Sachdokumentation:

Signatur: DS 2397

Permalink: www.sachdokumentation.ch/bestand/ds/2397

Zitierweise für graue Literatur

Elektronische Broschüren und Flugschriften (DS) aus den Dossiers der Sachdokumentation des Sozialarchivs werden gemäss den üblichen Zitierrichtlinien für wissenschaftliche Literatur wenn möglich einzeln zitiert. Es ist jedoch sinnvoll, die verwendeten thematischen Dossiers ebenfalls zu zitieren. Anzugeben sind demnach die Signatur des einzelnen Dokuments sowie das zugehörige Dossier.

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

Impressum

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

Sprachversionen
Deutsch

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[1] (Verordnung «IOP Grenzen») und 2019/818[2] (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.[3] 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.[4] 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.[5]

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 sensitiver Daten in immensem 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.

[1] 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.
[2] 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.
[3] 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).
[4] Vgl. Ziele des Bundesrates 2020, Bd. II, S. 15.
[5] 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.[6] 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.[7] 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.[8]

---

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

[7] 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 Interoperablility, 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.

[8] Vgl. hierzu etwa Brouwer, Evelien: Interoperability of Databases and Interstate Trust: a Perilous Combination for Fundamental Rights, *VerfBlog,* 2019/5/25; Progin-Theuerkauf, Sarah, Zoeteweij-Turhan, Margarite, 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.[9] 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.»*[10] 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.[11] Studien belegen indes, dass die Aufrüstung von Grenzschutzmassnahmen bis hin zu intelligenten Grenzen die irreguläre Migration nicht massgeblich verringert.[12] 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 Aufnahmestandards und Asylverfahren in allen Mitgliedstaaten.[13]

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.»*[14]

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

[9] 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.
[10] Ebd. S. 12
[11] Vgl. Verordnung „IOP Grenzen" (Fn1): Erwägungsgrund 9 sowie Erläuternder Bericht (Fn 3): S. 8.
[12] 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.
[13] Raphael Bossung: Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit der EU. Umsetzungsrisiken und rechtsstaatliche Anforderungen, SWP Studie 4, April 2018, S. 21.
[14] 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.»*[15] Dies gilt aus Sicht der SFH umso mehr im Zusammenhang mit migrationsrechtlichen Bestimmungen, da hier ein besonderes Bedürfnis nach Datenschutz besteht.[16]

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 präziserende 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**

[15] 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.
[16] 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.[17]

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.[18]
- 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

[17] 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.

[18] 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)**
> [2]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.[19]
- **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

[19] 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»).[20]
- 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.[21] 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-Interoperablilitätsverordnungen 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.**

[20] Vgl. EDSB, Stellungnahme 4/2018 (Fn 15), S. 18.
[21] 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 gespiesen. 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 rassischen 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-Interoperablititätsverordnungen 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.[22] **Es ist daher aus Sicht der SFH mehr als fraglich, ob die Schaffung einer Datenbank mit sensitiven Informationen über Millionen von Drittstaatangehörigen 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.[23]
- 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

[22] Vgl. EDSB, Stellungnahme 4/2018 (Fn 15), S. 13.
[23] 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».[24] 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.[25]
- 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 sensitiver 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.

[24] Erläuternder Bericht (Fn 3): S. 27.
[25] Vgl. Häfelin, Ulrich; Haller, Walter; Keller, Helen; Thurnherr, Daniela: Schweizerisches Bundesstaatsrecht, 9. Auflage, Zürich 2016.