

für neue Zwecke verwendet werden, die in den ursprünglichen Rechtsvorschriften der jeweiligen Datenbanken gar nie vorgesehen waren.

Damit untergraben die vorgelegten neuen Regeln für Interoperabilität eines der zentralen Datenschutzprinzipien: den Grundsatz der Zweckbindung. Der EDSB kritisiert dies scharf und hält dazu dezidiert fest: «*Das Erfordernis einer besseren Verwertung der Daten darf jedoch nie die Verletzung des Grundrechts auf Datenschutz zur Folge haben.*»<sup>15</sup> Dies gilt aus Sicht der SFH umso mehr im Zusammenhang mit migrationsrechtlichen Bestimmungen, da hier ein besonderes Bedürfnis nach Datenschutz besteht.<sup>16</sup>

## 3.2 Umsetzung EU-Verordnungen «IOP Grenzen» und «IOP Polizei»

Die beiden EU-Interoperabilitätsverordnungen sind «Parallelvorlagen», die zusammen gelesen werden müssen. Die Nummerierung der Artikel ist in beiden EU-Verordnungen inhaltlich im Wesentlichen gleich. Sofern nicht anders angegeben, bezieht sich die Nennung eines bestimmten Artikels auf beide Verordnungen. Ähnliches gilt für die Umsetzung im AIG und BPI, weshalb die entsprechenden Bestimmungen nachfolgend zusammen abgehandelt werden, sofern nicht anders angegeben.

### 3.2.1 Gemeinsamer Dienst für den Abgleich biometrischer Daten (sBMS) (Art. 110 E-AIG; Art. 18a E-BPI)

Der sBMS ist eine der vier neuen Zentralkomponenten der Interoperabilität. Er ermöglicht mithilfe sogenannter «biometrischer Templates» die Suche und den Vergleich biometrischer Daten aus mehreren EU-Datensystemen. Die Bestimmungen zum sBMS der beiden EU-Verordnungen «IOP Grenzen» und «IOP Polizei» (Kap. III) sind hier direkt anwendbar. Da jedoch im AIG wie im BPI trotzdem eine Bestimmung zum sBMS aufgenommen werden soll, empfiehlt die SFH, dabei eine präzisierende Ergänzung vorzunehmen.

Gemäss Art. 13 Abs. 2 der beiden EU-Verordnungen wird jedes biometrische Template einen Verweis auf die EU-Informationssysteme enthalten, in denen die betreffenden biometrischen Daten gespeichert sind, und einen Verweis auf die tatsächlichen Datensätze in diesen EU-Informationssystemen. Ist aber ein solcher Verweis für eine Behörde, die eine Abfrage zu einer Person durchführt, sichtbar, kann die einfache Kenntnis davon, dass in einem bestimmten IT-System mehr Informationen über die Person gespeichert sind, der Behörde bereits Hinweise auf diese Person geben, die sie sonst nicht hätte. Solche Hinweise können wiederum die Entscheidung beeinflussen, die die Behörde in Bezug auf die betroffene Person trifft.

Zwar geht die SFH davon aus, dass eine Behörde, die eine Abfrage einleitet, nur in der Lage sein wird, zu erkennen, ob in den Systemen, zu denen sie zugangsberechtigt ist, Informationen über die Person gespeichert sind. Denn die EU-Interoperabilitätsverordnungen ändern die Zugangsregeln und die Anforderungen für die Datenverarbeitung der zugrundeliegenden IT-Systeme nicht. Doch fehlt in Art. 13 Abs. 2 der EU-Verordnungen ein entsprechender expliziter Hinweis und ermöglicht damit unterschiedliche Auslegungen. **Die SFH schlägt deshalb vor, in Art. 110 Abs. 2 E-AIG (und Art. 18a Abs. 2 E-BPI) mit einem ergänzenden Satz klarzustellen, dass eine Behörde, die eine**

<sup>15</sup> Europäischer Datenschutzbeauftragter (EDSB): Stellungnahme 4/2018 zu den Vorschlägen für zwei Verordnungen über die Einrichtung eines Rahmens für die Interoperabilität von IT-Grosssystemen der EU, Wie, 16.4.2018. S. 11.

<sup>16</sup> Vgl. Peter Uebersax: Zur Revision des Ausländergesetzes gemäss der Botschaft des Bundesrates vom März 2018, in: Jusletter 9.7.2018; Caroline Gloor Scheidegger, Adrian Lobsiger: Rechtliche Fragen bei der Bearbeitung von Migrationsdaten, in: Stephan Breitenmoser, Otto Lagodny, Peter Uebersax (Hrsg.): Schengen und Dublin in der Praxis – aktuelle Herausforderungen, Zürich 2018, S. 317-338.

**Abfrage über den sBMS einleitet, nur die Verweise auf jene EU-Informationssysteme sieht, zu deren Zugang sie berechtigt ist.**

Im Übrigen ist – anders als im erläuternden Bericht ausgeführt – durchaus umstritten, ob die biometrischen Templates des sBMS nicht selbst personenbezogene Daten darstellen und die Bearbeitung und Speicherung solcher Templates damit den einschlägigen Datenschutzbestimmungen und der entsprechenden Rechtsprechung unterliegen.<sup>17</sup>

### 3.2.2 Gemeinsamer Speicher für Identitätsdaten (CIR) (Art. 110a ff. E-AIG)

Im CIR wird für jede Person, die im EES, VIS, ETIAS, Eurodac oder ECRIS-TCN erfasst ist, eine individuelle Datei angelegt, in der die Identitätsdaten, die Daten zu Reisedokumenten und die biometrischen Daten gespeichert werden. Der CIR enthält zudem einen Verweis auf das jeweilige Informationssystem, aus dem die Daten stammen, sowie einen Verweis auf die tatsächlichen Daten in diesem System.

**Art. 110b E-AIG**, der die Abfrage des CIR zwecks Identifikation regelt, ist aus Sicht der SFH problematisch, da er in der vorgelegten Form zu vage formuliert und zudem unvollständig ist.

- **Art. 110b Abs. 1 E-AIG:** So ist etwa nicht nachvollziehbar, weshalb bei der Umsetzung im Schweizer Recht die in Art. 20 Abs. 2 der EU-Interoperabilitätsverordnungen vorgegebene Ausschliesslichkeit aufgeweicht wird (Satz 1). Die SFH schlägt deshalb folgende Neuformulierung von Satz 1 vor: «***1 Abfragen des CIR dürfen nur durch eine Behörde nach Abs. 3 und ausschliesslich zum Zwecke der Identifikation durchgeführt werden***».
- **Art. 110b Abs. 2 E-AIG:** Als zulässige Zwecke für CIR-Abfragen werden hier aufgezählt die «Verhütung und Bekämpfung illegaler Einwanderung», die «Gewährleistung und Aufrechterhaltung der öffentlichen Sicherheit und Ordnung» sowie der «Schutz der inneren Sicherheit». Diese Zweckbeschreibungen sind aus Sicht der SFH deutlich zu breit gefasst und zu vage. Sie widersprechen damit auch den Vorgaben von Art. 20 Abs. 5 der EU-Interoperabilitätsverordnungen, wonach beim Erlass einer nationalen Rechtsvorschrift «die genauen Zwecke» festzulegen sind. Faktisch erlauben sie in der Form des Vernehmlassungsentwurfes beinahe beliebige Identitätskontrollen durch die Behörden, was entweder zu einem routinemässigen bis willkürlichen Gebrauch der Abfragen führen kann, der die erforderliche Zweckbindung letztlich ignoriert – oder zu diskriminierenden Praktiken, die allein auf der Grundlage eines umfassenden Profilings erfolgen. **Die SFH fordert deshalb, in Abs. 2 eine präzisere und genau abgegrenzte Definition der Zwecke vorzunehmen, für die eine CIR-Abfrage zulässig ist, damit die Erfordernisse der Notwendigkeit und der Verhältnismässigkeit erfüllt sind.** Erst dies würde auch den Vorgaben des Europäischen Gerichtshofes (EuGH) entsprechen, die auch Eingang in die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) gefunden haben.<sup>18</sup>
- Der EU-Gesetzgeber ist sich der erwähnten Diskriminierungsgefahr sehr wohl bewusst. Die EU-Interoperabilitätsverordnungen halten in Art. 5 denn auch fest: «Bei der Verarbeitung personenbezogener Daten [...] dürfen keine Personen aufgrund des Geschlechts, der

<sup>17</sup> Vgl. etwa European Parliamentary Research Service: [Interoperability of Justice and Home Affairs Information Systems](#), Study For the LIBE committee, April 2018, S. 58ff. sowie Els J. Kindt: Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, Dordrecht 2013, S. 94–100.

<sup>18</sup> Vgl. Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland/Kärntner Landesregierung and others*, 8 April 2014, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293>; Case C-362/14, *Schrems*, 6 October 2015, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362>; Joined Cases C-203/15 and C-698/15, *Tele2/Watson*, 21.12.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0203>; Case Opinion 1/15, *Opinion of Advocate General Mengozzi*, 8.9.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CC0001>; *Big Brother Watch and others v the United Kingdom*, application nos. 58170/13, 62322/14 and 24960/15, 13 September 2018, <http://hudoc.echr.coe.int/eng?i=001-186048>

Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, einer politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung diskriminiert werden. Die Menschenwürde und die Integrität sowie die Grundrechte der Betroffenen, darunter auch das Recht auf Achtung der Privatsphäre und auf Schutz der personenbezogenen Daten, müssen uneingeschränkt gewahrt werden.» Art. 20 Abs. 5 der EU-Interoperabilitätsverordnungen verlangt daher explizit, dass bei der Umsetzung in nationalen Rechtsvorschriften Massnahmen ergriffen werden, die «jede Diskriminierung von Drittstaatsangehörigen» vermeiden. **Die SFH fordert deshalb, den im AIG-Entwurf fehlenden Verweis auf diese Anforderungen zur Vermeidung jeder Form von Diskriminierung explizit ins Gesetz aufzunehmen. Vorgeschlagen wird dafür folgende Ergänzung von Art. 101 Abs. 2 E-AIG:**

**Art. 101 Abs. 2 E-AIG (neu)**

<sup>2</sup>Die für die Bearbeitung der Daten zuständige Behörde stellt sicher, dass die Bearbeitung von Personendaten in Informationssystemen des SEM und in den Schengen-Dublin-Informationssystemen in einem angemessenen Verhältnis zu den verfolgten Zielen steht und nur erfolgt, soweit sie für die Erfüllung ihrer Aufgaben erforderlich ist. Die Menschenwürde und die Integrität der Personen, deren Daten bearbeitet werden, bleiben gewahrt und es werden die erforderlichen Massnahmen ergriffen, um jegliche Diskriminierung zu vermeiden.

- Die SFH weist zudem darauf hin, dass die Aufsichtsbehörden in der Praxis ein besonderes Augenmerk darauf zu richten haben werden, dass eine Abfrage des CIR zur Identifizierung einer Person bei einer Identitätskontrolle anhand biometrischer Daten nur als letzte Möglichkeit erfolgt. Würden nämlich systematisch bei einer Identitätskontrolle biometrische Daten einer Person herangezogen, kann dies zu einer Stigmatisierung und Diskriminierung bestimmter Menschen oder Gruppen von Menschen aufgrund ihres Erscheinungsbildes oder der vermuteten ethnischen Herkunft oder Nationalität führen.<sup>19</sup>
- **Art. 110b Abs. 4 E-AIG:** Hier ist zu ergänzen, dass die Abfrage vor Ort und **«im Beisein der betroffenen Person»** eingeleitet werden muss, wie dies in Art. 20 Abs. 2 der EU-Interoperabilitätsverordnungen vorgesehen ist.

**Art. 110d E-AIG** ist aus Sicht der SFH äusserst problematisch. Geregelt wird hier die Abfrage des CIR zwecks Verhütung, Aufdeckung oder Ermittlung terroristischer Straftaten oder sonstiger schwerer Straftaten. Dabei haben Strafverfolgungsbehörden Zugang zu IT-Systemen, die ursprünglich für andere Zwecke als die Strafverfolgung eingerichtet wurden. Diese an sich schon bedenkliche Möglichkeit, die für andere Zwecke erhobenen Identitätsdaten aus dem EES, VIS, ETIAS oder Eurodac-System für die Verfolgung terroristischer oder anderer schwerer Straftaten zu verwenden, ist zwar nicht ganz neu. Doch bringen die beiden EU-Interoperabilitätsverordnungen nun eine erhebliche Lockerung der Bedingungen für den Zugang zu den Daten in diesen IT-Systemen mit sich.

- Gemäss Art. 110d Abs. 1 E-AIG können Strafverfolgungsbehörden künftig im Einzelfall eine CIR-Abfrage durchführen, wenn die Bedingungen nach Art. 22 Abs. 1 der EU-Interoperabilitätsverordnungen erfüllt sind. Demnach genügen dazu *«vernünftige Gründe dafür, dass die Abfrage der EU-Informationssysteme zur Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten beitragen kann»*. Die CIR-Abfrage erfolgt dann in zwei Stufen: Stimmen die Daten der Abfrage mit Daten überein, die in mindestens einem der zugrundeliegenden EU-Informationssysteme gespeichert sind, wird ein «Treffer» angezeigt sowie ein Verweis auf das betroffene IT-System (Art. 110d Abs. 3 E-AIG: Abfrage auf der ersten Ebene). Der vollständige Zugang zu den Daten unterliegt dann

<sup>19</sup> Vgl. EDSB, Stellungnahme 4/2018 (Fn 15), S. 16.

weiterhin den Voraussetzungen und Verfahren, die für das jeweils zugrundeliegende EU-Informationssystem gelten (Art. 110d Abs. 4 E-AIG: Abfrage auf der zweiten Ebene).

- Derzeit sehen alle diese bestehenden oder vorgeschlagenen EU-Informationssysteme als kumulative Zugangsbedingungen vor: Der Zugang muss in einem konkreten Einzelfall sowie für die Prävention, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerwiegender Straftaten erforderlich sein und es müssen berechtigte Gründe für die Annahme vorliegen, dass die Abfrage wesentlich zur Verhütung, Aufdeckung oder Untersuchung der fraglichen Straftaten beitragen wird. Zudem muss eine unabhängige Behörde prüfen, ob vor dem Zugang die genannten Bedingungen erfüllt sind. Und schliesslich sind die Strafverfolgungsbehörden bei Eurodac, ETIAS und EES verpflichtet, zuerst andere potenzielle Informationsquellen wie etwa nationale Datenbanken abzufragen (sogenannter «Kaskadenmechanismus»)<sup>20</sup>.
- Mit der vorgelegten Umsetzung der EU-Interoperabilitätsverordnungen wird nun aber der Zugang von Strafverfolgungsbehörden zu Daten anderer Behörden zum Zwecke der Strafverfolgung in zweifacher Hinsicht gelockert: Erstens sollen die genannten Bedingungen und Modalitäten erst bei der CIR-Abfrage auf der zweiten Stufe gelten – also für den vollen Datenzugang. Der Grund dafür ist augenscheinlich die beabsichtigte Beschleunigung eines Verfahrens. Zweitens müssen für den Zugang der Strafverfolgungsbehörden keine «berechtigten Gründe» mehr vorliegen für die Annahme, dass die Abfrage wesentlich zur Verhütung, Aufdeckung oder Untersuchung terroristischer oder anderer schwerer Straftaten beitragen wird. Es genügen vielmehr nicht näher definierte «vernünftige Gründe» sowie die vage Vermutung eines möglichen Beitrags zur Verhinderung, Aufdeckung oder Untersuchung (kann-Formulierung).
- Die SFH hält diese Lockerungen für ungerechtfertigt und bedenklich. Zum einen zeigt bereits die CIR-Abfrage auf der ersten Ebene mit den Informationen «Treffer/kein Treffer» personenbezogene Daten, die beispielsweise anzeigen, ob eine Person eine visumsbefreite Reisende oder ein Asylsuchender ist oder nicht. Die Verarbeitung solcher Daten stellt damit einen Grundrechtseingriff dar, der nur zulässig ist, wenn er notwendig und verhältnismässig ist. Die Zweckmässigkeit einer Massnahme allein genügt dafür nicht.<sup>21</sup> Zum andern ist der verwendete Begriff «vernünftige Gründe» (anstelle von «berechtigte Gründe») eine klare Abschwächung und beinahe beliebig interpretierbar, womit er der behördlichen Willkür Tür und Tor öffnet. Es braucht keine Phantasie, um abzusehen, dass dies schrittweise zu flächendeckenden CIR-Abfragen, behördlichen Daten-Fischzügen und einem routinemässigen Datenzugang führen wird, an dessen Ende mehr Verfolgungen und/oder Verurteilungen von Drittstaatsangehörigen stehen. Auch der Kaskadenmechanismus wird letztlich ad absurdum geführt: Wenn sich bei einer ersten Abfrage im CIR herausstellt, dass weitere Informationen über eine Person etwa in ETIAS oder EES gespeichert sind, was wäre dann der Sinn, das Kaskadenverfahren erst noch zu durchlaufen, um Zugang dazu zu erhalten? Das «Treffer/Kein Treffer»-System bedeutet damit letztlich die Abschaffung des Kaskadenmechanismus.
- **Die SFH empfiehlt aus den genannten Gründen, bei der Umsetzung der EU-Interoperabilitätsverordnungen in nationales Recht die Garantien zum Schutz des Grundrechts auf Achtung des Privat- und Familienlebens und des Grundrechts auf Schutz personenbezogener Daten soweit als möglich zu gewährleisten und Art. 110d E-AIG entsprechend zu präzisieren. Im Minimum sollte eine ergänzende Bestimmung festlegen, dass Strafverfolgungsbehörden, die einen Treffer erhalten, sich immer an die Aufsichtsbehörde wenden müssen, die überprüft, ob die Bedingungen für den CIR-Zugang erfüllt waren.**

<sup>20</sup> Vgl. EDSB, Stellungnahme 4/2018 (Fn 15), S. 18.

<sup>21</sup> Vgl. ebd.

- Zudem muss aus Sicht der SFH Ansicht auf Gesetzesstufe klarer definiert werden, was unter «sonstigen schweren Straftaten» im Sinne von Art. 110d Abs. 1 E-AIG zu verstehen ist. Dies umso mehr, als der NDB Zugang zum CIR bzw. zu sensitiven Personendaten hat. Folglich fordert die SFH auf Gesetzesstufe zu präzisieren, dass es sich dabei um Straftaten mit einer Mindestfreiheitsstrafe von 3 Jahren handeln muss.

### 3.2.3 Europäisches Suchportal (ESP) (Art. 110e E-AIG; Art. 18b E-BPI)

Das ESP soll einen raschen Zugang zu den EU-Informationssystemen sowie den Europol- und Interpol-Daten schaffen, indem es eine gleichzeitige Abfrage aller Datenbanken mittels biografischen und/oder biometrischen Daten ermöglicht. Obwohl es sich beim ESP im Wesentlichen lediglich um eine Suchschnittstelle handelt, gibt es aus Sicht der SFH einen problematischen Aspekt, der insbesondere Asylsuchende und Flüchtlinge betrifft.

So wird das ESP etwa auch zur Abfrage zweier Interpol-Datenbanken eingesetzt (Art 110e Abs. 1 E-AIG; Art. 18 b Abs. 1 E-BPI): nämlich für die Datenbank für gestohlene und verlorene Reisedokumente («*Stolen and Lost Travel Documents*», SLTD) sowie für die Datenbank «*Travel Documents Associated with Notices*» (TDAWN) für Personen, für die eine Interpol-Warnmeldung existiert (also etwa ein roter Hinweis auf den Aufenthaltsort und die Festnahme einer gesuchten Person). Diese Datenbanken werden mit Informationen der nationalen Polizeibehörden in den 194 Mitgliedsländern gespeisen. Ergibt eine Abfrage in diesen Datenbanken einen «Treffer», so wird jene nationale Behörde, die die Ausschreibung eingegeben hat, darüber informiert, wann, wo und von wem die Abfrage durchgeführt wurde.

Eine Überprüfung durch Interpol soll zwar Ausschreibungen aus politischen, militärischen, religiösen oder rassistischen Gründen ausschliessen. Trotzdem kann es Regimen in Drittländern gelingen, eine Ausschreibung zu einem ihrer Staatsangehörigen oder zu einem Dokument, das sich im Besitz dieser Person befindet, in die Interpol-Datenbanken aufzunehmen, um die Person an der Reise zu hindern oder um herauszufinden, wo sich die Person befindet. Werden die Daten von Personen, die internationalen Schutz benötigen, in den Interpol-Datenbanken abgefragt, besteht daher ein gewisses Risiko, dass Informationen über die Anwesenheit von Asylsuchenden oder Flüchtlingen in deren Herkunftsland preisgegeben werden. Dadurch sind diese Personen und/oder ihre Familienangehörigen einer erhöhten Gefahr ausgesetzt. **Aus Sicht der SFH darf der Dateneigentümer (also die nationale Polizeibehörde des Herkunftslandes) deshalb unter keinen Umständen Informationen darüber erhalten, dass seine Datenbanken über das ESP abgefragt wurden – insbesondere nicht im Falle anerkannter Flüchtlinge und jener Personen, die in Eurodac als Asylsuchende registriert sind.** Da dies aber wohl zuerst eine Änderung der Interpol-Regeln für die Verarbeitung und Weitergabe von Daten erfordert, sollte bei der Umsetzung der Interoperabilität im nationalen Recht zumindest eine genaue Kontrolle vorgesehen werden.

### 3.2.4 Detektor für Mehrfachidentitäten (MID) (Art. 110f und 110g E-AIG; Art. 18c und 18d E-BPI)

Der MID ist nicht nur ein Detektor, sondern auch eine neue grosse Datenbank, mit der insbesondere potenzieller Identitätsbetrug bekämpft werden soll. Der MID wird aktiviert, sobald Daten im EES, ETIAS, VIS, SIS oder Eurodac angelegt oder aktualisiert werden. Dann werden automatisiert mittels sBMS die biometrischen Daten in allen EU-Datenbanken verglichen und mittels Europäischem Suchportal (ESP) in CIR und SIS die biografischen und die Reisedokument-Daten (Art. 110f Abs. 2 und 3 E-AIG). Bestehen Verknüpfungen zwischen den Daten, so wird dies mit verschiedenfarbigen Treffern angezeigt und eine Identitätsbestätigungsdatei erstellt und gespeichert (Art. 110f Abs. 4 E-AIG). Je nach Art des Treffers bzw. der Verknüpfung wird dann eine manuelle Verifizierung erforderlich (Art. 110g E-AIG).

Für die manuelle Verifizierung und das Verfahren bei der Feststellung einer illegalen Mehrfachidentität oder der Verzeichnung einer Person in mehreren EU-Informationssystemen sind die Bestimmungen der EU-Interoperabilitätsverordnungen direkt anwendbar. Trotzdem nimmt die SFH hier kurz Stellung dazu, zumal damit aus grundrechtlicher Perspektive Probleme und Gefahren verbunden sind:

- Die Bekämpfung von Identitätsbetrug ist erklärtermassen eines der Hauptziele der Interoperabilität. Allerdings wird in den EU-Interoperabilitätsverordnungen und im erläuternden Bericht nirgends angegeben oder gar belegt, wie häufig und gravierend der Identitätsbetrug in der Praxis ist – argumentiert wird allein mit der Wahrscheinlichkeit von Identitätsbetrug und den Schwierigkeiten, diesen potenziellen Betrug aufzudecken.<sup>22</sup> **Es ist daher aus Sicht der SFH mehr als fraglich, ob die Schaffung einer Datenbank mit sensitiven Informationen über Millionen von Drittstaatsangehörigen geeignet, angemessen und verhältnismässig ist im Vergleich mit den daraus resultierenden Folgen für die Grundrechte.**
- In den EU-Interoperabilitätsverordnungen fehlt eine explizite Schutzklausel für Personen mit mehreren rechtmässigen Identitäten. Je nach dem, wie der Algorithmus ausgelegt ist, kann die automatisierte Generierung von Verknüpfungen durch den MID aber für bestimmte Personengruppen stärkere negative bzw. diskriminierende Auswirkungen haben. Insbesondere die Änderung eines Nachnamens, möglicherweise in Verbindung mit einer Änderung der Passdaten (z. B. nach der Erneuerung eines verlorenen Passes) könnte zu einem gelben Link führen, der eine manuelle Überprüfung erforderlich macht. Der häufigste Grund für eine Namensänderung ist Heirat. Betroffen wären also hauptsächlich Frauen, was nur zu verhindern wäre, wenn der MID auch Geburtsnamen berücksichtigen würde.
- Eine zweite Kategorie von Personen, die wahrscheinlich häufiger als andere zur manuellen Überprüfung angehalten werden, sind Personen mit doppelter Staatsangehörigkeit, die mit unterschiedlichen Pässen reisen.
- Eine dritte Kategorie sind Personen mit sehr gebräuchlichen Namen (z.B. Herr Mohammed oder Frau Lee), deren Identität fälschlicherweise mit der Identität einer anderen Person verwechselt werden kann, insbesondere wenn keine biometrischen Identitätsdaten vorliegen. Und schliesslich dürfte beim Vergleich alphanumerischer Daten eine grosse Anzahl von MID-Links angezeigt werden, die manuell überprüft werden müssen, was zu einer unverhältnismässigen Verarbeitung personenbezogener Daten führen kann.<sup>23</sup>
- Diese Probleme können bei Drittstaatsangehörigen stärker ausgeprägt sein, insbesondere bei Personen aus Ländern, die nicht-lateinische Alphabete verwenden und deren Namen in den EU-Datenbanken transliteriert werden sollen. Personen, die über keine Dokumente verfügen, können besondere Schwierigkeiten haben, die korrekte Erfassung ihres Namens in einer Datenbank zu gewährleisten. Deshalb legen die EU-Interoperabilitätsverordnungen denn auch so viel Wert auf die Verarbeitung mehrerer biometrischer Identifikatoren, die weniger anfällig für Doppelarbeit oder Fehler sind als alphanumerische Daten, die aber auch besondere Risiken in Bezug auf die Privatsphäre und den Datenschutz bergen.

### 3.2.5 Datenschutz und Datensicherheit

Die Vorlage zur Umsetzung der Interoperabilität wirft die Frage auf, ob das Verhältnis von Datenbeschaffung, -bearbeitung, -speicherung und -weitergabe im Vergleich zum Schutz der Interessen der betroffenen Personen ausgewogen ist. Da wie erwähnt noch gar nicht alle Teile des neuen

<sup>22</sup> Vgl. EDSB, Stellungnahme 4/2018 (Fn 15), S. 13.

<sup>23</sup> Teresa Quintel: Connecting personal data of Third Country Nationals: Interoperability of EU databases in the light of the CJEU's case law on data retention, 28.2. 2018, S.16, <https://orbilu.uni.lu/handle/10993/35318>

Systems eingerichtet bzw. in Betrieb sind, ist eine abschliessende Beurteilung der genauen Auswirkungen auf Privatsphäre und Datenschutz zum jetzigen Zeitpunkt nicht möglich. Erkennbar ist indes die klare Tendenz des staatlichen Zugriffs auf Daten weg vom Schutz der Interessen der Betroffenen. So bleibt etwa das Recht von Drittstaatsangehörigen an ihren Daten und deren Bearbeitung in der Vorlage unerwähnt.

Aus Sicht der SFH ist es bedenklich, wenn die Schweiz gemäss Vernehmlassungsentwurf zwar den Auf- und Ausbau der EU-Informationssysteme vollumfänglich übernimmt und umsetzt, beim Datenschutz aber zugleich kaum gleichwertige Vorkehrungen trifft. Das ist umso problematischer, als die komplexen IT-Grosssysteme der EU und deren Interoperabilität gewaltige Auswirkungen auf die Grundrechte natürlicher Personen haben. Der Schutz von Sicherheit und Ordnung ist zwar ein berechtigtes öffentliches Interesse, muss aber stets zweckdienlich und verhältnismässig umgesetzt werden und den Datenschutz der Betroffenen angemessen berücksichtigen. Die SFH erinnert zudem daran, dass der Schutz der Grundrechte, namentlich das Recht auf Privatsphäre und Datenschutz, allen Menschen gleichermaßen zusteht.

Angesichts dessen ergeben sich für die SFH folgende Anregungen und Forderungen hinsichtlich Datensicherheit und Datenschutz an die Umsetzung der EU-Interoperabilitätsverordnungen:

- Im erläuternden Bericht werden Bestimmungen zum Datenschutz der beiden EU-Interoperabilitätsverordnungen unter jenen Bestimmungen zusammengefasst, «die in der Schweiz erst auf Verordnungsstufe umzusetzen sein werden oder gar keiner Umsetzung ins Schweizer Recht bedürfen».<sup>24</sup> Im Vernehmlassungsentwurf selbst fehlt ein Hinweis auf die Delegation entsprechender Ausführungsbestimmungen an den Bundesrat. Das ist aus Sicht der SFH ungenügend, da die Anforderungen an die Normdichte bei Datenbearbeitungsvorgängen mit einem derart grossen Gefährdungspotenzial wie bei der Interoperabilität der EU-Datensysteme besonders hoch sind. **Nach Ansicht der SFH sollten daher die Grundzüge der Materie ins Gesetz aufgenommen werden.** Im Falle einer Delegation der Regelbefugnis müsste diese im Gesetz im formellen Sinne enthalten sein.<sup>25</sup>
- Die SFH vermisst im vorgelegten Vernehmlassungsentwurf eine rechtliche Klärung der Schnittstellen zum EDSB, zur nationalen Aufsichtsbehörde sowie zum neuen Schengen-Datenschutzgesetz, das seit dem 1. März 2019 in Kraft ist. **Da der Betrieb der Interoperabilität zur Sammlung und Verarbeitung sowie zum Austausch einer grossen Anzahl sensibler Personendaten durch staatliche Stellen führt, müssen diese Schnittstellen aus Sicht der SFH auf Gesetzesstufe geklärt und geregelt werden, um dem Datenschutz und der Datensicherheit die nötige Nachachtung zu verschaffen.**
- Die Komplexität der Interoperabilität wird Auswirkungen nicht nur auf den Datenschutz, sondern auch auf die Governance und Kontrolle der Systeme haben. Das erfordert eine effiziente und starke unabhängige Aufsicht. Die SFH fordert daher, dass die nationale Aufsichtsbehörde bzw. der EDÖB mit den erforderlichen (zusätzlichen) Ressourcen ausgestattet wird, damit die Aufsichtsfunktion auch angemessen wahrgenommen werden kann.

---

<sup>24</sup> Erläuternder Bericht (Fn 3): S. 27.

<sup>25</sup> Vgl. Häfelin, Ulrich; Haller, Walter; Keller, Helen; Thurnherr, Daniela: Schweizerisches Bundesstaatsrecht, 9. Auflage, Zürich 2016.

**Per E-Mail**

Eidgenössisches Justiz-  
und Polizeidepartement EJPD  
Bundesamt für Polizei (fedpol)  
Internationale Polizeikooperation  
Abteilung Internationale  
Beziehungen, EU und Stab  
Guisanplatz 1a  
3003 Bern

St. Gallen, 9. Januar 2020

**Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen-Besitzstands)**

Sehr geehrte Frau Bundesrätin  
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Einladung zur Vernehmlassung in rubrizierter Angelegenheit. Das zur Diskussion stehende Vorhaben beinhaltet keine Aspekte, welche im Lichte der statistischen Aufgaben der Schweizerischen Vereinigung der Richterinnen und Richter (SVR-ASM) nach einer besonderen Stellungnahme unsererseits verlangen würden. Entsprechend verzichten wir auf eine Vernehmlassung.

Mit freundlichen Grüssen



Prof. Dr. Patrick Guidon  
Präsident SVR-ASM

Geschäftsstelle  
Migrationsdienst des Kantons Bern  
Corinne Karli  
Ostermündingenstrasse 99B  
CH - 3006 Bern  
Telefon +41 31 633 42 99  
Fax +41 31 633 55 86  
www.vkm-asm.ch  
info@vkm-asm.ch

Vereinigung der Kantonalen Migrationsbehörden,  
Eigerstrasse 73, 3011 Bern

---

Eidgenössisches Justiz- und  
Polizeidepartement EJPD  
Bundesamt für Polizei fedpol  
Direktion und Geschäftsleitung  
Staatssekretariat für Migration SEM  
Stabsbereich Recht

(per E-Mail: [simone.rusterholz@fed-pol.admin.ch](mailto:simone.rusterholz@fed-pol.admin.ch) [anna.wolf@fedpol.admin.ch](mailto:anna.wolf@fedpol.admin.ch)  
[sandrine.favre@sem.admin.ch](mailto:sandrine.favre@sem.admin.ch)  
[helena.schaer@sem.admin.ch](mailto:helena.schaer@sem.admin.ch))

Ihr Zeichen  
Ihre Mitteilung vom 09.10.2019  
Unser Zeichen MS/sigr  
Zuständig Corinne Karli

Bern, 19. Dezember 2019

**Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) (Weiterentwicklungen des Schengen Besitzstands)**

Sehr geehrte Frau Bundesrätin  
Sehr geehrte Frau Rusterholz  
Sehr geehrte Frau Wolf  
Sehr geehrte Frau Favre  
Sehr geehrte Frau Schaer

Die Vereinigung der Kantonalen Migrationsbehörden dankt Ihnen für die Möglichkeit, zur Übernahme und Umsetzung der Rechtsgrundlagen für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und [EU] 2019/818) Stellung nehmen zu können.

Bei der geplanten Umsetzung der EU-Verordnungen bzw. bei der Vernetzung der EU-Informationssysteme handelt es sich um eine konsequente Weiterentwicklung des Schengen Besitzstands, welche zu einer Verbesserung des Informationsaustausches zwischen den EU-Informationssystemen in den Bereichen Grenzkontrolle, Migration und Strafverfolgung führt und dadurch für mehr Sicherheit in den Schengen-Mitgliedstaaten sorgt. Als Schengen-Mitgliedstaat ist die Schweiz grundsätzlich zur Übernahme der Weiterentwicklung des Schengen Besitzstands verpflichtet.

Durch die Herstellung von Interoperabilität bzw. durch die (technische) Verbindung der EU-Informationssysteme werden vorhandene Daten effizienter und gezielter ausgetauscht und genutzt. So können mit der Schaffung eines gemeinsamen europäischen Suchportals (ESP) künftig sämtliche verfügbaren Informationen zu Personen, welche in den entsprechenden (Schengen-) Informationssystemen bzw. Datenbanken (insb. von Interpol/Europol) erfasst sind, abgefragt werden. Des Weiteren werden ein gemeinsamer Dienst zum Abgleich biometrischer Daten, ein gemeinsamer Speicher für Identitätsdaten von Drittstaatsangehörigen (CIR) und ein Detektor für Mehrfachidentitäten (MID) geschaffen, welche ebenfalls zur Sicherheit im Schengenraum beitragen, effizientere Kontrollen an den Aussengrenzen ermöglichen und einen Beitrag an die Bekämpfung von irregulärer Migration leisten.

Vor diesem Hintergrund verspricht die Herstellung von Interoperabilität einen beachtlichen Mehrwert, weshalb die Migrationsbehörden die vorgeschlagenen Änderungen bzw. die Weiterentwicklung des Schengen Besitzstandes begrüssen. Zu einzelnen Punkten haben lediglich zwei städtische und einige kantonale Migrationsbehörden Anmerkungen und Anregungen. Diese legen wir Ihnen nachfolgend dar.

## 1. Änderungen des AIG und VG

### a. Einbezug des ZEMIS

Vorab halten wir fest, dass wir davon ausgehen, dass in den vorgesehenen Änderungen des AIG, insbesondere Art. 101 ff., nebst VIS, ORBIS, SIS und Eurodac, auch das ZEMIS mit einbezogen ist; wenngleich dies nicht explizit erwähnt wird.

### b. Art. 110c E-AIG

Art. 110c E-AIG regelt, welche Behörden zur Aufdeckung von Mehrfachidentitäten von Drittstaatsangehörigen auf die im CIR (gemeinsamer Speicher für Identitätsdaten) gespeicherten Daten und Verweise zugreifen können. Gemäss Art. 110c Abs. 1 lit. c E-AIG sind dies unter anderem die für die Visa zuständigen kantonalen Migrationsbehörden. Diese Regelung wird von Seiten der Migrationsbehörden begrüsst; zumal die Möglichkeit, mit einer einzigen Suchanfrage die Identität ausländischer Personen aus Drittstaaten überprüfen zu können, einem realen Bedürfnis der Migrationsbehörden entspricht und sich auch aus dem Aktionsplan integrierte Grenzverwaltung (IBM-Strategie 2012 bzw. IBM-Aktionsplan 2014) ableiten lässt. Darüber hinaus wird diese (Zugriffs-)Regelung wirksam zur Verhinderung von Missbrauch bei der Erteilung von Visa beitragen.

Ferner sollte der Kreis der Zugriffsberechtigten generell weit genug gezogen sein, um dem 4-Filter-Konzept des IBM-Aktionsplans entsprechen zu können; dies nicht zuletzt, weil ohnehin allen Behörden, die bereits heute auf mindestens eines der Schengen-Dublin-Informationssysteme (SIS; EES, VIS, ETIAS, Eurodac und CIR) oder die Datenbanken SLTD und TDAWN von Interpol sowie Europol-Daten zugreifen können, der Online-Zugriff auf das ESP ermöglicht wird.

## 2. Mehraufwand

Wie im erläuternden Bericht zu den Gesetzesanpassungen ausgeführt wird (gemäss Ziffer 6.1.2), wird die Umsetzung der Weiterentwicklung des Schengen-Besitzstandes – nicht zuletzt durch das erhöhte Fallaufkommen – auch für die Migrationsbehörden in verschiedener Hinsicht zu Mehraufwand führen. Wie hoch dieser Mehraufwand jeweils sein wird, ist nach Ansicht verschiedener Migrationsbehörden derzeit nur schwer quantifizierbar. Darüber hinaus wird sich der Bearbeitungsaufwand zusätzlich erhöhen; nicht zuletzt durch die bereits beschlossenen Weiterentwicklungen des Schengen-Besitzstandes (Übernahme und Umsetzung der Verordnung [EU] 2018/1240 über die Einrichtung eines Europäischen Reiseinformations- und Genehmigungssystems [ETIAS] und Übernahme und Umsetzung der Rechtsgrundlagen zur Nutzung des Schengener Informationssystems [SIS] Verordnungen [EU] 2018/1862, [EU] 2018/1861 und [EU] 2018/1860) und die Änderung des BGIAA zur Registrierung der Landesverweisung im ZEMIS und zur Verbesserung der Statistik über Rückkehrentscheide.

Ferner ist gemäss Ziffer 6.3 des erläuternden Berichts aufgrund der Neuerungen der Interoperabilität bzw. der Anbindung der Schweizer Systeme an das ESP mit technischen Anpassungen verschiedener kantonaler Anwendungen zu rechnen. Der damit einhergehende Mehraufwand sowie allfällige weitere Anpassungen können zum jetzigen Zeitpunkt noch nicht abschliessend benannt werden. Gleiches gilt für den Mehraufwand im Zusammenhang mit der Verifizierung von MID-Verknüpfungen (Detektor für Mehrfachidentitäten [*Multiple Identity Detector*]), welcher aktuell nicht bzw. nur schwer abschätzbar ist.

Aus Sicht der Migrationsbehörden erscheint es deshalb zentral, dass die noch offenen Fragen zur technischen Anpassung der kantonalen Abfragesysteme sowie die konkreten Prozesse zur Verifizierung von MID-Verknüpfungen möglichst rasch geklärt werden, um daraus die notwendigen konkreten Schlüsse zu ziehen (vgl. wiederum Ziffer 6.3 des erläuternden Berichts).

Nach dem Gesagten ist damit zu rechnen, dass die genannten Mehraufwände die vorhandenen personellen Ressourcen einzelner Migrationsbehörden übersteigen werden. Nichtsdestotrotz ist sich die Mehrheit der Migrationsbehörden einig, dass der Nutzen der Interoperabilität, insbesondere in Bezug auf Sicherheitsgewinn, Verhinderung missbräuchlicher Mehrfachidentitäten und Datenqualität, (allfällige) Mehraufwände im Zusammenhang mit der vorliegenden Weiterentwicklung des Schengen-Besitzstandes aufwiegt.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und bitten Sie höflich, diese in die weiteren Revisionsarbeiten einzubeziehen.



VKM | ASM |

Vereinigung der Kantonalen Migrationsbehörden

Association des services cantonaux de migration

Associazione dei servizi cantonali di migrazione

4

Freundliche Grüsse

Marcel Suter  
Präsident