Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

20.xxx

Botschaft zur Genehmigung und Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Verordnungen (EU) 2019/817 und (EU) 2019/818 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (Weiterentwicklungen des Schengen-Besitzstands)

vom 2. September 2020

Sehr geehrte Frau Nationalratspräsidentin
Sehr geehrter Herr Ständeratspräsident
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf eines Bundesbeschlusses über die Genehmigung und die Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Verordnungen (EU) 2019/817 und (EU) 2019/818 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (Weiterentwicklungen des Schengen-Besitzstands).

Wir versichern Sie, sehr geehrte Frau Nationalratspräsidentin, sehr geehrter Herr Ständeratspräsident, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

…

Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Simonetta Sommaruga
Der Bundeskanzler: Walter Thurnherr

Übersicht

Die Interoperabilität wird verschiedene EU-Informationssysteme miteinander vernetzen. Mit einer Abfrage erhalten Grenzkontroll-, Migrations- und Strafverfolgungsbehörden künftig umfassende Informationen aus allen für sie relevanten Informationssystemen. Darüber hinaus wird die Identifizierung von Personen erleichtert, indem neu biometrische Daten aus verschiedenen Informationssystemen miteinander abgeglichen werden. Damit können die Behörden Mehrfachidentitäten und Identitätsbetrug aufdecken. Die Interoperabilität soll die Sicherheit in der Schweiz und im Schengen-Raum verbessern, effizientere Kontrollen an den Aussengrenzen ermöglichen und einen Beitrag zur Migrationssteuerung leisten. Die Zugriffsrechte der jeweiligen Behörden auf die einzelnen Systeme bleiben mit der Einführung der Interoperabilität unverändert. Die vorliegende Botschaft führt die für die Übernahme und gesetzliche Umsetzung der zwei EU-Interoperabilitätsverordnungen nötigen rechtlichen Massnahmen auf und gibt einen Überblick über die Auswirkungen auf Bund und Kantone.

Ausgangslage

Die Grenzkontroll-, Migrations- und Strafverfolgungsbehörden können auf zahlreiche Informationssysteme der EU zugreifen. Allerdings sind diese Systeme heute untereinander nicht verbunden. Um Informationen über eine Person zu erlangen, muss daher jedes Informationssystem separat abgefragt werden. Dadurch werden Synergien nicht genutzt. Mit der Interoperabilität werden die EU-Informationssysteme so miteinander vernetzt, dass vorhandene Informationen effizienter und gezielter genutzt werden können. Künftig kann eine Abfrage parallel in mehreren Informationssystemen gleichzeitig durchgeführt werden, soweit die jeweiligen Behörden über die erforderlichen Zugriffsrechte für die abgefragten Systeme verfügen. Diese werden durch die Interoperabilität nicht erweitert. Die Interoperabilität ermöglicht die Erkennung von Verknüpfungen zwischen bestehenden Daten.

Inhalt der Vorlage

Mit der Interoperabilität wird ein europäisches Suchportal geschaffen, das die gleichzeitige Abfrage in allen relevanten Informationssystemen ermöglicht. Die Interoperabilität sieht die zentrale Speicherung der Identitätsdaten und biometrischen Daten (Fingerabdrücke und Gesichtsbilder) von Drittstaatsangehörigen in einem gemeinsamen Speicher vor und ermöglicht den automatisierten Abgleich biometrischer Daten einer Person.

Durch eine effizientere Nutzung vorhandener Informationen soll die Interoperabilität die Sicherheit im Schengen-Raum und in der Schweiz verstärken sowie die Migrationssteuerung verbessern. Damit trägt die Interoperabilität zur Erreichung der Jahresziele 2020 des Bundesrates in den Bereichen Sicherheit und Migration bei. In der Kriminalitätsbekämpfung und in der Migrationssteuerung steht die Schweiz vor transnationalen Herausforderungen. Eine enge Zusammenarbeit und ein zeitnaher Informationsaustausch mit den anderen Schengen-Staaten ist für die Schweizer

Behörden von zentraler Bedeutung. Die Interoperabilität wird es den Schweizer Grenzkontroll-, Migrations- und Strafverfolgungsbehörden erleichtern, Personen zu identifizieren, die eine Bedrohung für die Sicherheit darstellen oder falsche Angaben zu ihrer Identität machen.

Die Umsetzung der beiden EU-Verordnungen (Weiterentwicklungen des Schengen-Besitzstands) bedingt Anpassungen im Ausländer- und Integrationsgesetz, im Bundesgesetz über das Informationssystem für den Ausländer- und den Asylbereich, im Verantwortlichkeitsgesetz und im Bundesgesetz über die polizeilichen Informationssysteme des Bundes.

Die Umsetzung der EU-Interoperabilitätsverordnungen ist mit einem finanziellen und personellen Mehraufwand für die Bundesverwaltung und die Kantone verbunden. Schweizer Informationssysteme und bestehende Prozesse müssen angepasst werden, um von den Möglichkeiten der Interoperabilität zu profitieren.

Inhaltsverzeichnis

Bundesbeschluss

über die Genehmigung und die Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Verordnungen (EU) 2019/817 und (EU) 2019/ 818 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen

(Weiterentwicklungen des Schengen-Besitzstands) *(Entwurf)*

Notenaustausch vom 19. Juni 2019[1] zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Verordnung (EU) 2019/817 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, der Entscheidung 2004/512/EG und des Beschlusses 2008/633/JI;

Notenaustausch vom 19. Juni 2019[2] zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Verordnung (EU) 2019/818 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.

1 SR **0.362.380.xxx**; AS **xxxxx**
2 SR **0.362.380.xxx**; AS **xxxxx**

Botschaft

1 Einleitung

Die Interoperabilität soll die Sicherheit in der Schweiz und im Schengen-Raum verbessern, effizientere Kontrollen an den Aussengrenzen ermöglichen und einen Beitrag zur Migrationssteuerung leisten. Die bestehenden EU-Informationssysteme der Schengen-/Dublin-Zusammenarbeit sollen mit der Interoperabilität künftig so vernetzt werden, dass Identitätsdaten, Daten zu den Reisedokumenten und biometrische Daten (Fingerabdrücke und Gesichtsbilder) automatisiert abgeglichen werden können. So werden die vorhandenen Informationen einfacher und schneller abgefragt. Damit wird die Sicherheit im Schengen-Raum verstärkt und die Migrationssteuerung verbessert. Von der Interoperabilität werden Strafverfolgungs-, Grenzkontroll- und Migrationsbehörden profitieren. Dabei bleiben die Zugriffsrechte der jeweiligen Behörden auf die einzelnen Systeme unverändert. Die vorliegende Botschaft betrifft die Übernahme und Umsetzung der Verordnungen (EU) 2019/817[3] und (EU) 2019/818[4] zwecks Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei.

2 Ausgangslage

2.1 Handlungsbedarf und Ziele

Schon heute können die Grenzkontroll-, Migrations- und Strafverfolgungsbehörden auf verschiedene Informationssysteme der Europäischen Union zugreifen. Jedoch sind diese Systeme untereinander technisch nicht verbunden. Die Daten sind separat in den einzelnen Informationssystemen gespeichert. Synergien können daher nicht genutzt werden und wichtige Informationen und Zusammenhänge können unentdeckt bleiben, wenn das Informationssystem, in dem die Daten erfasst sind, nicht abgefragt wird. Das Risiko besteht, dass die Behörden relevante Informationen verpassen. Folgendes Beispiel zeigt eine heute bestehende Sicherheitslücke. Diese kann mit der Interoperabilität künftig geschlossen werden.

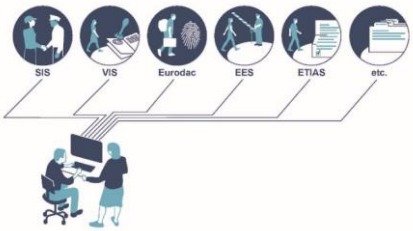
Eine kriminelle Person aus einem Drittstaat ist in der Schweiz im Schengener In-

3 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, Fassung gemäss ABl. L 135 vom 22.5.2019, S. 27.

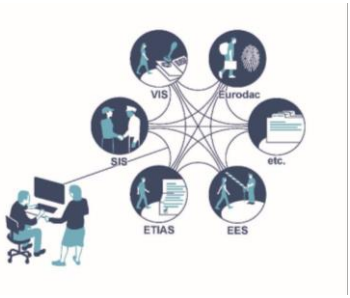
4 Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862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

formationssystem (SIS) zwecks Einreiseverbot ausgeschrieben und wurde in ihr Herkunftsland zurückgeschickt. Dieselbe Person beantragt bei einer Botschaft eines anderen Schengen-Staates ein Visum. Sie verwendet dazu eine falsche Identität. Ihre Fingerabdrücke werden zwar im Visa-Informationssystem (VIS) registriert, aber nicht mit den im SIS gespeicherten Abdrücken verglichen. Sie erhält das Visum und schafft es dadurch, wieder in den Schengen-Raum zurückzukehren.

Dank der Interoperabilität zwischen den EU-Informationssystemen werden künftig Identitätsdaten, Daten zu den Reisedokumenten und biometrische Daten (Fingerabdrücke und Gesichtsbilder) von Drittstaatsangehörigen automatisiert abgeglichen und kriminelle Personen, welche falsche Identitäten benutzen, können identifiziert werden. Somit können alle Informationssysteme (in diesem Fall das SIS und das VIS) gleichzeitig und mit nur einer Abfrage konsultiert werden.



Ohne Interoperabilität müsste jedes System separat angefragt werden.



Mit Interoperabilität werden die Behörden durch eine Abfrage alle Informationssysteme gleichzeitig abfragen können.

Interoperabilität bedeutet also, die EU-Informationssysteme so miteinander zu vernetzen, dass vorhandene Informationen effizienter und gezielter genutzt werden können. Mit der Interoperabilität sollen die berechtigten Behörden künftig über alle für ihre Aufgaben relevanten Informationen verfügen und damit rasch und effizient ein umfassendes Bild einer Person erhalten. Ziel ist, dass die Behörden stets über die relevanten Informationen verfügen können, sodass – in Situationen wie im vorher erwähnten Beispiel – kein Visum an eine kriminelle Person aus einem Drittstaat ausgestellt wird.

Zu diesem Zweck verabschiedeten das Europäische Parlament und der Rat der Europäischen Union am 20. Mai 2019 zwei Verordnungen, die die Herstellung der Interoperabilität zwischen EU-Informationssystemen zum Ziel haben.

– Die Verordnung (EU) 2019/817 betrifft die Bereiche Grenzen und Visa (nachfolgend: Verordnung «IOP Grenzen»).

– Die Verordnung (EU) 2019/818 betrifft die Bereiche polizeiliche und justizielle Zusammenarbeit, Asyl und Migration (nachfolgend: Verordnung «IOP Polizei»).

Mit der Interoperabilität sollen folgende Komponenten geschaffen werden:

- das Europäische Suchportal (ESP), das den zuständigen Behörden gleichzeitige Abfragen in mehreren Informationssystemen ermöglichen wird;
- der gemeinsame Dienst für den Abgleich biometrischer Daten (sBMS), der den Abgleich biometrischer Daten (Fingerabdrücke und Gesichtsbilder) aus mehreren Systemen möglich machen wird;
- der gemeinsame Speicher für Identitätsdaten (CIR), der Identitätsdaten, Daten zu den Reisedokumenten und biometrische Daten von Drittstaatsangehörigen aus mehreren EU-Informationssystemen enthalten wird;
- der Detektor für Mehrfachidentitäten (MID), mit dem sich Verknüpfungen zwischen Daten aus den angeschlossenen Systemen aufzeigen (sog. MID-Verknüpfungen) und die Nutzung falscher oder mehrerer Identitäten aufdecken lassen werden.

Mit der Interoperabilität werden keine neuen Daten erhoben, sondern lediglich zusätzliche Funktionen für die bestehenden und zukünftigen Informationssysteme (SIS, VIS, Einreise- und Ausreisesystem [EES], Europäisches Reiseinformations- und -genehmigungssystem [ETIAS], zentrale Datenbank der Europäischen Union, in der Fingerabdrücke von Personen gespeichert sind, die in einem Dublin-Staat ein Asylgesuch einreichen oder bei der illegalen Einreise aufgegriffen werden [Eurodac]) geschaffen. Für die Behörden ändert sich dadurch nichts an den bestehenden Zugriffsrechten auf die zugrundeliegenden Informationssysteme.

Die zwei EU-Verordnungen zur Interoperabilität wurden im Nachgang an die seit 2015 im Schengen-Raum verübten terroristischen Anschläge und die gesteigerten Herausforderungen im Migrationsbereich erarbeitet. Die Weiterentwicklung und der Ausbau der IT-Struktur der EU stellen zentrale Elemente zur Verbesserung der Sicherheit im Schengen-Raum dar. Die Interoperabilität der EU-Informationssysteme spielt eine wichtige Rolle bei der Schliessung bestehender Sicherheitslücken. Der erleichterte Datenaustausch zwischen den verschiedenen Informationssystemen soll aber auch schnellere und wirksamere Kontrollen an den Schengen-Aussengrenzen ermöglichen und einen Beitrag zur Bekämpfung der irregulären Migration leisten. So sollen in Zukunft vorhandene Informationen effizienter und gezielter genutzt werden können, was einen grossen Mehrwert für die Arbeit der Strafverfolgungs-, Grenzkontroll- und Migrationsbehörden darstellt.

Die Schweiz hat sich mit dem Schengen-Assoziierungsabkommen (SAA)[5] grundsätzlich zur Übernahme aller Weiterentwicklungen des Schengen-Besitzstands verpflichtet (Art. 2 Abs. 3 und Art. 7 SAA). Die Übernahme eines neuen Rechtsakts erfolgt dabei in einem besonderen Verfahren, das die Notifikation der Weiterentwicklung durch die zuständigen EU-Organe und die Übermittlung einer Antwortnote seitens der Schweiz umfasst.

Die zwei EU-Verordnungen wurden der Schweiz am 21. Mai 2019 als Weiterentwicklungen des Schengen-Besitzstands notifiziert. Der Bundesrat hat die Notenaustausche zur Übernahme der EU-Verordnungen am 14. Juni 2019 unter Vorbehalt der parlamentarischen Genehmigung gutgeheissen. Die entsprechende Antwortnote wurde der EU am 19. Juni 2019 übermittelt. Ziel dieser Vorlage ist es, die Schengen-Weiterentwicklungen fristgerecht zu übernehmen und die notwendigen rechtlichen Grundlagen für deren Umsetzung zu schaffen. Die Schweiz verfügt hierfür über eine Frist von maximal zwei Jahren. Die Frist läuft am 21. Mai 2021 ab.

2.2 Verhandlungsverlauf

Am 12. Dezember 2017 stellte die EU-Kommission die zwei Verordnungsvorschläge zur Interoperabilität vor, welche gemeinsam die Rechtsgrundlage für die Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei bilden. Die Diskussionen im Rat der EU dauerten von Januar bis September 2018, und die Verhandlungen mit dem europäischen Parlament (Trilog) von Oktober 2018 bis Februar 2019. Die Vertreter der Schweiz haben an allen Sitzungen teilgenommen, konnten technische Fragen klären und ihre Lösungsvorschläge in allen Verhandlungsetappen einbringen.

Besonders intensive Diskussionen fanden zu den folgenden Themen statt:

- Umsetzung: Thematisiert wurden nebst den finanziellen Folgen für die Schengen-Staaten auch die Auswirkungen der Implementierung auf die Personenkontrollen an den Schengen-Aussengrenzen. Bedenken bestanden insbesondere zur technischen Machbarkeit einer zeitnahen Abfrage in allen interoperablen Systemen während Personenkontrollen an den Schengen-Aussengrenzen.
- Personeller Mehrbedarf: Wiederholt traktandiert waren der zusätzliche Personalaufwand für die Schengen-Staaten und die Zusatzbelastung für bestehende Stellen wie die nationalen SIRENE-Büros, welche für den Informationsaustausch und die Koordination des Vorgehens im Fall eines SIS-Treffers zuständig sind.
- «Variable Geometrie»: Der Begriff der variablen Geometrie umfasst die Problematik der Nicht-Teilnahme einzelner Staaten an einem oder mehreren EU-Informationssystemen. Der unterschiedlich ausgeprägte Integrationsgrad führt

5 Abkommen vom 26. Okt. 2004 zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, SR **0.362.31**

bei interoperablen Systemen zu unterschiedlichen Abfrageresultaten der interoperablen Zentralsysteme. Betroffen sind derzeit vor allem das Vereinigte Königreich und Irland, welche ohne Zugang zum SIS die Funktionalität des MID zur Erkennung von Mehrfachidentitäten einbüssen, aber auch die Schweiz und andere assoziierte Staaten, aufgrund des eingeschränkten Zugangs zu Daten des Europäischen Polizeiamts (Europol) oder des fehlenden Zugangs zum Europäischen Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN).

- Abfrage der Datenbanken der Internationalen Kriminalpolizeilichen Organisation (Interpol): Die mit der Interoperabilität vorgesehenen rechtlichen Grundlagen für eine Abfrage der Interpol-Datenbanken sind weiterhin Gegenstand von Diskussionen. Die offenen Fragen sollen in einem Abkommen zwischen der EU und Interpol geregelt werden.
- Weitere Themen: Zugriff auf den CIR zu Identifikationszwecken bzw. zu Zwecken der Strafverfolgung und die Information der betroffenen Drittstaatsangehörigen.

Der erzielte Kompromiss wurde vom Plenum des Europäischen Parlaments am 16. April 2019 und vom Ministerrat am 14. Mai 2019 gebilligt. Die formelle Verabschiedung der Verordnungen folgte am 20. Mai 2019 mittels Unterzeichnung des Rechtsaktes durch die Präsidenten des Europäischen Parlaments und des Rates der EU. Die Weiterentwicklungen des Schengen-Besitzstands wurden der Schweiz am 21. Mai 2019 notifiziert.

2.3 Verfahren zur Übernahme der Weiterentwicklungen des Schengen-Besitzstands

Gestützt auf Artikel 2 Absatz 3 SAA hat sich die Schweiz grundsätzlich verpflichtet, alle Rechtsakte, welche die EU seit der Unterzeichnung des SAA am 26. Oktober 2004 als Weiterentwicklungen des Schengen-Besitzstands erlassen hat, zu übernehmen und, soweit erforderlich, in das Schweizer Recht umzusetzen.

Artikel 7 SAA sieht ein spezielles Verfahren für die Übernahme und Umsetzung von Weiterentwicklungen des Schengen-Besitzstands vor. Zunächst notifiziert die EU der Schweiz «unverzüglich» die Annahme eines Rechtsakts, der eine Weiterentwicklung des Schengen-Besitzstands darstellt. Danach verfügt der Bundesrat über eine Frist von dreissig Tagen, um dem zuständigen Organ der EU (Rat der EU oder EU-Kommission) mitzuteilen, ob und gegebenenfalls innert welcher Frist die Schweiz die Weiterentwicklung übernimmt. Die dreissigtägige Frist beginnt mit der Annahme des Rechtsakts durch die EU zu laufen (Art. 7 Abs. 2 Bst. a SAA).

Soweit die zu übernehmende Weiterentwicklung rechtlich verbindlicher Natur ist, bilden die Notifizierung durch die EU und die Antwortnote der Schweiz einen Notenaustausch, der aus Sicht der Schweiz einen völkerrechtlichen Vertrag darstellt. Im Einklang mit den verfassungsrechtlichen Vorgaben muss dieser Vertrag entweder vom Bundesrat oder vom Parlament und, im Fall eines Referendums, vom Volk genehmigt werden.

Die zur Übernahme anstehenden zwei EU-Verordnungen sind rechtsverbindlich. Die Übernahme der vorliegenden EU-Verordnungen muss deshalb mittels Abschluss eines Notenaustauschs erfolgen.

Vorliegend ist die Bundesversammlung für die Genehmigung der Notenaustausche zuständig (vgl. Ziff. 10.1). Entsprechend hat die Schweiz der EU am 19. Juni 2019 in ihren Antwortnoten mitgeteilt, dass die betreffende Weiterentwicklung für sie erst «nach Erfüllung ihrer verfassungsrechtlichen Voraussetzungen» rechtsverbindlich werden kann (Art. 7 Abs. 2 Bst. b SAA). Ab der Notifizierung der Rechtsakte durch die EU verfügt die Schweiz für die Übernahme und Umsetzung der Weiterentwicklungen über eine Frist von maximal zwei Jahren. Innerhalb dieser Frist muss auch eine allfällige Referendumsabstimmung stattfinden.

Sobald das innerstaatliche Verfahren abgeschlossen ist und alle verfassungsrechtlichen Voraussetzungen im Hinblick auf die Übernahme und Umsetzung der EU-Verordnungen erfüllt sind, unterrichtet die Schweiz den Rat der EU und die EU-Kommission unverzüglich in schriftlicher Form hierüber. Wird kein Referendum gegen die Übernahme und Umsetzung der EU-Verordnungen ergriffen, erfolgt diese Mitteilung, die der Ratifizierung der Notenaustausche gleichkommt, unverzüglich nach Ablauf der Referendumsfrist.

Setzt die Schweiz eine Weiterentwicklung des Schengen-Besitzstandes nicht fristgerecht um, so riskiert sie die Beendigung der Zusammenarbeit von Schengen insgesamt, und damit auch von Dublin (Art. 7 Abs. 4 SAA i. V. m. Art. 14 Abs. 2 DAA[6]).

Ausgehend vom Datum der Notifikation durch die EU (21. Mai 2019) endet die Frist von maximal zwei Jahren für die Übernahme und Umsetzung der EU-Verordnungen somit am 21. Mai 2021. Da die Inbetriebnahme der Interoperabilitätskomponenten und damit der Anwendungsbeginn der einschlägigen Bestimmungen der EU-Verordnungen erst für einen späteren Zeitpunkt vorgesehen ist (zu Einzelheiten s. u. Ziff. 4.2), dürfte aber *de facto* ein gewisses Mass an Flexibilität bestehen, das es erlaubt, die Frist gegebenenfalls in pragmatischer Weise etwas zu überschreiten. Dies ist bei den EU-Interoperabilitätsverordnungen der Fall, da die einzelnen Zentralkomponenten zeitlich gestaffelt in Betrieb genommen werden und die vollständige Umsetzung nicht vor 2023 geplant ist.

2.4 Verhältnis zur Legislaturplanung und zur Finanzplanung sowie zu Strategien des Bundesrates

Die Verabschiedung der vorliegenden Botschaft ist ein Jahresziel des Bundesrates für das Jahr 2020. Die Vorlage ist in der Botschaft vom 29. Januar 2020 zur Legislaturplanung 2019–2023 angekündigt[7].

6 Abkommen vom 26. Okt. 2004 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags; SR **0.142.392.68.**

Mit der optimalen und interoperablen Anwendung der verschiedenen EU-Informationssysteme erneuert und entwickelt die Schweiz ihre politischen und wirtschaftlichen Beziehungen zur EU. Die umfassende und zeitnahe Bereitstellung der relevanten Informationen für die zuständigen Behörden trägt zum Ziel der Migrationssteuerung und Verhinderung der irregulären Migration bei. Die Schweiz soll Gewalt, Kriminalität und Terrorismus vorbeugen und wirksam bekämpfen. Sie soll die Sicherheitsbedrohungen kennen und über die notwendigen Instrumente verfügen, um diesen wirksam entgegenzutreten. Die Interoperabilität unterstützt dies, indem sie eine effizientere Nutzung der EU-Informationssysteme ermöglicht.

Für die Realisierung der Interoperabilität der EU-Informationssysteme ist im Voranschlag 2020 mit integriertem Aufgaben- und Finanzplan 2021-2023 eine erste Tranche enthalten. Nachdem die aktualisierten Projektmanagementpläne sowie ein Qualitäts- und Risikobericht der betroffenen Projekte vorliegen, wird der Bundesrat die zweite Tranche des Verpflichtungskredites «Weiterentwicklung Schengen/Dublin» freigeben. Die Freigabe sämtlicher Mittel darf nur erfolgen, wenn die Bundesversammlung die gesetzlichen Grundlagen beschlossen hat.

Die Übernahme und Umsetzung der EU-Interoperabilitätsverordnungen stehen mit keiner Strategie des Bundesrats in Konflikt. Sie ist angezeigt, um den Verpflichtungen der Schweiz aus dem SAA nachzukommen.

3 Vernehmlassungsverfahren

3.1 Übersicht

Gestützt auf Artikel 3 Absatz 1 Buchstabe c des Vernehmlassungsgesetzes vom 18. März 2005[8] wurde vom 9. Oktober 2019 bis zum 9. Januar 2020 eine Vernehmlassung durchgeführt.

Zur Vorlage sind 44 Rückmeldungen eingegangen. Insgesamt haben sich alle Kantone, drei politische Parteien, fünf Dachverbände, das Bundesverwaltungsgericht sowie neun weitere interessierte Kreise schriftlich geäussert. Davon haben sieben Teilnehmende ausdrücklich auf eine Stellungnahme verzichtet.

32 Vernehmlassungsteilnehmende begrüssen die Vorlage. Davon haben elf keine Bemerkungen angebracht. Drei Vernehmlassungsteilnehmende fordern Nachbesserungen bei der Umsetzung. Die Ergebnisse der Vernehmlassung können dem Ergebnisbericht[9] entnommen werden.

Zahlreiche Kantone (AI, FR, GE, JU, LU, NE, OW, SH, SO, TI, VS, ZG) sowie die Vereinigung der kantonalen Migrationsbehörden (VKM) verweisen auf zusätzliche Kosten und Mehraufwand, wobei ein Teil davon (AI, LU, VS, VKM) darauf hinweist, dass der Mehrwert der Interoperabilität für die Sicherheit überwiege. JU und

7 BBI **2020** 1777, hier 1896
8 SR **172.061**
9 www.admin.ch > Bundesrecht > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2019 > EJPD

TI fordern eine klarere Auskunft des Bundesrats an die Kantone über das Ausmass der Kosten und den potenziellen Mehraufwand. OW und GE fordern vom Bund finanzielle Unterstützung oder Entschädigungszahlungen für die Kantone. FDP und SVP erwarten für die parlamentarische Beratung genauere Angaben zu Machbarkeit, Umsetzung und Finanzierung der Interoperabilität.

Mehrere Organisationen (Schweizerische Flüchtlingshilfe (SFH), Schweizerischer Gewerkschaftsbund (SGB), AsyLex, SP) befürworten zwar die Übernahme dieser Schengen-Weiterentwicklungen, die sicherstellen, dass die Schweiz weiterhin Mitglied bei Schengen/Dublin bleibt, stehen der Vorlage aber eher kritisch gegenüber und sprechen sich teilweise für eine Verstärkung des Grundrechts- und des Datenschutzes aus. Angesichts der überwiegend positiven Stellungnahmen bleibt der Bundesbeschluss unverändert. Nachfolgend wird vertieft auf die Anliegen der Vernehmlassungsteilnehmenden eingegangen.

3.2 Detaillierte Vorbringen

Datenschutz

Mehrere Vernehmlassungsteilnehmende kritisieren, dass der Grundrechts- und Datenschutz von Drittstaatsangehörigen nicht ausreichend gewahrt werde. Ferner werden Hackerangriffe befürchtet. Deswegen fordern mehrere Vernehmlassungsteilnehmende die Einführung und Durchsetzung staatlicher Kontrollpflichten und von Datenschutzvorgaben. Aufgrund zusätzlicher Aufgaben für die Datenschutzaufsichtsbehörden fordern einige Vernehmlassungsteilnehmende eine personelle, eventuell sogar organisatorische Aufstockung beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und den kantonalen Datenschutzaufsichtsbehörden.

Die Sozialdemokratische Partei Schweiz (SP) schlägt einen neuen Artikel 111*k* E-AIG vor, gemäss welchem der EDÖB als nationale Aufsichtsbehörde jährlich die Zahl der Anträge auf Berichtigungen, Löschungen oder Einschränkungen der Verarbeitung personenbezogener Daten sowie die Zahl der tatsächlich vorgenommenen Berichtigungen und Löschungen veröffentlichen sollte. Des Weiteren beschreibt er die Berichterstattung des EDÖB an den Europäischen Datenschutzbeauftragten, die anderen nationalen Aufsichtsbehörden und ans Schweizer Parlament.

Der Bundesrat habe zudem für eine ausreichende Ressourcenausstattung des EDÖB zu sorgen. Der Bundesrat hält dazu fest, dass die beiden EU-Interoperabilitätsverordnungen, die unter Einbezug des Europäischen Datenschutzbeauftragten erarbeitet wurden, ein ganzes Kapitel dem Datenschutz und dessen Überwachung widmen (Kap. VII der EU-Interoperabilitätsverordnungen). Dabei ist etwa auch eine Kontrolle durch den Europäischen Datenschutzbeauftragten vorgesehen. Zudem kann auf das Kapitel 14*c* E-AIG verwiesen werden, welches neu alle Bestimmungen enthält, welche den Datenschutz im Rahmen des Schengen-Assoziierungsabkommens betreffen. Es gelten die datenschutzrechtlichen Grundprinzipien. Folglich muss der Zugriff auf die Daten in einem angemessenen Verhältnis zu den verfolgten Zielen stehen und darf nur erfolgen, soweit die Daten für die

Erfüllung der Aufgaben der zuständigen Behörden erforderlich sind. Zentral für die datenschutzrechtliche Beurteilung ist zudem, dass Zugriffsrechte der Behörden auf die der Interoperabilität zugrundeliegenden Informationssysteme nicht erweitert werden. Diese bleiben unverändert in den spezifischen Rechtsgrundlagen dieser Informationssysteme geregelt.

Soweit die Datenabfrage und -bearbeitung zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung erfolgt, gelten die Vorgaben der Richtlinie (EU) 2016/680[10], die mit dem Schengen-Datenschutzgesetz vom 28. September 2018[11] (SDSG) ins schweizerische Recht übernommen wurde. Soweit die Datenbearbeitung zu anderen Zwecken erfolgt, so setzen die EU-Interoperabilitätsverordnungen die Anwendung der Datenschutz-Grundverordnung (Verordnung [EU] 2016/679)[12] voraus. Diese ist als solche zwar für die Schweiz nicht verbindlich, da sie von der EU seinerzeit nicht als Schengen-relevant qualifiziert und von der Schweiz in der Folge auch nicht als Weiterentwicklung übernommen worden ist. Gleichwohl sind deren Vorgaben für Datenbearbeitungen im Rahmen der Schengener Zusammenarbeit *mittelbar* relevant. Ihnen wird im Rahmen der laufenden Totalrevision des Bundesgesetzes vom 19. Juni 1992[13] über den Datenschutz (DSG) Rechnung getragen. Ziel der umfassend angelegten DSG-Revision ist es, sowohl im privaten als auch im öffentlichen Sektor ein äquivalentes Schutzniveau in der Schweiz herzustellen[14], weshalb sich eine gesonderte Umsetzung der Datenschutz-Grundverordnung im Rahmen dieser Vorlage erübrigt.

Die Datensätze in den Interoperabilitätskomponenten unterliegen denselben hohen Datenschutzstandards wie diejenigen der Informationssysteme, welche der Interoperabilität zugrunde liegen. Für die Verarbeitung von Daten im sBMS und im CIR sind diejenigen Behörden der Schengen/Dublin-Staaten zuständig, die jeweils für die Datenverarbeitung im SIS, VIS und EES zuständig sind. Für die Verarbeitung von Daten im MID sind die ETIAS-Zentralstelle sowie diejenigen Behörden der Schengen/Dublin-Staaten zuständig, die Daten in der Identitätsbestätigungsdatei hinzufügen oder ändern. Für die Sicherheit der Zentralkomponenten und der Kommunikationsinfrastruktur ist die europäische Agentur für das Betriebsmanagement von IT-Grosssystemen (eu-LISA) zuständig. eu-LISA wird beispielsweise im Störungsfall für die Wiederherstellung des Normalbetriebs sorgen.

10 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 4.5.2016, S. 89.

11 SR **235.3**

12 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27, April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. 119 vom 4.5.2016, S. 1.

13 SR **235.1**

14 Vgl. Botschaft vom 15. Sept. 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl **2017** 6941.

Zum vorgeschlagenen Artikel 111k E-AIG hält der Bundesrat fest, dass die Forderungen Artikel 51 Absätze 2 und 4 sowie Artikel 37 Absatz 5 der EU-Interoperabilitätsverordnungen entsprechen. Diese sind für die Schweiz mit der Übernahme rechtlich verbindlich. Der Bundesbeschluss wiederholt Bestimmungen aus den EU-Verordnungen nur insoweit als dies insbesondere nach dem DSG erforderlich ist. So sind beispielsweise die Zwecke der Datenbearbeitung, die Zugriffsrechte, die Datenweitergabe und die Sanktion der missbräuchlichen Datenbearbeitung formell-gesetzlich zu regeln. Eine Wiederholung aller Artikel der EU-Interoperabilitätsverordnungen im Schweizerischen Gesetz ist aber nicht zielführend.

Hinsichtlich der Anforderungen an die Aufsichtsbehörden verweisen die EU-Interoperabilitätsverordnungen auf die Richtlinie (EU) 2016/680 sowie die Verordnung (EU) 2016/679. Soweit auf die Richtlinie (EU) 2016/680 Bezug genommen wird, wurde die Aufsichtsbehörde so ausgestattet, wie es die Richtlinie vorsieht (vgl. Artikel 21–25 SDSG).

Bezüglich der Kontrollmechanismen ist darauf hinzuweisen, dass in der Schweiz bereits bewährte Strukturen bestehen, die zudem im Bereich der Schengen/Dublin-Informationssysteme kontinuierlich ausgebaut wurden. Der EDÖB und die kantonalen Datenschutzbehörden arbeiten im Rahmen ihrer jeweiligen Zuständigkeiten aktiv zusammen und sorgen für eine koordinierte Aufsicht über die Bearbeitung von Personendaten. Der EDÖB koordiniert die Aufsichtstätigkeit mit den kantonalen Datenschutzbehörden und ist die nationale Ansprechstelle für den Europäischen Datenschutzbeauftragten. Der EDÖB wurde bezüglich seiner Aufgabe in dieser Vorlage konsultiert und hatte keine Einwände. Bestimmungen betreffend die Wahrnehmung der Rechte Betroffener (Recht auf Auskunft, Berichtigung und Löschung), die Datensicherheit und die Aufsicht über die Datenbearbeitung werden in der ausführenden Verordnung zu erlassen sein.

Schliesslich haben die Schengen/Dublin-Staaten gemäss den EU-Interoperabilitätsverordnungen sicherzustellen, dass jede unrechtmässige Verarbeitung oder jeder unrechtmässige Austausch von Daten nach nationalem Recht geahndet wird. Die entsprechende Sanktionsbestimmung besteht bereits in Artikel 120*d* E-AIG. Die Bestimmung wurde in Umsetzung der EU-VIS-Verordnung[15] eingeführt und in der Folge mit dem EES und dem ETIAS und jetzt wiederum mit dem MID und dem CIR ergänzt. Es sind keine Gründe ersichtlich, die Höhe der Strafsanktion anzupassen.

Stigmatisierung und Diskriminierung von Drittstaatsangehörigen

Mehrere Vernehmlassungsteilnehmende (AsyLex, SGB, SFH, SP) sehen diese Vorlage als weiteren Schritt zur Diskriminierung, Ungleichbehandlung und Stigma-

15 Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung), ABl. L 218 vom 13.8.2008, S. 60; zuletzt geändert durch Verordnung (EU) 2019/817, ABl. L 135 vom 22.5.2019, S. 27.

tisierung von Drittstaatsangehörigen gegenüber EU/EFTA-Bürgerinnen und -Bürgern. Dies äussere sich insbesondere im systematischen Gebrauch von biometrischen Daten. Kritisiert wird auch die der Vorlage zugrundeliegende Tendenz, Migration hauptsächlich unter dem Aspekt der inneren Sicherheit zu betrachten.

Der Bundesrat nimmt diese Bedenken zur Kenntnis und hält dazu fest, dass durch die Interoperabilität keine zusätzlichen Daten erhoben werden. Die Interoperabilität stellt keine Benachteiligung von Drittstaatsangehörigen dar, sondern erleichtert die eindeutige Identifizierung von Personen anhand biometrischer Daten und damit auch die Mobilität von rechtmässig reisenden Drittstaatsangehörigen im Schengen-Raum.

Information des ausschreibenden Staates bei Interpol-Abfragen

Einzelne Vernehmlassungsteilnehmende (AsyLex, SGB, SFH) kritisieren, dass bei der Abfrage von Interpol-Datenbanken über das ESP die ausschreibende Behörde, d.h. allenfalls auch ein Drittstaat, bei einem Treffer über den Zeitpunkt und den Ort der Abfrage informiert wird. Das könne zu Missbrauchsfällen führen.

Der Bundesrat hält dazu fest, dass Treffer nach den EU-Interoperabilitätsverordnungen nicht mit dem ausschreibenden Staat geteilt werden. Es finden derzeit Gespräche zwischen der EU und Interpol über die Anbindung von Interpol-Datenbanken an die Interoperabilität statt, damit diese Voraussetzung erfüllt werden kann.

Verfassungsmässigkeit

Die SP kritisiert eine ungenügende materielle Verfassungsgrundlage, da die Umsetzung der Interoperabilität über die Aussenpolitik hinausgeht, weil sie in die Bereiche Asyl, Migration und Sicherheit eingreift.

Der Bundesrat hält fest, dass die Umsetzung der Interoperabilität über eine Verfassungsgrundlage verfügt (Art. 54 Abs. 1 der Bundesverfassung [BV][16]), da die Interoperabilität den Schengen-Raum betrifft, an den die Schweiz assoziiert ist, und sich daher auf die Aussenpolitik bezieht. Diese Kooperation beinhaltet Aspekte der Sicherheit und Migration. Da es sich um die Übernahme von internationalen Verträgen handelt, ist diese Bestimmung der BV massgebend.

Der Bundesrat stellt fest, dass die Interoperabilität weitreichende Auswirkungen hat, da sie alle Drittstaatsangehörigen betrifft und verschiedene Grundrechte berührt. Dazu gehört das Recht auf Bewegungsfreiheit (Art. 10 Abs. 2 BV). Die Bewegungsfreiheit wird durch die Interoperabilität nicht übermässig eingeschränkt. Weiterhin gilt auch das Recht auf Schutz vor Missbrauch der persönlichen Daten (Art. 13 Abs. 2 BV). Der Bundesrat unterstreicht hierbei die Rolle des EDÖB sowie der kantonalen Datenschutzbehörden in der Aufsicht. Des Weiteren gilt es festzuhalten, dass die Interoperabilität nicht direkt den Asylbereich betrifft. Die Einreise- und Aufenthaltsbedingungen werden mit der Interoperabilität nicht verändert.

16 SR **101**

Unabhängig davon engagiert sich die Schweiz auf verschiedenen Ebenen zugunsten schutzbedürftiger Personen. Der Bundesrat hat 2019 ein Resettlement-Programm verabschiedet, in dessen Rahmen er jeweils für einen Zeitraum von zwei Jahren die Aufnahme besonders vulnerabler Flüchtlinge festlegt. Ebenfalls kann die Schweiz humanitäre Visa erteilen, wenn bei einer Person aufgrund des konkreten Einzelfalls offensichtlich davon ausgegangen werden muss, dass sie im Heimat- oder Herkunftsstaat unmittelbar, ernsthaft und konkret an Leib und Leben gefährdet ist (Art. 4 Abs. 2 der Verordnung vom 15. August 2018[17] über die Einreise und die Visumerteilung).

4 Grundzüge der EU-Verordnungen

4.1 Übersicht

Die Interoperabilität ist aufgrund des unterschiedlichen Beteiligungsgrades der Staaten an der Schengener Zusammenarbeit in der EU in zwei Verordnungen geregelt. Die erste Verordnung, die Verordnung «IOP Grenzen» betrifft die Bereiche Grenzen und Visa, die Verordnung «IOP Polizei» die polizeiliche und justizielle Zusammenarbeit, Asyl und Migration. Die beiden EU-Verordnungen sind bis auf wenige Bestimmungen deckungsgleich. Die Interoperabilität schafft keine zusätzlichen Datenbanken, sondern integriert neue Funktionen in existierende und zukünftige Informationssysteme.

Mit den beiden EU-Interoperabilitätsverordnungen werden die folgenden vier neuen Zentralkomponenten für die EU-Informationssysteme geschaffen:

- das Europäische Suchportal (*European Search Portal*, nachfolgend «ESP»), das es den zuständigen Behörden erlauben wird, mittels einer Abfrage gleichzeitig mehrere EU-Informationssysteme zu konsultieren;
- der gemeinsame Dienst für den Abgleich biometrischer Daten (*shared Biometric Matching Service*, nachfolgend «sBMS»), der die systemübergreifende Abfrage mehrerer EU-Informationssysteme mittels biometrischer Daten möglich machen wird;
- der gemeinsame Speicher für Identitätsdaten (*Common Identity Repository*, nachfolgend «CIR»), der die Identitätsdaten (bspw. Name und Geburtsdatum), die Daten zu den Reisedokumenten und die biometrischen Daten von Drittstaatsangehörigen enthält und damit deren Identifizierung erleichtern wird; und
- der Detektor für Mehrfachidentitäten (*Multiple Identity Detector*, nachfolgend «MID»), der Zusammenhänge zwischen neuen und bestehenden Daten in verschiedenen EU-Informationssystemen aufdecken und so zur Bekämpfung von Identitätsbetrug beitragen wird.

Betroffen von den EU-Interoperabilitätsverordnungen sind die folgenden EU-Informationssysteme und Datenbanken:

17 SR **142.204**

- das Schengener Informationssystem (SIS), welches Informationen zu gesuchten oder vermissten Personen sowie gesuchten Fahrzeugen und Sachen enthält und in welchem Einreiseverbote und künftig auch Rückkehrentscheide ausgeschrieben werden;
- das Visa-Informationssystem (C-VIS), welches die Informationen zu den Schengen-Visa enthält;
- Eurodac, die zentrale Datenbank für Fingerabdrücke von Asylsuchenden und Personen, die bei der illegalen Einreise aufgegriffen werden;
- das Europäische Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN), ein elektronisches System für den Austausch über Strafregistereinträge zwischen den EU-Staaten;
- das Einreise- und Ausreisesystem (EES), in welchem künftig die Angaben zu Ein- und Ausreisen von Drittstaatsangehörigen, die für einen Aufenthalt von höchstens 90 Tagen je Zeitraum von 180 Tagen in den Schengen-Raum einreisen, sowie die Einreiseverweigerungen erfasst werden;
- das Europäische Reiseinformations- und -genehmigungssystem (ETIAS), durch welches visumsbefreite Drittstaatsangehörige in Zukunft eine Reisegenehmigung beantragen und erhalten müssen, bevor sie in den Schengen-Raum einreisen;
- die Europol-Daten (*Europol Information System*); und
- die Interpol-Datenbanken für gestohlene und verlorene Reisedokumente (*Stolen and Lost Travel Documents*, nachfolgend «SLTD») und jene zur Erfassung von Ausschreibungen zugeordneten Reisedokumenten (*Travel Documents Associated with Notices*, nachfolgend «TDAWN»).

Die Schweiz beteiligt sich bereits an den Informationssystemen SIS, VIS und Eurodac. Eine Beteiligung an den neuen Systemen EES und ETIAS, welche auch Teil des Schengen-Besitzstandes sind, ist ebenfalls vorgesehen. Die Übernahme und Umsetzung der EES-Verordnung wurde im Juni 2019 durch das Parlament gutgeheissen.[18] Die Botschaft zur Übernahme und Umsetzung der ETIAS-Verordnung verabschiedete der Bundesrat am 6. März 2020.[19] Diese Vorlage befindet sich derzeit in der parlamentarischen Beratung. Bis November 2020 hat die Schweiz auch die Weiterentwicklungen des SIS zu übernehmen, wodurch zusätzliche Möglichkeiten für die Polizei- und Migrationskooperation geschaffen werden, u.a. durch die Einführung einer neuen Rückkehrausschreibung. Der Bundesrat verabschiedete die Botschaft zu den SIS-Verordnungen am 6. März 2020.[20] Diese Vorlage befindet sich derzeit in der parlamentarischen Beratung.

Das ECRIS-TCN stellt hingegen keine Weiterentwicklung des Schengen-Besitzstandes dar und die Schweiz hat folglich keinen Zugang dazu. Sie prüft derzeit eine mögliche Teilnahme. Es wird daher in den EU-Verordnungen von der Interope-

18 BBl **2019** 4573
19 BBl **2020** 2885
20 BBl **2020** 3575

rabilität der «EU-Informationssysteme» gesprochen. Diese Formulierung wird in der vorliegenden Botschaft verwendet mit Ausnahme des Kapitels 7. Was die rechtliche Umsetzung in der Schweiz angeht, wird hingegen der Begriff «Schengen/Dublin-Informationssysteme» verwendet, da nur diese im Schweizer Recht umgesetzt werden müssen.

Auch auf Europol-Daten hat die Schweiz derzeit keinen direkten Zugriff. Basierend auf den Artikeln 8 und 9 des Abkommens vom 24. September 2004[21] zwischen der Schweizerischen Eidgenossenschaft und dem Europäischen Polizeiamt kann die Schweiz Ersuchen an Europol richten, um Informationen aus dem Europol-Informationssystem zu erhalten. Die Schweiz setzt sich für einen direkten Zugriff auf Europol-Daten ein. Gegenwärtig laufen Diskussionen dazu, ob die EU den Schengen-assoziierten Staaten zukünftig via ESP einen direkten Zugang zu ihren Daten einräumt. Wie genau die Zentralkomponenten auf die Europol-Daten zugreifen werden, ist derzeit noch Gegenstand von Abklärungen. Das Abfragerecht wird sich allerdings in den bestehenden Rechtsrahmen (Kooperationsabkommen zwischen der Schweiz und Europol) einordnen müssen. Es erscheint deshalb angezeigt, im Ausländer- und Integrationsgesetz vom 16. Dezember 2005[22] (AIG) und im Bundesgesetz vom 13. Juni 2008[23] über die polizeilichen Informationssysteme des Bundes (BPI) bereits die ESP-Zugriffsmöglichkeit auf die Europol-Datenbestände vorzusehen. Auf die vorher erwähnten Interpol-Datenbanken verfügt die Schweiz als Mitgliedstaat über einen Zugriff.

4.2 Stufenweise Anwendbarkeit der EU-Interoperabilitätsverordnungen

Die beiden EU-Interoperabilitätsverordnungen traten am 11. Juni 2019 in der EU in Kraft, anwendbar wird der überwiegende Teil der materiellen Bestimmungen allerdings erst später. So obliegt es der EU-Kommission über die gestaffelte Inbetriebnahme der einzelnen Zentralkomponenten zu entscheiden, womit die jeweils einschlägigen Bestimmungen erst dann anwendbar werden (vgl. Art. 79 der Verordnung «IOP Grenzen», Art. 75 der Verordnung «IOP Polizei»). Voraussetzung für die Inbetriebnahme der einzelnen Zentralkomponenten ist u.a. der erfolgreiche Abschluss eines umfassenden Tests der jeweiligen Zentralkomponente in Zusammenarbeit mit den Schengen-Staaten und den europäischen Agenturen. Zusätzlich müssen die technischen und rechtlichen Vorkehrungen für die Erhebung und Übermittlung von Daten getroffen worden sein (Art. 72 der Verordnung «IOP Grenzen», Art. 68 der Verordnung «IOP Polizei»). Die einzelnen Zentralkomponenten werden folglich zu unterschiedlichen Zeitpunkten operativ werden. Gemäss heutigem Zeitplan der EU-Kommission sollen der sBMS bis Ende 2021, der CIR bis Mitte 2022 und das ESP sowie der MID bis Mitte bzw. Ende 2023 in Betrieb genommen werden. Es sind ausserdem verschiedene Übergangsphasen geplant, bevor die einzelnen Zentralkomponenten zur Anwendung kommen werden.

21 SR **0.362.2**
22 SR **142.20**
23 SR **361**

Schliesslich ist in Artikel 79 der Verordnung «IOP Grenzen» resp. Artikel 75 der Verordnung «IOP Polizei» festgehalten, dass die Verordnungen für Eurodac erst ab dem Tag der Anwendbarkeit der Neufassung der Verordnung (EU) Nr. 603/2013[24] gelten werden. Die Einbindung von Eurodac im Rahmen der Interoperabilität ist aber vorgesehen, deshalb wird Eurodac auch in Kapitel 5 erwähnt. Konkrete Bestimmungen fehlen allerdings noch. Die diesbezügliche rechtliche Umsetzung in der Schweiz wird deshalb erst mit der Übernahme der revidierten Eurodac-Verordnung erfolgen.

5 Inhalt der EU-Verordnungen

Dieses Kapitel gibt einen Überblick über den Inhalt der beiden EU-Verordnungen. In Ziffer 5.1 liegt der Fokus auf den vier Zentralkomponenten. Weitere Neuerungen, die ebenfalls Auswirkungen auf die Schweiz haben, werden in Ziffer 5.2 aufgeführt. Dies sind beispielsweise Bestimmungen zur Auskunftsplicht oder zu Datenqualitätsanforderungen sowie zu Änderungen, die an anderen Rechtsakten vorgenommen werden.

Da die beiden EU-Verordnungen bis auf wenige Bestimmungen deckungsgleich sind, wird in Kapitel 5 auf eine getrennte Darstellung verzichtet und der Inhalt als Ganzes präsentiert. Die Kapitel- und Artikelnummern stimmen in beiden Texten grösstenteils überein. Erst ab Ende des achten Kapitels der EU-Verordnungen trifft dies nicht mehr zu, ein Verweis ist an entsprechender Stelle angebracht.

5.1 Die vier neuen Zentralkomponenten

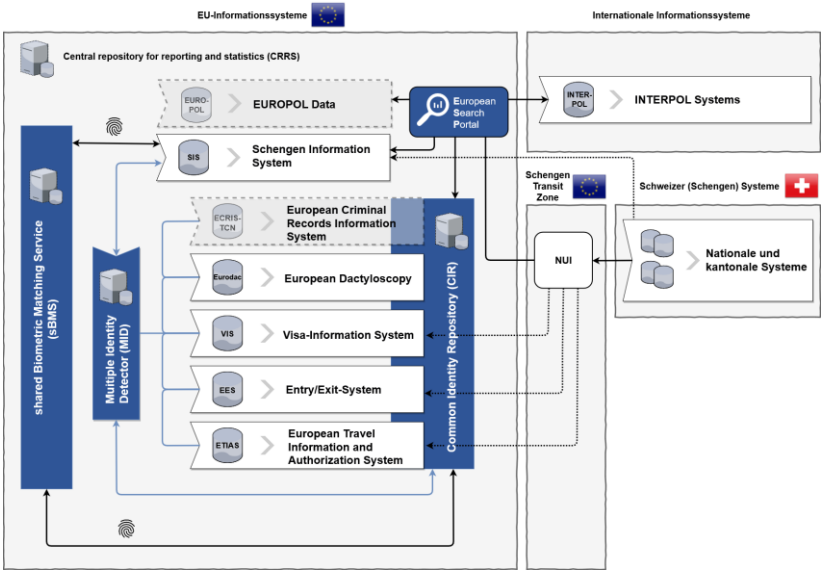
Die vier neuen Zentralkomponenten bilden das Herzstück der Interoperabilität. Dank ihnen sollen die verschiedenen EU-Informationssysteme gezielt miteinander kommunizieren. Der Informationsaustausch wird dadurch effizienter, bestehende Sicherheitslücken werden geschlossen. Die verschiedenen Zentralkomponenten unterstützen und ergänzen sich gegenseitig. Erst deren Kombination ermöglicht es, die Ziele der Interoperabilität vollständig zu erreichen.

Das ESP wird künftig Abfragen in mehreren EU-Informationssystemen gleichzeitig ermöglichen. Via ESP kann sowohl eine direkte Abfrage der Daten in den einzelnen Systemen (SIS, VIS, Eurodac, EES, ETIAS, ECRIS-TCN, Europol- und Interpol-

[24] Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, ABl. L 180 vom 29.6.2013, S. 1.

Datenbanken, s. Ziff. 4.1) erfolgen als auch eine Abfrage der Daten im CIR. Der MID dient dazu, zwischen den verschiedenen Systemen Mehrfachidentitäten aufzudecken. Dazu gleicht er die Daten im CIR mit denen im SIS ab. Für den Abgleich der biometrischen Daten nimmt der MID den sBMS zu Hilfe, während über das ESP der Abgleich mit Identitätsdaten und Daten zu den Reisedokumenten realisiert wird. Zusammen erleichtern die vier Zentralkomponenten daher nicht nur den Informationsaustausch und eine korrekte Identifizierung von Personen, sondern ermöglichen auch die Aufdeckung von Mehrfachidentitäten und Identitätsbetrug.

Die untenstehende Grafik zeigt, wie die Zentralkomponenten zusammenhängen und welche Systeme sie betreffen. Das NUI (National Uniform Interface) ist die Schnittstelle, welche eine standardisierte Verbindung zwischen den nationalen Systemen der Schengen-Staaten und den EU-Zentralkomponenten herstellt. Für das ETIAS, EES und VIS wird eine Verbindung zwischen den jeweiligen EU-Komponenten und den nationalen Komponenten ebenfalls über das NUI etabliert. In den folgenden Unterkapiteln wird jede Zentralkomponente der Interoperabilität einzeln vorgestellt.



5.1.1 Europäisches Suchportal (ESP) (Kapitel II)

Die Schaffung des ESP ist eine zentrale Funktion der Interoperabilität. Das ESP soll den zuständigen Behörden, nach Massgabe ihrer Zugangsrechte, einen raschen, unterbrechungsfreien, effizienten, systematischen und kontrollierten Zugang zu den verschiedenen EU-Informationssystemen, Europol- und Interpol-Datenbanken ermöglichen (Art. 6). Dank dem ESP sollen die zuständigen Behörden in Zukunft durch eine Abfrage auf alle für sie relevanten Informationen zugreifen und ein umfassendes Bild einer zu prüfenden Person erhalten können.

Nutzung des Europäischen Suchportals (Art. 7)

Das ESP dürfen alle nationalen Behörden und europäischen Agenturen nutzen, die auf mindestens eines der EU-Informationssysteme (EES, ETIAS, VIS, SIS, Eurodac, Europol-Datenbanken oder ECRIS-TCN), auf den CIR oder den MID oder Interpol-Datenbanken Zugriff haben. Künftig nutzen die zuständigen Behörden der Schengen-Staaten sowie die Stellen der EU das ESP für Abfragen im EES, VIS, ETIAS, in Eurodac oder im ECRIS-TCN sowie für Abfragen im CIR für die in den Artikeln 20–22 genannten Zwecke (für Abfragen im CIR s. ausführlich Ziff. 5.1.3). Sie können das ESP auch für Abfragen im zentralen SIS sowie von Europol- und Interpol-Datenbanken nutzen. Die Zugriffsrechte der jeweiligen Behörden auf die einzelnen Systeme bleiben unverändert.

Erstellung von ESP-Nutzerprofilen (Art. 8)

In Zusammenarbeit mit den Schengen-Staaten erstellt die Agentur eu-LISA Nutzerprofile für alle Kategorien von ESP-Nutzerinnen und -Nutzern. Jedes Profil enthält insbesondere die Informationen dazu, welche EU-Informationssysteme, Europol- und Interpol-Datenbanken abgefragt werden dürfen. Welche Behörde zu welchen Zwecken Zugriff auf die jeweiligen Informationssysteme hat, bestimmt sich nach Massgabe der für diese Systeme geltenden Rechtsgrundlagen. Die Nutzerprofile werden mindestens einmal pro Jahr von eu-LISA in Zusammenarbeit mit den Schengen-Staaten überprüft und falls erforderlich aktualisiert.

Abfragen (Art. 9)

Eine Abfrage über das ESP kann mittels Identitätsdaten, Daten zu den Reisedokumenten oder biometrischer Daten erfolgen. Das ESP fragt entsprechend der Nutzerprofile gleichzeitig alle relevanten Informationssysteme (EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, CIR sowie Europol- und Interpol-Datenbanken) ab. Sofern aus einem der Systeme Daten verfügbar sind, werden diese der Nutzerin oder dem Nutzer im Rahmen ihrer oder seiner Zugangsrechte über das ESP angezeigt. Dabei wird jeweils ersichtlich, aus welchem EU-Informationssystem die Daten stammen, ausser wenn es sich um eine Abfrage des CIR zu Identifikationszwecken gemäss Artikel 20 handelt. Bei diesen Abfragen geht es lediglich darum, eine Person zu identifizieren, die zuständigen Polizeibehörden sollen allerdings nicht erfahren, in welchem System die Daten der betroffenen Person erfasst sind (s. Ziff. 5.1.3 zu Art. 20). Bei Abfragen des CIR nach Artikel 22 zwecks Verhinderung, Aufdeckung oder Untersuchung terroristischer oder anderer schwerer Straftaten wird den Strafverfolgungsbehörden lediglich angezeigt, ob Daten in einem Informationssystem vorhanden sind. Die jeweiligen Daten selbst werden jedoch nicht angezeigt. Der Zugang zu den entsprechenden Daten muss separat beantragt werden (s. Ziff. 5.1.3 zu Art. 22). Bei Abfragen in den Interpol-Datenbanken über das ESP wird der ausschreibende Staat nicht informiert.

Führen von Protokollen (Art. 10)

Sowohl eu-LISA als auch die Schengen-Staaten haben über die Abfragen via ESP Protokoll zu führen. Die Schengen-Staaten protokollieren die Nutzung des ESP bis auf die Stufe der Mitarbeitenden. Die Protokolle dürfen ausschliesslich zur datenschutzrechtlichen Kontrolle verwendet werden. Sie sollen vor unbefugten Zugriffen geschützt werden und ein Jahr nach Erstellung gelöscht werden, es sei denn, sie werden für ein bereits eingeleitetes Kontrollverfahren benötigt.

Ausweichverfahren für den Fall, dass eine Nutzung des Europäischen Suchportals technisch nicht möglich ist (Art. 11)

Artikel 11 regelt das Vorgehen für den Fall, dass das ESP aus technischen Gründen nicht genutzt werden kann. Ist dies aufgrund eines Ausfalls des ESP nicht möglich, informiert eu-LISA die Nutzerinnen und Nutzer automatisch. Besteht ein Problem bei der nationalen Infrastruktur eines Schengen-Staates, so informiert dieser automatisch eu-LISA und die EU-Kommission. Bis die technischen Probleme behoben sind, können die EU-Informationssysteme oder der CIR direkt abgefragt werden.

Übergangszeitraum für die Nutzung des Europäischen Suchportals

In Artikel 67 der Verordnung «IOP Grenzen» resp. Artikel 63 der Verordnung «IOP Polizei» ist geregelt, dass die Nutzung des ESP innert der ersten beiden Jahre ab Inbetriebnahme der Zentralkomponente fakultativ ist. Diese Frist kann einmal um ein weiteres Jahr verlängert werden.

5.1.2 Gemeinsamer Dienst für den Abgleich biometrischer Daten (sBMS) (Kapitel III)

Der sBMS soll die systemübergreifende Abfrage mehrerer EU-Informationssysteme anhand biometrischer Daten ermöglichen (Art. 12). In den EU-Verordnungen wird die Abkürzung «BMS» benutzt, die im Schweizer Recht jedoch bereits anderweitig angewandt wird. Um Verwechslungen zu vermeiden, wird «sBMS» verwendet.

Speicherung biometrischer Templates im gemeinsamen Dienst für den Abgleich biometrischer Daten (Art. 13)

Der sBMS speichert die biometrischen Templates, die er aus den biometrischen Daten des EES, VIS, SIS und des ECRIS-TCN sowie in Zukunft von Eurodac generiert. Bei den Templates handelt sich um eine mathematische Repräsentation, die mittels Merkmalsauszug aus biometrischen Daten generiert wird und die auf die für Identifizierungs- und Verifizierungszwecke erforderlichen Merkmale begrenzt sind (Art. 4 Abs. 12). Das ETIAS ist nicht betroffen, da es keine biometrischen Daten enthält. Jedes Template enthält einen Verweis auf das EU-Informationssystem, aus dem es stammt, sowie einen Verweis auf die darin enthaltenen Datensätze. Nur Templates biometrischer Daten, die punkto Datenqualität einen Mindeststandard erfüllen, dürfen in den sBMS eingegeben werden.

Abfrage biometrischer Daten mithilfe des gemeinsamen Dienstes für den Abgleich biometrischer Daten (Art. 14)

Die Abfrage biometrischer Daten im CIR und im SIS erfolgt über die biometrischen Templates im sBMS und ist nur zu den vorgesehenen Zwecken erlaubt.

Speicherdauer für Daten im gemeinsamen Dienst für den Abgleich biometrischer Daten (Art. 15)

Die Templates und die Verweise auf die EU-Informationssysteme, aus denen sie stammen, werden nur so lange im sBMS gespeichert, wie die biometrischen Daten im CIR (aus dem VIS, dem EES, dem ETIAS, Eurodac und dem ECRIS-TCN) oder im SIS vorhanden sind, und werden danach automatisch gelöscht.

Führen von Protokollen (Art. 16)

Sowohl eu-LISA als auch die Schengen-Staaten haben über die Datenverarbeitungsvorgänge Protokoll zu führen. Die Bestimmungen zur Verwendung der Protokolle und der zu treffenden Sicherheitsmassnahmen, die in Ziffer 5.1.1 zu Artikel 10 aufgeführt sind, gelten analog.

5.1.3 Gemeinsamer Speicher für Identitätsdaten (CIR) (Kapitel IV)

Im gemeinsamen Speicher für Identitätsdaten («CIR») wird für jede im EES, VIS, ETIAS, in Eurodac oder im ECRIS-TCN erfasste Person eine individuelle Datei angelegt. Der CIR stellt damit einen Bestandteil dieser Systeme dar. Die Daten bleiben weiterhin im jeweiligen System erfasst. Dies soll die korrekte Identifizierung von Personen, die in einem der genannten EU-Informationssysteme erfasst sind, erleichtern. Mit dem CIR wird u.a. der Zugang von Strafverfolgungsbehörden zu EU-Informationssystemen, die nicht der Strafverfolgung dienen, für die Verhütung, Aufdeckung oder Ermittlung terroristischer und anderer schwerer Straftaten vereinheitlicht und erleichtert (Art. 17 mit Verweis auf Art. 22). Aufgrund der komplexen technischen Architektur des SIS sind die Daten des SIS nicht Teil des CIR.

Im gemeinsamen Speicher für Identitätsdaten gespeicherte Daten (Art. 18)

Der CIR speichert die Identitätsdaten sowie, falls vorhanden, Daten zu den Reisedokumenten und die biometrischen Daten aus dem EES, VIS, ETIAS, ECRIS-TCN und Eurodac. Die Speicherung erfolgt dabei logisch voneinander getrennt und nach den Informationssystemen, aus welchen die Daten stammen. Für jeden im CIR gespeicherten Datensatz wird auch ein Verweis auf das EU-Informationssystem, aus dem er stammt, hinterlegt («tatsächliche Datensätze», gemäss der EU-Terminologie). Die Zugriffsrechte der Behörden auf den CIR richten sich dabei nach den Rechtsgrundlagen der jeweiligen EU-Informationssysteme sowie nach den in den EU-Interoperabilitätsverordnungen festgelegten Zugriffsrechten für die Zwecke nach den Artikeln 20–22.

Hinzufügung, Änderung und Löschung von Daten im gemeinsamen Speicher für Identitätsdaten (Art. 19)

Die im CIR gespeicherten Daten werden automatisch angepasst, sobald Daten im EES, VIS, ETIAS oder ECRIS-TCN und in Zukunft in Eurodac hinzugefügt, geändert oder gelöscht werden. Wenn eine weisse oder eine rote MID-Verknüpfung (für Details dazu s. Ziff. 5.1.4) erstellt wird, die Daten aus dem CIR betrifft, werden keine neuen Dateien angelegt, sondern die neuen Daten werden der bestehenden individuellen Datei der verknüpften Daten hinzugefügt.

Zugang zum gemeinsamen Speicher für Identitätsdaten zwecks Identifizierung (Art. 20)

Der CIR soll die Identifizierung von Drittstaatsangehörigen erleichtern. Artikel 20 sieht deshalb vor, dass Polizeibeamtinnen und Polizeibeamte bei Kontrollen innerhalb eines Landes unter bestimmten Bedingungen zwecks Identifikation den CIR über das ESP abfragen dürfen. Absatz 1 listet die Fälle, in denen dies möglich ist, auf: a) Eine Person kann wegen Fehlens eines Reisedokuments oder eines anderen glaubwürdigen Dokuments zum Nachweis der Identität nicht identifiziert werden. b) Es bestehen Zweifel an den gemachten Identitätsangaben. c) Es bestehen Zweifel an der Echtheit des vorgelegten Reisedokuments oder anderen Dokuments. d) Es bestehen Zweifel an der Identität der Inhaberin oder des Inhabers des Reisedokuments oder anderen Dokuments. e) Eine Person kann oder will bei der Identifizierung nicht kooperieren. Eine Abfrage des CIR zwecks Identifizierung ist bei Minderjährigen unter 12 Jahren nur zum Wohle des Kindes erlaubt.

Normalerweise erfolgt die Abfrage des CIR mittels der bei einer Identitätskontrolle direkt vor Ort abgenommenen biometrischen Daten der Person (Abs. 2). Wenn die biometrischen Daten nicht verwendet werden können oder die Abfrage damit erfolglos ist, wird die Abfrage mit den Identitätsdaten der Person in Verbindung mit den Daten zu den Reisedokumenten durchgeführt. Sofern im CIR Daten zu der betroffenen Person vorhanden sind, darf die Polizeibehörde diese konsultieren, ohne dass jedoch ersichtlich wird, aus welchem EU-Informationssystem die Daten stammen. In Absatz 4 ist vorgesehen, dass die Daten im CIR für die Identifizierung von Opfern terroristischer Anschläge, von Unfällen oder Naturkatastrophen sowie nichtidentifizierter menschlicher Überreste verwendet werden können. Schengen-Staaten, die diese beiden neuen Möglichkeiten nutzen wollen, müssen ihre nationalen Gesetze entsprechend anpassen und bestimmen, welche Behörden zur Abfrage berechtigt sind.

Zugang zum gemeinsamen Speicher für Identitätsdaten zwecks Aufdeckung etwaiger Mehrfachidentitäten (Art. 21)

Zugang zum CIR ist auch im Zusammenhang mit MID-Verknüpfungen vorgesehen (für Details dazu s. Ziff. 5.1.4). Zur Verifizierung unterschiedlicher Identitäten bei gelben Verknüpfungen und zur Bekämpfung von Identitätsbetrug bei roten Verknüpfungen dürfen die jeweils zuständigen Behörden auf die verknüpften Daten im CIR zugreifen.

Abfrage des gemeinsamen Speichers für Identitätsdaten zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten (Art. 22)

Die für die Verhütung, Aufdeckung oder Untersuchung von terroristischen oder sonstigen schweren Straftaten zuständigen Behörden (sogenannte «benannte Behörden»), die von jedem Land entsprechend der Rechtsgrundlagen der einzelnen Systeme definiert werden, verfügen nicht unbedingt über einen direkten Zugriff auf die Daten im EES, VIS, ETIAS oder in Eurodac, sondern müssen diese jeweils bei einer ebenfalls im Landesrecht definierten zentralen Zugangsstelle beantragen.

Mit der Interoperabilität wird der Zugang der benannten Behörden auf Daten in diesen Systemen neu geregelt. Konkret ist ein zweistufiges Verfahren via Abfrage im CIR vorgesehen. Sofern hinreichende Gründe vorliegen, dass die Abfrage der EU-Informationssysteme zur Verhütung, Aufdeckung oder Ermittlung von schweren Straftaten und Terrorismus beiträgt, insbesondere wenn der Verdacht besteht, dass eine Person in einem der Systeme erfasst ist, dürfen die benannten Behörden und Europol den CIR abfragen. Dieser erste Schritt erfolgt gemäss dem «Treffer/kein Treffer»-Verfahren. Liegt ein Treffer vor (sprich, sind Daten zu einer Person in einem der Systeme EES, ETIAS, VIS oder Eurodac vorhanden), so meldet der CIR der abfragenden Behörde, in welchem EU-Informationssystem Daten vorhanden sind. Anschliessend hat diese – wie bisher – die Möglichkeit, Gesuch auf uneingeschränkten Zugang zu mindestens einem der vom Treffer betroffenen EU-Informationssysteme zu stellen. Die Gewährung des vollständigen Zugangs auf die betroffenen Daten aus dem EES, ETIAS, VIS oder Eurodac unterliegt dabei weiterhin den Voraussetzungen und Verfahren, die in den Rechtsgrundlagen der zugrundeliegenden Informationssysteme festgelegt sind. Wird ausnahmsweise kein Zugang verlangt, so ist dies schriftlich zu begründen und zu protokollieren.

Datenspeicherung im gemeinsamen Speicher für Identitätsdaten (Art. 23)

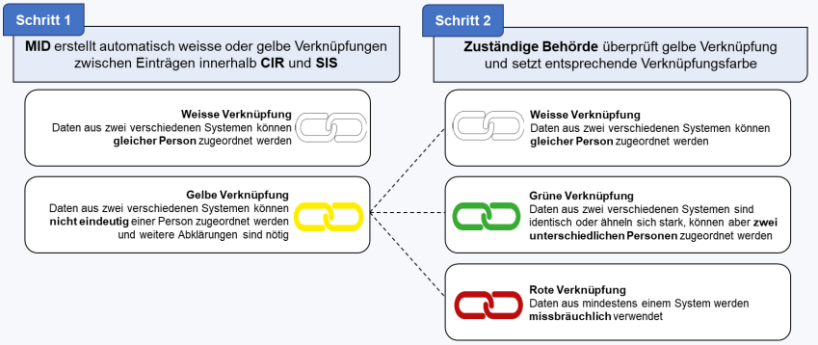
Die Daten im CIR werden nach Massgabe der Datenspeicherungsbestimmungen des jeweiligen EU-Informationssystems, aus dem sie stammen, automatisch gelöscht. Die individuellen Dateien im CIR werden nur so lange gespeichert, wie die entsprechenden Daten in mindestens einem der EU-Informationssysteme gespeichert sind.

Führen von Protokollen (Art. 24)

eu-LISA führt Protokoll über sämtliche Datenverarbeitungsvorgänge und Abfragen im CIR. Die Schengen-Staaten haben Protokoll über die Abfragen des CIR nach den Artikeln 20–22 zu führen, Europol über die Zugriffe nach den Artikeln 21 und 22. Die Bestimmungen zur Verwendung der Protokolle und der zu treffenden Sicherheitsmassnahmen, die in Ziffer 5.1.1 zu Artikel 10 aufgeführt sind, gelten analog.

5.1.4 Detektor für Mehrfachidentitäten (MID) (Kapitel V)

Der MID ist die vierte Zentralkomponente. Er soll dazu beitragen, Personen zu erkennen, die mehrere oder falsche Identitäten benutzen mit dem doppelten Ziel, Identitätsprüfungen zu vereinfachen und Identitätsbetrug zu bekämpfen. Dazu werden im MID Identitätsbestätigungsdateien erstellt und gespeichert, die Verknüpfungen von Daten aus den verschiedenen EU-Informationssystemen enthalten (Art. 25). Konkret wird jeweils geprüft, ob die in einem System neu erfassten Personendaten, Daten zu den Reisedokumenten oder biometrischen Daten auch in anderen Systemen vorhanden sind. Je nach Konstellation werden vom MID automatisch weisse oder gelbe Verknüpfungen erstellt. Alle gelben Verknüpfungen müssen durch die zuständigen Behörden manuell verifiziert werden. Diese müssen die verschiedenen Identitäten prüfen und, je nachdem ob es sich um dieselbe oder eine andere Person handelt, die Verknüpfung auf Rot, Grün oder Weiss setzen. Die untenstehende Grafik gibt einen ersten Überblick über diese Prozesse. Die genauen Verfahren und die Bedeutung der Verknüpfungen werden im Folgenden detailliert ausgeführt und am Ende des Kapitels anhand dreier Beispiele illustriert.



Zugriff auf den Detektor für Mehrfachidentitäten (Art. 26)

Artikel 26 regelt, wer für welche Zwecke auf die im MID gespeicherten Daten zugreifen darf. Einerseits erhalten die für die manuelle Verifizierung verschiedener Identitäten zuständigen Behörden gemäss Artikel 29 Zugriff. Dies sind die Behörden, die Daten im EES, VIS, ETIAS, ECRIS-TCN, SIS und in Eurodac erfassen oder aktualisieren. Sie sind in den jeweiligen Rechtsgrundlagen der Informationssysteme definiert. Andererseits erhalten die Behörden der Schengen-Staaten und die Agenturen der EU (hier Europol und die Europäische Grenz- und Küstenwache), über den MID Zugriff auf rote Verknüpfungen, wenn sie auf mindestens eines der betroffenen EU-Informationssysteme Zugriff haben. Zugriffe auf weisse oder grüne Verknüpfungen sind möglich, wenn die Behörden auf beide EU-Informationssysteme Zugriff haben, zwischen deren Daten eine Verknüpfung besteht.

Prüfung auf Mehrfachidentitäten (Art. 27)

Artikel 27 beschreibt, wie die Prüfung auf Mehrfachidentitäten ablaufen wird. Eine solche Prüfung wird bei jeder Erfassung oder Aktualisierung von Daten in einem der EU-Informationssysteme (VIS, SIS, ETIAS, EES) ausgelöst. Dazu werden jeweils die neuen Daten mit jenen, die bereits im CIR und im SIS vorhandenen sind, verglichen. Dabei dient der sBMS zum Abgleich der biometrischen Daten und das ESP zum Abgleich der Identitätsdaten und der Daten zu den Reisedokumenten. Eine Prüfung auf Mehrfachidentitäten erfolgt nur, um Daten zwischen den verschiedenen EU-Informationssystemen abzugleichen.

Ergebnisse der Prüfung auf Mehrfachidentitäten (Art. 28)

Die möglichen Ergebnisse einer Prüfung auf Mehrfachidentitäten und die darauffolgenden Verfahren sind in Artikel 28 beschrieben. Ergibt die Prüfung auf Mehrfachidentitäten keine Überstimmung mit Daten anderer EU-Informationssysteme, dann erfolgt die Erfassung von Daten wie in den einschlägigen Rechtsgrundlagen vorgesehen. Ergibt die Überprüfung eine oder mehrere Übereinstimmungen, werden Verknüpfungen zwischen den für die Abfrage verwendeten neuen oder aktualisierten Daten und den bereits in einem anderen EU-Informationssystem vorhandenen Daten erstellt. Falls es mehrere Übereinstimmungen gibt, wird eine Verknüpfung zwischen allen betroffenen Daten erstellt. Sind die Daten bereits verknüpft, so wird die bestehende Verknüpfung auf die neuen Daten ausgeweitet.

Sind die Identitätsdaten der verknüpften Dateien gleich oder ähnlich, wird automatisch eine weisse Verknüpfung erstellt. Können die Identitätsdaten hingegen nicht als ähnlich angesehen werden, wird automatisch eine gelbe Verknüpfung erstellt und eine manuelle Verifizierung durch die zuständigen Behörden wird nötig. Die Kriterien, wann Identitätsdaten als gleich oder ähnlich angesehen werden, werden von der EU-Kommission definiert und in einem delegierten Rechtsakt festgehalten, den die Schweiz als Weiterentwicklung des Schengen-Besitzstands übernehmen werden muss. Alle Verknüpfungen werden in der Identitätsbestätigungsdatei nach Artikel 34 gespeichert.

Manuelle Verifizierung verschiedener Identitäten und zuständige Behörden (Art. 29)

Wird bei der Prüfung auf Mehrfachidentitäten durch den MID eine gelbe Verknüpfung erstellt, so müssen die verschiedenen Identitäten manuell überprüft werden. Zuständig für diese Verifizierung ist diejenige Behörde, die Daten in einem der EU-Informationssysteme erfasst oder aktualisiert.

Absatz 2 definiert eine Ausnahme von dieser generellen Regelung. Wenn eine Verknüpfung mit einer SIS-Ausschreibung gemäss Artikel 26, 32, 34 oder 36 der

Verordnung (EU) 2018/1862[25] geprüft werden muss, ist das SIRENE-Büro des Schengen-Staates, der die Ausschreibung eingegeben hat, für die manuelle Verifizierung zuständig. Dabei handelt es sich um folgende Ausschreibungskategorien: Ausschreibung zwecks Verhaftung zum Zweck der Auslieferung (Art. 26); Vermisste Personen (Art. 32); Aufenthaltsnachforschung (Art. 34); verdeckte Registrierung, Ermittlungsanfrage oder gezielte Kontrollen (Art. 36). Mit Ausnahme von Einreiseverboten und Rückkehrentscheiden ist das SIRENE-Büro also für alle Personenfahndungen zuständig. Der MID verweist in der Identitätsbestätigungsdatei auf die jeweils zuständige Behörde.

Die Prüfung soll unverzüglich erfolgen. Sobald sie abgeschlossen ist, aktualisiert die zuständige Behörde die Verknüpfung gemäss den Artikeln 31–33 auf Grün, Rot oder Weiss. Die Verknüpfung gilt sodann als verifiziert. Absatz 4 der Verordnung «IOP Grenzen» enthält zusätzliche Bestimmungen für die Prüfung, welche aufgrund einer Anlegung oder Aktualisierung eines Dossiers im EES nötig wird. So muss die Verifizierung im Beisein der betroffenen Person eingeleitet werden, welche die Möglichkeit erhält, sich zu den Umständen zu äussern. Erfolgt die manuelle Verifizierung an der Schengen-Aussengrenze, hat der ganze Prozess möglichst innerhalb von 12 Stunden zu erfolgen.

Werden mehrere Verknüpfungen erstellt, so sind diese einzeln zu prüfen. Die zuständigen Behörden sollen bei der Beurteilung, ob eine neue Verknüpfung erstellt werden muss, jeweils berücksichtigen, ob Daten, die zu einer Übereinstimmung geführt haben, bereits verknüpft sind.

Gelbe Verknüpfung (Art. 30)

Gelb sind jene Verknüpfungen, bei denen die Prüfung auf Mehrfachidentitäten Unklarheiten ergeben hat, die noch nicht manuell überprüft worden sind. Dies ist beispielsweise der Fall, wenn die verknüpften Daten dieselben Identitätsdaten, aber unterschiedliche biometrische Daten enthalten oder wenn die Identitätsdaten unterschiedlich sind, die biometrischen Daten aber übereinstimmen. Letzteres ist beispielsweise im Falle einer Heirat mit Namenswechsel vorstellbar. Bei einer gelben Verknüpfung wird in jedem Fall eine manuelle Verifizierung gemäss Artikel 29 durch die jeweils zuständigen Behörden nötig.

Grüne Verknüpfung (Art. 31)

Eine grüne Verknüpfung wird immer erst nach erfolgter manueller Verifizierung erstellt. Sie zeigt an, dass die Identitätsdaten der verknüpften Daten nicht zu dersel-

25 Verordnung (EU). 2018/1862 des europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission, ABl. L 312 vom 7.12.2018, S. 56; zuletzt geändert durch Verordnung (EU) 2019/817, ABl. L 135 vom 22.5.2019, S. 27.

ben Person gehören. Dies kann beispielsweise der Fall sein, wenn die verknüpften Daten unterschiedliche biometrische Daten, aber dieselben Identitätsdaten enthalten, weil zwei Personen zufällig gleich heissen und dasselbe Geburtsdatum haben. Damit wird die Identitätskontrolle für die betroffenen rechtmässig reisenden Personen künftig erleichtert.

Wenn einer Behörde eines Schengen-Staates Hinweise vorliegen, dass eine grüne Verknüpfung unrichtig erfasst wurde, nicht aktuell ist oder Daten in Umgehung der EU-Interoperabilitätsverordnungen bearbeitet wurden, muss sie die betreffenden Daten überprüfen und die Verknüpfung, falls nötig, berichtigen oder löschen. Die ursprünglich für die manuelle Verifizierung der verschiedenen Identitäten zuständige Behörde muss unverzüglich informiert werden.

Rote Verknüpfung (Art. 32)

Eine rote Verknüpfung wird immer erst nach erfolgter manueller Verifizierung erstellt. Sie zeigt an, dass unrechtmässige Mehrfachidentitäten oder Identitätsbetrug vorliegen. Unterschiedliche Konstellationen führen zu einer roten Verknüpfung:

– Eine Person verwendet mehrere unterschiedliche Identitäten: In diesem Fall sind dieselben biometrischen Daten resp. dieselben Daten aus Reisedokumenten mit unterschiedlichen Identitätsdaten in verschiedenen EU-Informationssystemen verzeichnet, sie beziehen sich jedoch auf ein und dieselbe Person.

– Eine Person verwendet das Reisedokument einer anderen: Die verknüpften Daten enthalten in diesem Fall unterschiedliche biometrische Daten, aber dieselben Reisedokumentdaten, sie beziehen sich also auf zwei verschiedene Personen.

– Eine Person gibt sich als jemand anderes aus: In diesem Fall sind unterschiedliche biometrische Daten mit denselben Identitätsdaten in verschiedenen EU-Informationssystemen verzeichnet. Die verknüpften Daten beziehen sich also auf zwei verschiedene Personen.

Eine rote Verknüpfung alleine hat für die betroffene Person keine Konsequenzen. Allfällige Massnahmen sind nur gestützt auf EU-Recht oder das nationale Recht möglich. Wird eine rote Verknüpfung zwischen Daten im EES, ETIAS, VIS, in Eurodac oder im ECRIS-TCN erstellt, wird die entsprechende individuelle Datei im CIR aktualisiert.

Sobald eine rote Verknüpfung erstellt wird, informiert die für die manuelle Verifizierung zuständige Behörde die betroffene Person mittels Standardformular, dass illegale Mehrfachidentitäten vorliegen, und teilt ihr mit, wie und wo sie Informationen zu den Daten erhält; dafür wird ihr die einmalige Kennnummer und die Adresse des Webportals (s. Ziff. 5.2, Datenschutz) mitgeteilt. Die Behörde kann auf eine Information der Person verzichten, wenn dies zur Wahrung der Bestimmungen für die Handhabung von Ausschreibungen im SIS, zum Schutze der Sicherheit und öffentlichen Ordnung, zur Verhinderung von Kriminalität oder um sicherzustellen, dass keine nationalen Ermittlungen beeinträchtigt werden, nötig ist (Abs. 4 und 5).

Jedes Mal, wenn eine rote Verknüpfung erstellt wird, werden die Behörden, welche für die verknüpften Daten zuständig sind, automatisch vom MID informiert.

Wenn einer Behörde eines Schengen-Staates Hinweise vorliegen, dass eine rote Verknüpfung falsch erfasst wurde oder Daten in Umgehung der EU-Interoperabilitätsverordnungen bearbeitet wurden, muss sie in den meisten Fällen die betreffenden Daten überprüfen und die Verknüpfung, falls nötig, berichtigen oder löschen. Handelt es sich hingegen um eine Verknüpfung auf eine SIS-Ausschreibung gemäss Artikel 26, 32, 34 oder 36 der Verordnung (EU) 2018/1862, muss sie umgehend das zuständige SIRENE-Büro des Schengen-Staates, der die Ausschreibung erfasst hat, informieren. In diesem Fall übernimmt das SIRENE-Büro die Verifizierung und berichtigt oder löscht gegebenenfalls die Verknüpfung. Die Behörde, welche die Hinweise auf falsche Verknüpfungen erhalten hat, informiert in jedem Fall unverzüglich die für die manuelle Verifizierung der verschiedenen Identitäten zuständige Behörde über jegliche Berichtigung oder Löschung der roten Verknüpfung.

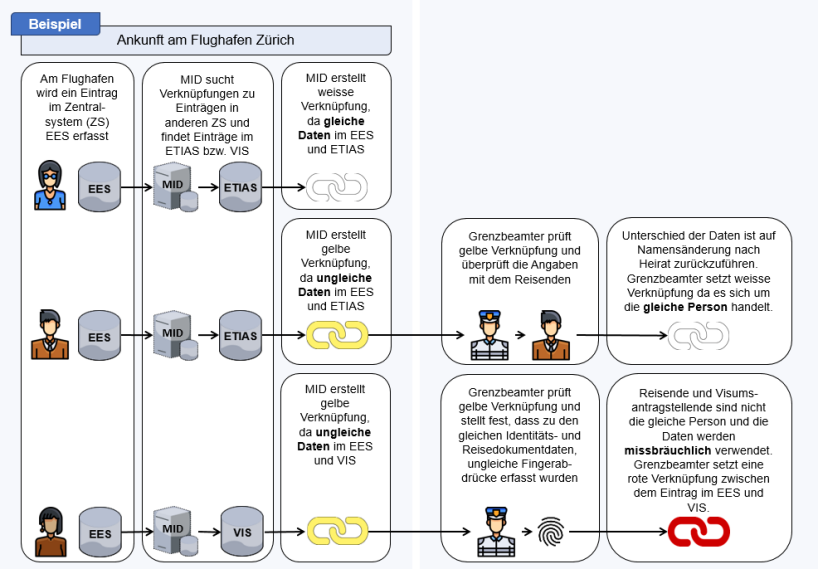
Weisse Verknüpfung (Art. 33)

Eine weisse Verknüpfung entsteht entweder automatisch bei der Prüfung auf Mehrfachidentitäten durch den MID gemäss Artikel 27 (wenn zum Beispiel die Identitätsdaten und die biometrischen Daten in den verknüpften Daten übereinstimmen) oder als Resultat der manuellen Verifizierung gemäss Artikel 29 (wenn die biometrischen Daten identisch sind, die Identitätsdaten aber ähnlich oder unterschiedlich sind und die für die Verifizierung zuständige Behörde feststellt, dass es sich um dieselbe Person handelt). Eine weisse Verknüpfung zeigt demnach an, dass es sich bei den verknüpften Daten um ein und dieselbe Person handelt, diese also schon in mindestens einem anderen EU-Informationssystem verzeichnet ist. Damit wird die Mobilität für Personen, die beispielsweise rechtmässig mehrere gültige Reisedokumente besitzen, vereinfacht. Wird eine weisse Verknüpfung zwischen Daten im EES, ETIAS, VIS, in Eurodac oder im ECRIS-TCN erstellt, wird die entsprechende individuelle Datei im CIR aktualisiert.

Wenn eine weisse Verknüpfung als Resultat der Verifizierung durch die zuständige Behörde erstellt wird, informiert diese die betroffene Person mittels Standardformular, dass ähnliche oder unterschiedliche Identitätsdaten vorliegen, und teilt ihr mit, wie sie Informationen zu den Daten erhält. Wie bei einer roten Verknüpfung kann die Behörde darauf verzichten, die Person zu informieren, wenn dies aus Sicherheitsgründen nötig ist.

Wenn einer Behörde eines Schengen-Staates Hinweise vorliegen, dass eine weisse Verknüpfung unrichtig erfasst wurde, nicht aktuell ist oder Daten in Umgehung der EU-Interoperabilitätsverordnungen bearbeitet wurden, muss sie die betreffenden Daten überprüfen und die Verknüpfung falls nötig berichtigen oder löschen. Die ursprünglich für die manuelle Verifizierung der verschiedenen Identitäten zuständige Behörde muss unverzüglich informiert werden.

Die folgenden drei Beispiele veranschaulichen die Funktionsweise des MID und die Bedeutung der verschiedenen Verknüpfungen.



Die Resultate der manuellen Verifizierung werden in der Identitätsbestätigungsdatei gespeichert.

Identitätsbestätigungsdatei (Art. 34)

Im MID werden ausschliesslich Identitätsbestätigungsdateien gespeichert. Nebst der Art der Verknüpfung (Art. 30–33) wird darin auch angegeben, in welchen EU-Informationssystemen die verknüpften Dateien gespeichert sind. Jede Identitätsbestätigungsdatei enthält eine einmalige Kennnummer, die das Abrufen der verknüpften Daten aus den entsprechenden EU-Informationssystemen ermöglicht. Auch die für die manuelle Verifizierung zuständige Behörde sowie das Datum, an dem die Verknüpfung erstellt oder aktualisiert wurde, werden gespeichert.

Datenspeicherung im Detektor für Mehrfachidentitäten (Art. 35)

Die Identitätsbestätigungsdateien und die darin enthaltenen Daten, einschliesslich der Verknüpfungen, werden nur so lange im MID gespeichert, wie die verknüpften Daten in mehreren der zugrundeliegenden EU-Informationssysteme vorhanden sind. Anschliessend werden sie automatisch gelöscht.

Führen von Protokollen (Art. 36)

Sowohl eu-LISA als auch die Schengen-Staaten haben über die Datenverarbeitungsvorgänge und Abfragen im MID Protokoll zu führen. Die Bestimmungen zur Verwendung der Protokolle und der zu treffenden Sicherheitsmassnahmen, die in Ziffer 5.1.1 zu Artikel 10 aufgeführt sind, gelten analog.

Übergangszeitraum für die Prüfung auf Mehrfachidentitäten

In Artikel 69 der Verordnung «IOP Grenzen» resp. Artikel 65 der Verordnung «IOP Polizei» ist der Übergangszeitraum für die Prüfung auf Mehrfachidentitäten geregelt. Nachdem der MID fertig entwickelt und erfolgreich getestet wurde, und bevor er in Betrieb genommen wird, sollen alle bereits im EES, VIS, in Eurodac und im SIS vorhandenen Daten auf Mehrfachidentitäten geprüft werden. Diese Prüfung erfolgt ausschliesslich anhand biometrischer Daten. Zuständig für diese Verifizierung ist die ETIAS-Zentralstelle. Sofern eine gelbe Verknüpfung zu einer SIS-Ausschreibung gemäss Artikel 26, 32, 34 oder 36 der Verordnung (EU) 2018/1862 erstellt wird, wird das zuständige SIRENE-Büro in die Verifizierung miteinbezogen. Erst wenn alle gelben Verknüpfungen geprüft und aktualisiert wurden, informiert die ETIAS-Zentralstelle die EU-Kommission, die danach den Zeitpunkt der effektiven Inbetriebnahme des MID festlegt. Die Prüfung sollte innerhalb eines Jahres abgeschlossen sein, eine Fristverlängerung ist möglich.

5.2 Weitere Bestimmungen

Die zwei EU-Verordnungen enthalten, neben den Bestimmungen zu den vier neuen Zentralkomponenten, zahlreiche weitere Bestimmungen. Deren Inhalt wird im Folgenden zusammengefasst dargestellt. Dabei ist zu beachten, dass verschiedene der erwähnten Bestimmungen in der Schweiz erst auf Verordnungsstufe umzusetzen sein werden oder gar keiner Umsetzung im schweizerischen Recht bedürfen.

Massnahmen zur Unterstützung der Interoperabilität (Kapitel VI)

Um die Interoperabilität der verschiedenen EU-Informationssysteme zu ermöglichen, sind folgende unterstützende Massnahmen geplant:

Artikel 37 enthält Bestimmungen über die Datenqualitätsanforderungen. Einerseits sind Verfahren für die automatische Datenqualitätskontrolle vorgesehen, andererseits werden Mindeststandards eingeführt, die für die Eingabe von Daten in die EU-Informationssysteme und die Zentralkomponenten erfüllt sein müssen. Mit dem universellen Nachrichtenformat (*Universal Message Format*) wird ein gemeinsamer Standard für den grenzüberschreitenden Informationsaustausch eingeführt (Art. 38). Dieser Standard soll beim EES, ETIAS, bei Eurodac, beim ECRIS-TCN, ESP, CIR und MID verwendet werden und könnte auch von zukünftigen Informationssystemen genutzt werden. Für Analyse- und Statistikzwecke wird ein zentraler Speicher für Berichte und Statistiken (*Central Repository for Reporting and Statistics*) aufgebaut (Art. 39). Dieser soll systemübergreifende statistische Daten bereitstellen. Die

Daten werden dazu anonymisiert, damit die Identifizierung von Einzelpersonen nicht möglich ist.

Datenschutz (Kapitel VII)

Das Kapitel VII ist dem Datenschutz gewidmet. Es werden einerseits die für die Verarbeitung von Daten verantwortlichen Stellen genannt (Art. 40), andererseits jene, die für die Sicherheit der Datenverarbeitung zuständig sind (Art. 42). eu-LISA kommt hier eine besondere Bedeutung zu, da die Agentur für die Sicherheit der Zentralkomponenten und der Kommunikationsinfrastruktur zuständig ist und beispielsweise für die Wiederherstellung des Normalbetriebs im Störungsfall sorgen muss.

Die Schengen-Staaten haben Massnahmen zur Überwachung der Einhaltung der EU-Interoperabilitätsverordnungen zu treffen (Art. 44). Artikel 45 verpflichtet die Schengen-Staaten dazu, Sanktionen für den Missbrauch von Daten sowie die unrechtmässige Verarbeitung oder den unrechtmässigen Austausch von Daten vorzusehen. Die Sanktionen sollen wirksam, verhältnismässig und abschreckend sein. In Artikel 46 ist die Haftung im Schadensfall geregelt. Grundsätzlich hat jede Person, der durch rechtswidrige Datenverarbeitung oder andere gegen die Verordnung verstossende Handlungen ein Schaden entstanden ist, das Recht, Schadenersatz zu verlangen. Die verantwortliche Stelle wird von der Haftung befreit, wenn sie nachweislich nicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Führt eine Pflichtverletzung eines Schengen-Staates zu einem Schaden an den Zentralkomponenten, ist er ebenfalls haftbar, soweit von eu-LISA oder einem anderen Schengen-Staat angemessene Massnahmen zur Verhütung oder Verringerung des Schadens ergriffen wurden.

Das Recht auf Information bezüglich im sBMS, CIR oder MID gespeicherter Daten ist in Artikel 47 geregelt. Werden personenbezogene Daten erfasst, die im sBMS, CIR oder MID gespeichert werden, so muss die betroffene Person in einfacher und ihr verständlicher Sprache informiert werden.

Artikel 48 regelt das Recht auf Auskunft, Berichtigung und Löschung von im MID gespeicherten Daten. Verlangt eine Person Auskunft darüber, ob sie betreffende personenbezogene Daten verarbeitet werden, oder strebt sie deren Berichtigung, Löschung oder Einschränkung der Verarbeitung an, kann sie sich an die zuständige Behörde eines beliebigen Schengen-Staates wenden, der den Antrag prüft und beantwortet. Wird der Antrag bei einem Staat gestellt, der nicht dafür zuständig ist, nimmt dieser mit dem zuständigen Schengen-Staat oder der ETIAS-Zentralstelle, falls diese für die Verifizierung zuständig ist, für die Prüfung der Daten Kontakt auf. Die Prüfung hat generell innert 45 Tagen nach Antragseingang zu erfolgen, Fristverlängerungen sind möglich. Die Person wird über das Resultat der Überprüfung und die allfällige Berichtigung oder Löschung schriftlich informiert. Ist der prüfende Staat der Meinung, dass die Daten nicht rechtswidrig bearbeitet oder gespeichert wurden, informiert er die betroffene Person entsprechend und gibt auch an, wie sie gegebenenfalls Klage erheben oder Beschwerde einlegen kann. Über den ganzen Prozess ist schriftlich Protokoll zu führen. Ein neues Webportal soll es den betroffenen Personen erleichtern, ihre Rechte auf Auskunft und Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten auszuüben und mit

den zuständigen Behörden in Kontakt zu treten (Art. 49). Mittels Eingabe der einmaligen Kennnummer nach Artikel 34c wird die zuständige Behörde ermittelt. Auf dem Webportal sind auch eine E-Mail-Vorlage für eine erleichterte Kommunikation sowie Informationen über Rechte und Verfahren vorhanden.

Personendaten, die in den Zentralkomponenten gespeichert oder verarbeitet werden, dürfen nicht an Drittstaaten, internationale Organisationen, private Stellen oder natürliche Personen übermittelt oder diesen zur Verfügung gestellt werden (Art. 50). Gemäss Artikel 50 gilt dies unter Vorbehalt der jeweiligen Datenschutzbestimmungen zur Übermittlung von Daten nach den Rechtsgrundlagen der EU-Informationssysteme sowie unter Vorbehalt der Abfrage von Interpol-Daten durch das ESP nach den EU-Interoperabilitätsverordnungen.

Die Artikel 51 und 52 regeln die Überwachung durch die Aufsichtsbehörden sowie die Prüfungen durch den Europäischen Datenschutzbeauftragten. Die Schengen-Staaten haben dafür zu sorgen, dass die Aufsichtsbehörden die Rechtsmässigkeit 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 Folgemassnahmen veröffentlichen. Mindestens alle vier Jahre müssen sie die Datenverarbeitungsvorgänge nach einschlägigen internationalen Standards prüfen. Der Europäische Datenschutzbeauftragte ist für die Überwachung der Datenverarbeitungsvorgänge seitens eu-LISA, ETIAS-Zentralstelle und Europol zuständig. Die nationalen Aufsichtsbehörden und der Europäische Datenschutzbeauftragte arbeiten aktiv zusammen und sorgen für eine koordinierte Aufsicht der Nutzung der Zentralkomponenten und der Anwendung anderer Bestimmungen der EU-Interoperabilitätsverordnungen (Art. 53). Alle zwei Jahre erstellt der Europäische Datenschutzbeauftragte einen gemeinsamen Bericht über diese Tätigkeiten. Der Bericht enthält für jeden Schengen-Staat ein Kapitel, das von der Aufsichtsbehörde des betreffenden Staats erstellt wird.

Verantwortlichkeiten (Kapitel VIII)

Bis zu Artikel 57 stimmen die Artikelnummern in den beiden Interoperabilitätstexten überein. In den Artikeln 54 und 55 sind die Zuständigkeiten von eu-LISA während der Entwicklungsphase und nach der Inbetriebnahme aufgeführt. eu-LISA ist zuständig für die Entwicklung der Zentralkomponenten für die Anpassungen, die aufgrund der Interoperabilität an den Zentralsystemen des EES, VIS, ETIAS, SIS, von Eurodac und des ECRIS-TCN nötig werden, sowie für die Kommunikationsinfrastruktur. Nach Inbetriebnahme garantiert eu-LISA den Betrieb, übernimmt die technische Verwaltung und die Wartung der Systeme. Dabei ist sichergestellt, dass eu-LISA keinen Zugang zu personenbezogenen Daten hat. Artikel 56 listet die Zuständigkeiten der Schengen-Staaten auf. Dazu gehören unter anderem die Anbindung der nationalen Systeme an die neuen Zentralkomponenten oder die Verwaltung und Regelung des Zugangs der berechtigten nationalen Behörden zum ESP, CIR und MID. Die Verordnung «IOP Polizei» listet in Artikel 57 die Verantwortlichkeiten von Europol auf. Die Zuständigkeiten der ETIAS-Zentralstelle (Art. 57 der Verord-

nung «IOP Grenzen», Art. 58 der Verordnung «IOP Polizei») lauten wieder in beiden Verordnungstexten gleich.

Änderungen anderer Rechtsakte der Union (Kapitel IX)

Mit den EU-Interoperabilitätsverordnungen werden Änderungen an bestehenden Rechtsakten vorgenommen. Dabei handelt es sich um Rechtsakte, welche die Schweiz mittels Notenaustausch bereits übernommen hat bzw. für die derzeit das Übernahmeverfahren läuft. Es sind dies die Verordnung (EG) Nr. 767/2008 zum VIS, die Verordnung (EU) 2016/399[26] zum Schengener Grenzkodex, die Verordnung (EU) 2017/2226[27] zum EES, die Verordnung (EU) 2018/1240[28] zum ETIAS, die Verordnung (EU) 2018/1726[29] zu eu-LISA, die Verordnung (EU) 2018/1861[30] zum SIS, die Entscheidung 2004/512/EG[31] betreffend die Einrichtung des VIS sowie der Beschluss 2008/633/JI[32] betreffend den Zugang der Strafverfolgungsbehörden auf das VIS. Die Änderungen an diesen Rechtsakten werden in den Artikeln 58–65 der Verordnung «IOP Grenzen» geregelt. Die Verordnung «IOP Polizei» führt in den Artikeln 59–62 die Änderungen an der Verordnung (EU) 2018/1726 zu eu-

26 Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex), ABl. L 77 vom 23.3.2016, S. 1.

27 Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Aussengrenzen der Mitgliedstaaten und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011, ABl. L 327 vom 9.12.2017, S. 20; zuletzt geändert durch Verordnung (EU) 2019/817, ABl. L 135 vom 22.5.2019, S. 27.

28 Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226, ABl. L 236 vom 19.9.2018, S. 1; zuletzt geändert durch Verordnung (EU) 2019/817, ABl. L 135 vom 22.5.2019 S. 27.

29 Verordnung (EU) 2018/1726 des Europäischen Parlaments und des Rates vom 14. November 2018 über die Agentur der Europäischen Union für das Betriebsmanagement von IT-Grosssystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA), zur Änderung der Verordnung (EG) Nr. 1987/2006 und des Beschlusses 2007/533/JI des Rates sowie zur Aufhebung der Verordnung (EU) Nr. 1077/2011, ABl. L 295 vom 21.11.2018, S. 99.

30 Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr. 1987/2006, ABl. L 312 vom 7.12.2018, S. 14.

31 Entscheidung des Rates vom 8. Juni 2004 zur Einrichtung des Visa-Informationssystems (VIS), ABl. L 213 vom 15.6.2004, S. 5.

32 Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten, ABl. L 218 vom 13.8.2008, S. 129.

LISA, der Verordnung (EU) 2018/1862 zum SIS und der Verordnung (EU) 2019/816[33] zum ECRIS-TCN auf. Die Schweiz ist durch Letztere allerdings nicht gebunden.

Die Anpassungen sind nötig, um den neuen Möglichkeiten, die mit der Interoperabilität geschaffen werden, Rechnung zu tragen. Insbesondere müssen die Datenkategorien, die in den neuen Zentralkomponenten erfasst oder bearbeitet werden, definiert werden und die Verbindung der einzelnen Systeme zu den neuen Zentralkomponenten vorgesehen werden.

Schlussbestimmungen (Kapitel X)

Das letzte Kapitel enthält Bestimmungen zu den Übergangsphasen für die Nutzung der einzelnen Zentralkomponenten sowie den Aufgaben der verschiedenen Behörden, die dabei erfüllt werden müssen (Art. 67–69 der Verordnung «IOP Grenzen» resp. Art. 63–65 der Verordnung «IOP Polizei»). Auch die Aufnahme des Betriebs (Art. 72 der Verordnung «IOP Grenzen» resp. Art. 68 der Verordnung «IOP Polizei»), die Schulung der zuständigen Behörden (Art. 76 der Verordnung «IOP Grenzen» resp. Art. 72 der Verordnung «IOP Polizei»), die Überwachung und Bewertung der Entwicklung und des Betriebs der Zentralkomponenten (Art. 78 der Verordnung «IOP Grenzen» resp. Art. 74 der Verordnung «IOP Polizei») sowie das Inkrafttreten (Art. 79 der Verordnung «IOP Grenzen» resp. Art. 75 der Verordnung «IOP Polizei») sind in diesem Kapitel geregelt.

6 Grundzüge des Umsetzungserlasses

6.1 Die beantragte Neuregelung

Bei der Vorlage handelt es sich um die Übernahme von Weiterentwicklungen des Schengen-Besitzstandes. Um deren Umsetzung in der Schweiz sicherzustellen, sind Anpassungen in Bundesgesetzen und später auch im zugehörigen Verordnungsrecht nötig (s. Ziff. 6.2).

6.2 Rechtlicher Umsetzungsbedarf

Die Verordnungen «IOP Grenzen» und «IOP Polizei» enthalten sowohl direkt anwendbare Bestimmungen wie auch solche, die landesrechtlich konkretisiert werden müssen. Der Bundesbeschluss wiederholt Bestimmungen aus den EU-Verordnungen nur insoweit, als dies insbesondere nach dem DSG erforderlich ist. So sind beispielsweise die Zwecke der Datenbearbeitung, die Zugriffsrechte, die Da-

33 Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) 2018/1726, ABl. L 135 vom 22.5.2019, S. 1.

tenweitergabe und die Sanktion der missbräuchlichen Datenbearbeitung formell-gesetzlich zu regeln. Zusätzlich werden einzelne Bestimmungen wiederholt, die für das Verständnis des Kontextes notwendig sind, wie beispielsweise die Definition der Interoperabilitätskomponenten.

Diejenigen Neuerungen, welche eine Anpassung von Bundesgesetzen erfordern, werden in diesem Abschnitt beschrieben. Zahlreiche Neuerungen haben demgegenüber nur Auswirkungen auf das später zu erlassende Verordnungsrecht und bleiben im Folgenden unberücksichtigt. Durch die EU-Interoperabilitätsverordnungen werden weder die bestehenden Zugriffsrechte der einzelnen Behörden auf die zugrundeliegenden Systeme erweitert noch die Zwecke geändert, für die der Zugriff besteht. Stattdessen werden unter anderem mit dem Webportal neue Möglichkeiten geschaffen, welche die Kommunikation zwischen erfassten Personen und den zuständigen nationalen Behörden erleichtern sollen. Der Zugang auf sensible Personendaten bleibt damit auch nach Übernahme der beiden EU-Verordnungen klar geregelt.

Die Zentralkomponenten verbinden Informationssysteme, die im AIG geregelt sind, sowie polizeiliche Datenbanken, die im BPI geregelt sind. Aus Gründen der Transparenz sollen die Zentralkomponenten entsprechend in diesen beiden Gesetzen geregelt werden, soweit sie Informationssysteme betreffen, die aktuell in einem dieser Gesetze ihre formell-gesetzliche Grundlage haben. Die Zentralkomponenten werden in der Reihenfolge entsprechend ihrer voraussichtlichen Inbetriebnahme geregelt (sBMS zuerst, gefolgt vom CIR, ESP und MID).

Sowohl im AIG als auch im BPI drängen sich aufgrund der Einführung der Zentralkomponenten Anpassungen der Gliederung auf.

Der konkrete Anpassungsbedarf in den einzelnen Gesetzen wird im Folgenden zusammengefasst (vgl. Ziff. 7 für die Erläuterungen zu den einzelnen Artikeln).

Ausländer- und Integrationsgesetz

Da es sich bei einzelnen der im AIG geregelten Informationssysteme um Systeme handelt, die im DAA geregelt sind, und auch um Verwechslungen mit dem nationalen Teil des Schengener Informationssystems (N-SIS) zu verhindern, wird der Begriff «Schengen/Dublin-Informationssysteme» eingeführt.

Aufgrund der Einführung der Zentralkomponenten bei den Schengen/Dublin-Informationssystemen sind die Kapitel 14–14c AIG neu zu gliedern. Ein Kapitel soll die allgemeinen Bestimmungen zum Datenschutz enthalten. Ein anderes soll alle Informationssysteme regeln, ein Kapitel soll die Regelungen zur Interoperabilität zwischen den Schengen/Dublin-Informationssystemen und ein weiteres soll die Datenschutzbestimmungen im Schengen/Dublin-Bereich enthalten.

Da mit der Einführung der Interoperabilität neun EU-Verordnungen angepasst werden mussten, sind auch die entsprechenden Bestimmungen im AIG anzupassen, die diese Schengen/Dublin-Informationssysteme heute regeln bzw. in Zukunft regeln werden.

Neu wird der CIR Bestandteil vom EES, ETIAS, VIS (und zu einem späteren Zeitpunkt von Eurodac). Im AIG sind die entsprechenden Bestimmungen anzupassen, da der CIR einen Teil des Zentralsystems der verschiedenen EU-Systeme wie VIS,

Eurodac, EES und ETIAS insoweit ersetzt, als im CIR neu gewisse alphanummerische (Identitätsdaten und Daten zu den Reisedokumenten) und biometrische Daten der einzelnen Systeme gespeichert werden. So muss im AIG geregelt werden, welche Daten im Zentralsystem des jeweiligen Informationssystems gespeichert bleiben und welche Daten neu im CIR-Teil gespeichert werden.

Des Weiteren sind die einzelnen Zentralkomponenten zu regeln. So werden speziell der Inhalt und die Zugriffe auf die einzelnen Zentralkomponenten definiert (sBMS in Art. 110, CIR in Art. 110*a*–110*d* und MID in Art. 110*f*). Dies entspricht der Vorgabe nach Artikel 17 Absatz 1 DSG, der vorsieht, dass Organe des Bundes Personendaten nur bearbeiten dürfen, wenn dafür eine gesetzliche Grundlage besteht.

Beim CIR sind die unterschiedlichen Zugriffsmöglichkeiten je nach Zweck zu regeln (Identitätsabklärung in Art. 110*b*, Verifizierung von Mehrfachidentitäten in Art. 110*c* und Aufdeckung von Straftaten in Art. 110*d*). Bei Letzterem sollen alle benannten Behörden, insbesondere der Nachrichtendienst des Bundes (NDB), im CIR überprüfen können, ob Daten in den nicht polizeilichen Schengen/Dublin-Informationssystemen (EES, ETIAS, VIS) vorhanden sind («Treffer/kein Treffer»-Mechanismus gemäss Art. 22 der EU-Interoperabilitätsverordnungen). Zum Zweck der Identitätsabklärung sind die Polizeibehörden zu bezeichnen. Es ist weiter festzulegen, welche Behörde für die Verifizierung von Mehrfachidentitäten in welchen Fällen zuständig ist.

Auch die Datenabfrage mittels ESP (Art. 110*e*) sowie die unterschiedlichen Zugriffsrechte auf den MID (Art. 110*g*) durch die zuständigen Behörden sind zu regeln.

Die Datenweitergabe an berechtigte Stellen (Art. 110*h*), die Verantwortung für die Datenbearbeitung im sBMS, CIR und MID sowie die Sanktionen bei der missbräuchlichen Verwendung der Daten sind ebenfalls auf Gesetzesstufe zu regeln (Art. 120*d*). Dabei werden auch die aktuellen Bestimmungen zum zentralen Visa-Informationssystem (C-VIS), EES und ETIAS angepasst.

Zusätzlich sind weitere Ausführungen und Präzisierungen in den Durchführungsrechtsakten und delegierten Rechtsakten der EU zu erwarten, die der Schweiz zu gegebener Zeit ebenfalls notifiziert werden und voraussichtlich ebenfalls auf Verordnungsstufe umzusetzen sein werden.

Schliesslich sind die Verweise auf die EU-Verordnungen im Gesetz zu aktualisieren.

Bundesgesetz über das Informationssystem für den Ausländer- und den Asylbereich

Im Bundesgesetz vom 20. Juni 2003[34] über das Informationssystem für den Ausländer- und den Asylbereich (BGIAA) müssen einzelne Verweise auf Bestimmungen im AIG angepasst werden, die im Rahmen der vorliegenden Revision geändert werden. Damit sind keine materiellen Änderungen im BGIAA verbunden.

34 SR **142.51**

Verantwortlichkeitsgesetz

Das Verantwortlichkeitsgesetz vom 14. März 1958[35] (VG) regelt in den Artikeln 19*a* und 19*b* aktuell die Haftung für Schäden im Zusammenhang mit dem Betrieb des SIS. Die EU-Rechtsgrundlagen von EES, VIS, ETIAS und der Zentralkomponenten kennen ähnliche Haftungsbestimmungen bei einem Schaden, der durch eine widerrechtliche Datenbearbeitung erfolgt ist, wie sie bereits für das SIS gelten. Es erscheint deswegen angezeigt, alle Schengen/Dublin-Informationssysteme bzw. deren Komponenten, die Haftungsbestimmungen kennen, im Verantwortlichkeitsgesetz zu regeln. Der sBMS und das ESP stellen keine Zusammenstellung von Daten im Sinne von Artikel 3 Buchstabe d DSG dar, da darin keine Personendaten gespeichert sind. Entsprechend wird auch der Begriff «Komponenten» eingefügt und nicht nur von «Informationssystemen» gesprochen.

Bundesgesetz über die polizeilichen Informationssysteme des Bundes

Neben dem AIG ist auch das BPI anzupassen. Dieses regelt die Rechtsgrundlagen der polizeilichen Informationssysteme des Bundes. Auch hier gilt, dass die meisten Bestimmungen der beiden EU-Interoperabilitätsverordnungen direkt anwendbar sind und entsprechend keiner Umsetzung im schweizerischen Recht bedürfen. Nach Artikel 17 DSG bedarf die Datenbearbeitung besonders schützenswerter Personendaten durch Behörden des Bundes einer formell-gesetzlichen Grundlage. Entsprechend sind die Zentralkomponenten, die im BPI geregelte Schengen/Dublin-Informationssysteme betreffen, dort zu regeln. Dies betrifft die Zentralkomponenten, die das SIS miteinbeziehen.

Im BPI werden somit entsprechend dem AIG weitgehend gleichlautende Bestimmungen eingefügt, die den sBMS, das ESP und den MID regeln.

Die Schengen/Dublin-Informationssysteme oder deren Komponenten und deren Datenbearbeitung und Verantwortung dafür sollen in aufeinander folgenden Artikeln (16–16*f* BPI) geregelt werden. Sie werden der Reihenfolge ihrer voraussichtlichen Inbetriebnahme folgend festgelegt (sBMS in Art. 16*a*, ESP in Art. 16*b* und MID in Art. 16*c*). Auf eine stärkere Neugliederung wurde verzichtet, da das BPI in verschiedenen Gesetzgebungsvorlagen, welche sich aktuell in parlamentarischer Beratung befinden (Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus[36] und Bundesbeschluss über die Genehmigung und die Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Rechtsgrundlagen über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems [SIS][37]), geändert werden soll. Derzeit ist auch die Reihenfolge des Inkrafttretens der vorerwähnten Vorlagen noch offen. Da das BPI in naher Zukunft einer Totalrevision unterzogen werden soll, wird aktuell auf eine Anpassung der Systematik verzichtet.

35 SR **170.32**
36 BBl **2019** 4157
37 BBl **2020** ....

Mit der per 1. März 2019 in Kraft getretenen Umsetzung der Richtlinie (EU) 2016/680 regelt Artikel 349*c* des Schweizerischen Strafgesetzbuches (StGB)[38] die Bekanntgabe von Personendaten an einen Drittstaat oder an ein internationales Organ.[39] Im Bundesgesetz vom 7. Oktober 1994[40] über die kriminalpolizeilichen Zentralstellen des Bundes und gemeinsame Zentren für Polizei- und Zollzusammenarbeit mit anderen Staaten hält der ebenfalls am 1. März 2019 in Kraft getretene Artikel 13 Absatz 2 fest, dass sich die Bekanntgabe von Personendaten im Rahmen der Polizeizusammenarbeit mit ausländischen Strafverfolgungsbehörden nach den Artikeln 349a–349h StGB richtet.[41] Demgegenüber regelt das BPI generell die Nutzung polizeilicher Informationssystem des Bundes und wird mit der Umsetzung der vorliegenden EU-Interoperabilitätsverordnungen noch erweitert. Entsprechend ist in einer separaten Bestimmung die Datenbekanntgabe an Dritte und internationale Organisationen im Bereich der Interoperabilität festzulegen (Art. 16*e*). Weiter ist auch die Verantwortung für die Datenbearbeitung in den Schengen/Dublin-Informationssystemen oder deren Komponenten zu regeln (Art. 16*f*).

6.3 Besonderer Koordinationsbedarf

Bei der Interoperabilität besteht ein besonderer Koordinationsbedarf in Hinblick auf die Übernahme und Umsetzung der Rechtsgrundlagen über die Errichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS). Da die ETIAS-Vorlage[42] derzeit im Parlament beraten wird, kann in vorliegendem Entwurf des Bundesbeschlusses kein Bezug auf dieses Informationssystem genommen werden, obwohl es einen integralen Bestandteil der Interoperabilität darstellt. Es besteht bei der Interoperabilität auch Koordinationsbedarf mit der Übernahme der Rechtsgrundlagen über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS); die SIS-Vorlage[43] befindet sich ebenfalls noch in parlamentarischer Beratung. Nach den Schlussabstimmungen müssen die entsprechenden Artikel des vorliegenden Entwurfs des Bundesbeschlusses entsprechend ergänzt oder angepasst werden. Des Weiteren besteht ein Koordinationsbedarf beim Inkrafttreten der Rechtsgrundlagen zur Errichtung und Nutzung des Einreise- und Ausrei-

38 SR **311.0**
39 AS **2019** 625
40 SR **360**
41 AS **2019** 625
42 Botschaft vom 6. März 2020 zur Genehmigung und Umsetzung des Notenaustauschs zwischen der Schweiz und der EU betreffend die Übernahme der Verordnung (EU) 2018/1240 über das Europäische Reiseinformations- und -genehmigungssystem (ETIAS) (Weiterentwicklung des Schengen-Besitzstands) und zur Änderung des Ausländer- und Integrationsgesetzes (Unterstellung des Nachrichtendienstes des Bundes unter das Schengen-Datenschutzgesetz), 20.027, BBl **2020** 2885.
43 Botschaft vom 6. März 2020 zur Genehmigung und Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Rechtsgrundlagen über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) (Weiterentwicklungen des Schengen-Besitzstands) und zur Änderung des Bundesgesetzes über das Informationssystem für den Ausländer- und den Asylbereich, 20.025, BBl **2020** 3465.

sesystems (EES)[44]. Ein allfälliger Koordinationsbedarf besteht zudem mit der Änderung vom 14. Dezember 2018 des AIG zur Umsetzung der Verfahrensregelungen und Informationssysteme.[45] Der Koordinationsbedarf zwischen den verschiedenen Vorlagen wird unter Ziffer 8 detailliert aufgeführt.

7 Erläuterungen zu einzelnen Artikeln des Umsetzungserlasses

7.1 Ausländer- und Integrationsgesetz (AIG) vom 16. Dezember 2005

Art. 7 Abs. 3 erster Satz Fussnote

Da die Verordnung (EU) 2016/399 zum Schengener Grenzkodex durch die Verordnung «IOP Grenzen» angepasst wird, ist die Fussnote in Artikel 7 Absatz 3 entsprechend anzupassen.

Art. 9a

Artikel 9*a* übernimmt den Inhalt des bestehenden Artikel 103 AIG ohne materielle Änderungen. Dieser Artikel befasst sich mit der Überwachung der Ankunft am Flughafen. Aufgrund dieser Änderung müssen die Verweise in Artikel 1 Absatz 2 BGIAA angepasst werden.

Art. 92a

Artikel 92*a* übernimmt den Inhalt des bestehenden Artikel 104 AIG ohne materielle Änderungen. Dieser Artikel befasst sich mit der Meldepflicht der Luftverkehrsunternehmen. Aufgrund dieser Änderung müssen die Verweise in Artikel 104*a* Absätze 1bis, 2, 3, 3bis, 4 und 5, in Artikel 104*b* Absatz 1, in Artikel 122*b* Absatz 2 und in Artikel 122*c* Absatz 3 Buchstabe b angepasst werden.

14. Kapitel: Datenbearbeitung und Datenschutz

Aufgrund der Einführung der neuen Zentralkomponenten, welche Einfluss auf alle Schengen/Dublin-Informationssysteme haben, sollen die Kapitel 14–14*c* neu gegliedert werden:

– Das 14. Kapitel soll neu alle Bestimmungen enthalten, welche den Datenschutz und die Datenbearbeitung im Allgemeinen betreffen.

44 Bundesbeschluss über die Genehmigung und die Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Rechtsgrundlagen zur Errichtung und Nutzung des Einreise- und Ausreisesystems (EES) (Verordnungen [EU] 2017/2226 und 2017/2225) (Weiterentwicklungen des Schengen-Besitzstands), BBl **2019** 4573.

45 AS **2019** 1413

- Das 14*a*. Kapitel soll neu alle Informationssysteme (die nationalen Systeme und die Schengen/Dublin-Informationssysteme) regeln.
- Das 14*b*. Kapitel, welches bis anhin die Datenschutzbestimmungen im Rahmen der Schengen-Assoziierungsabkommen enthielt, enthält neu die Bestimmungen zur «Interoperabilität zwischen den Schengen/Dublin-Informationssystemen».
- Das 14*c*. Kapitel, welches bis anhin die Bestimmungen zu Eurodac enthielt, soll neu die Datenschutzbestimmungen im Rahmen der Schengen-Assoziierungsabkommen enthalten. Die Bestimmungen zu Eurodac werden neu ins 14*a*. Kapitel integriert (eigener Abschnitt für Eurodac).

Der Gliederungstitel des 14. Kapitels wird angepasst. Es regelt neu nur die Datenbearbeitung und den Datenschutz. Die Informationssysteme erhalten ein eigenes Kapitel (14*a*).

Das 14. Kapitel umfasst neben den bestehenden Artikeln 101 AIG (Datenbearbeitung), 102 AIG (Datenerhebung zur Identifikation und zur Altersbestimmung), 102*a* AIG (Biometrische Daten für Ausweise) und102*b* AIG (Kontrolle der Identität der Ausweisinhaberinnen oder -inhaber) neu die folgenden Artikel:

- 102*c* (Bekanntgabe von Personendaten ans Ausland);
- 102*d* (Bekanntgabe von Personendaten an den Heimat- oder Herkunftsstaat)
- 102*e* (Bekanntgabe von Personendaten bei Rückübernahme- und Transitabkommen)

Die Unterteilung in Abschnitte wird aufgehoben.

Art. 102c Bekanntgabe von Personendaten ans Ausland

Artikel 102*c* übernimmt den Inhalt des bestehenden Artikels 105 AIG ohne materielle Änderungen. Dieser Artikel befasst sich mit der Bekanntgabe von Personendaten ans Ausland.

Art. 102d Bekanntgabe von Personendaten an den Heimat- oder Herkunftsstaat

Artikel 102*d* übernimmt den Inhalt des bestehenden Artikel 106 AIG ohne materielle Änderungen. Dieser Artikel befasst sich mit der Bekanntgabe von Personendaten an den Heimat- oder Herkunftsstaat.

Art. 102e Bekanntgabe von Personendaten bei Rückübernahme- und Transitabkommen

Artikel 102*e* übernimmt den Inhalt des bestehenden Artikels 107 AIG ohne materielle Änderungen. Dieser Artikel befasst sich mit der Bekanntgabe von Personendaten bei Rückübernahme- und Transitabkommen.

Art. 103

Siehe Kommentar zu Artikel 9*a*.

14a. Kapitel: Informationssysteme

Das 14*a*. Kapitel beginnt neu vor Artikel 103*a* AIG (Informationssystem Einreiseverweigerungen) und befasst sich mit folgenden Informationssystemen:

- 1. Abschnitt (Informationssystem Einreiseverweigerungen [INAD-System]: Art. 103*a* AIG[46];
- 2. Abschnitt (Einreise- und Ausreisesystem [EES] und automatisierte Grenzkontrolle): Art. 103*b*–103*g* AIG[47];
- 3. Abschnitt (Passagier-Informationssystem [API-System]): Art. 104*a*–104*c* sowie 108 AIG (wobei Art. 108 AIG bereits aufgehoben ist);
- 4. Abschnitt (Zentrales Visa-Informationssystem [C-VIS] und nationales Visumsystem [ORBIS]): Art. 109*a*–109*e* AIG;
- 5. Abschnitt (Informationssystem für die Durchführung der Rückkehr): Art. 109*f*–109*j* AIG;
- 6. Abschnitt (Eurodac): Art. 109*k* und 109*l* E-AIG;
- 7. Abschnitt Personendossier- und Dokumentationssystem: Art. 109*m* E-AIG.

1. Abschnitt: Informationssystem Einreiseverweigerungen (INAD-System)

Vor Artikel 103*a* wird neu ein Abschnitt eingefügt mit dem Titel «Informationssystem Einreiseverweigerungen (INAD-System)».

Art. 103a[48]

Da unter dem 1. Abschnitt nur ein Artikel aufgeführt wird, kann der Titel des Artikels 103*a* gestrichen werden.

2. Abschnitt: Einreise- und Ausreisesystem (EES) und automatisierte Grenzkontrolle

Vor Artikel 103*b* wird neu ein Abschnitt eingefügt. Er enthält Bestimmungen zum EES sowie zur automatisierten Grenzkontrolle.

46 BBl **2019** 4573
47 BBl **2019** 4573
48 BBl **2019** 4573

Art. 103b Abs. 1 Fussnote, Abs. 2 Bst. a und b^bis und Abs. 4[49]

Abs. 1 Fussnote

Da die Verordnung (EU) 2017/2226 zum EES durch die Verordnung «IOP Grenzen» angepasst wird, ist die Fussnote in Artikel 103*b* Absatz 1 entsprechend anzupassen.

Abs. 2 Bst. a und b^bis

In Artikel 103*b* Absatz 2 Buchstabe a werden die Daten über die erteilten Visa nicht mehr aufgeführt. Sie werden separat in Buchstabe b^bis geregelt. Dies ermöglicht einen präzisen Verweis in Absatz 4 auf die Daten, welche neu im CIR gespeichert werden. Der Begriff «alphanumerische Daten» wird durch «Identitätsdaten und Daten zu den Reisedokumenten» ersetzt.

Abs. 4

Absatz 4 präzisiert, welche Daten im CIR (s. hierzu Ausführungen zu Art. 110*a*) gespeichert werden. Die Identitätsdaten und die Daten zu den Reisedokumenten (Art. 103*b* Abs. 2 Bst. a AIG) sowie das Gesichtsbild und gegebenenfalls die Fingerabdrücke (Art. 103*b* Abs. 2 Bst. b und Abs. 3 AIG) werden im CIR gespeichert. Die Informationen zum Zeitpunkt der Ein- und Ausreise in den und aus dem Schengen-Raum sowie die Grenzübergangsstelle und die für die Grenzkontrolle zuständige Behörde sowie die Daten zu den Einreiseverweigerungen sind von einer Speicherung im CIR ausgenommen; sie bleiben nach wie vor nur im EES gespeichert.

Art. 103d Sachüberschrift (betrifft nur den französischen Text) und Abs. 3[50]

Die Sachüberschrift wird in der französischen Fassung an die Formulierung der Bestimmungen angepasst. Hinsichtlich der Weitergabe von EES-Daten, welche im CIR gespeichert sind, verweist Absatz 3 auf Artikel 110*h*. Dieser verweist wiederum auf Artikel 40 der beiden EU-Interoperabilitätsverordnungen (vgl. Erläuterungen zu Art. 110*h* und Ziff.3.2, Datenschutz). Grundsätzlich sind bei den EES-Stammdaten, die im CIR gespeichert sind, die Bestimmungen des VII. Kapitels der EU-Interoperabilitätsverordnungen zu beachten.

Art. 104

Vgl. Kommentar zu Artikel 92*a*.

3. Abschnitt: Passagier-Informationssystem (API-System) und Zugang zu Passagierdaten im Einzelfall

Vor Artikel 104*a* wird ein neuer Abschnitt eingefügt. Der Abschnitt enthält Regelungen zum Passagier-Informationssystem API (Art. 104*a*–104*c*). Bei einzelnen

49 BBl **2019** 4573
50 BBl **2019** 4573

Bestimmungen dieses Abschnittes müssen formelle Anpassungen vorgenommen werden. Materielle Änderungen gibt es keine.

Art. 104a Sachüberschrift und Abs. 1bis–5 Einleitungsteil

Da Artikel 104*a* neu eine von mehreren Bestimmungen des Abschnitts «Passagier-Informationssystem» bildet, muss die Sachüberschrift dieser Bestimmung angepasst werden. Ausserdem müssen die Verweise in den erwähnten Absätzen angepasst werden (vgl. Kommentar zu Art. 92*a*).

Art. 104b Abs. 1

Vgl. Kommentar zu Artikel 92*a*.

14. Kapitel 3. Abschnitt (Art. 105–107)

Aufgehoben

Der 3. Abschnitt des 14. Kapitels wird aufgehoben. Dieses enthält neu keine Unterteilung in Abschnitte mehr. Die Artikel 105–107 sind neu materiell unverändert in den Artikeln 102*c*–102*e* geregelt.

4. Abschnitt: Zentrales Visa-Informationssystem (C-VIS) und nationales Visumsystem (ORBIS)

Vor Artikel 109*a* wird ein neuer Abschnitt eingefügt. Der Abschnitt enthält Regelungen zum C-VIS und zum ORBIS (Art. 109*a*–109*e* und Art. 109*f*–109*j*).

Art. 109a Sachüberschrift, Abs. 1 und Abs. 1bis

Abs. 1

Da die Verordnung (EG) Nr. 767/2008 zum VIS durch die Verordnung «IOP Grenzen» angepasst wird, ist die Fussnote in Artikel 109*a* Absatz 1 entsprechend anzupassen.

Abs. 1bis

Absatz 1bis präzisiert, welche Daten im C-VIS gespeichert sind und welche Daten im CIR (s. hierzu Ausführungen zu Art. 110*a*) gespeichert werden. So werden die Identitätsdaten und die Daten zu den Reisedokumenten sowie die biometrischen Daten im CIR gespeichert. Die übrigen Informationen zum Visumverfahren werden nicht im CIR gespeichert; sie bleiben nur im C-VIS gespeichert.

Art. 109b, Abs. 1, 2 Einleitungssatz und 2bis –4

In Absatz 1 wird der Begriff «ORBIS» für das nationale Visumsystem neu im AIG eingeführt. Entsprechend ersetzt der Begriff ORBIS in den nachfolgenden Bestim-

mungen den Begriff «nationales Visumsystem». Einzelne Bestimmungen werden formell und redaktionell angepasst, bleiben jedoch materiell unverändert.

Art. 109c Sachüberschrift und Einleitungssatz

Vgl. Erläuterungen zu Artikel 109*b*

Art. 109d Fussnote

Die Fussnote muss aktualisiert werden.

5. Abschnitt: Informationssystem für die Durchführung der Rückkehr

Vor Artikel 109*f* AIG wird ein neuer Abschnitt eingefügt. Der Abschnitt enthält Regelungen zum Informationssystem für die Durchführung der Rückkehr. Diese Bestimmungen wurden mit der Änderung des AIG (Verfahrensregelungen und Informationssysteme) vom 14. Dezember 2018 eingeführt und sind am 1. April 2020 in Kraft getreten.[51] Materielle Anpassungen der Bestimmungen gibt es keine.

6. Abschnitt: Eurodac

Vor Artikel 109*k* wird ein neuer Abschnitt eingefügt. Der Abschnitt enthält Regelungen zu Eurodac.

Art. 109k Datenerhebung und -übermittlung in Eurodac

Artikel 109*k* übernimmt den Inhalt des bestehenden Artikel 111*i* AIG ohne materielle Änderungen. Lediglich die Sachüberschrift wird angepasst. Dieser Artikel befasst sich mit Eurodac.

Die Zentralkomponenten sollten sich auch auf Eurodac erstrecken. So soll der CIR eine gemeinsame Speichereinheit für Identitäts- und biometrische Daten sowie Daten zu den Reisedokumenten von in Eurodac erfassten Personen einschliessen. Jedoch gilt die Verordnung «IOP Polizei» für Eurodac erst ab dem Tag der Anwendbarkeit der Neufassung der Verordnung (EU) Nr. 603/2013 (Art. 75 Verordnung «IOP Polizei»).

Art. 109l Bekanntgabe von Eurodac-Daten

Dieser Artikel übernimmt den aktuellen Artikel 111*d* Absatz 5 ohne materielle Änderungen, jedoch mit redaktionellen Anpassungen. Diese Bestimmung regelt die Datenbekanntgabe von Eurodac-Daten und gehört thematisch zum 7. Abschnitt.

51 AS **2019** 1413, **2020** 881

7. Abschnitt: Personendossier- und Dokumentationssystem

Der bisherige 3. Abschnitt wird zum 7. Abschnitt. Der Abschnitt enthält eine Bestimmung zum Personendossier und Dokumentationssystem des Staatssekretariats für Migration (SEM).

Art. 109m

Dieser Artikel übernimmt den aktuellen Artikel 110 ohne materielle Änderungen.

14b. Kapitel: Interoperabilität zwischen den Schengen/Dublin-Informationssystemen

1. Abschnitt: Gemeinsamer Dienst für den Abgleich biometrischer Daten (sBMS)

Art. 110

Neu regelt Artikel 110 den gemeinsamen Dienst für den Abgleich biometrischer Daten (sBMS). Die Regelung im geltenden Artikel 110 AIG (automatisiertes Personendossier- und Dokumentationssystem) ist nicht mehr notwendig und wird daher aufgehoben.

Abs. 1 und 3

Der sBMS ermöglicht mit Hilfe sogenannter «Templates» bzw. biometrischer Merkmalsdaten, die aus den biometrischen Personendaten in den Schengen/Dublin-Informationssystemen generiert wurden, die systemübergreifende Abfrage der von der Interoperabilität betroffenen Schengen/Dublin-Informationssysteme. Der Rückschluss vom Template auf die effektiven biometrischen Daten ist nicht möglich.

Im Gegensatz zum CIR (Art. 110*a*–110*d* E-AIG) oder zum MID (Art. 110*g* E-AIG) handelt es sich beim sBMS nicht um eine Datensammlung bzw. «Datenbank» im Sinne von Artikel 3 Buchstabe g DSG. Die im sBMS enthaltenen biometrischen Merkmalsdaten sind keine biometrischen Personendaten, es werden auch keine weiteren Personendaten in diesem System gespeichert (vgl. dazu Ziff. 5.2.1). Obwohl die Bestimmungen zum sBMS in den beiden EU–Interoperabilitätsverordnungen direkt anwendbar sind, soll der Vollständigkeit halber eine Bestimmung zum sBMS im AIG aufgenommen werden. Bei anderen neuen Bestimmungen im AIG wird auf den sBMS verwiesen.

Abs. 2

Der Verweis im sBMS auf das jeweilige Informationssystem dient dazu, eruieren zu können, aus welchem Schengen/Dublin-Informationssystem (EES, VIS, Eurodac, SIS) und aus welchen tatsächlichen Datensätzen dieser Informationssysteme die biometrischen Personendaten ursprünglich stammen, auf deren Grundlage die biometrischen Merkmalsdaten generiert wurden.

Die detaillierten Regelungen zum sBMS sind in Kapitel III der beiden EU-Interoperabilitätsverordnungen enthalten. Ausführliche Informationen zum sBMS sind unter Ziffer 5.1.2 zu finden.

2. Abschnitt: Gemeinsamer Speicher für Identitätsdaten (CIR)

Art. 110a Inhalt des Gemeinsamen Speichers für Identitätsdaten

Abs. 1

Der CIR enthält für jede Person, welche im EES, im C-VIS, im ETIAS oder zu einem späteren Zeitpunkt in Eurodac erfasst ist, eine individuelle Datei mit ihren Identitätsdaten, Daten zu den Reisedokumenten und biometrischen Daten aus diesen Schengen/Dublin-Informationssystemen. Die alphanumerischen Daten umfassen die Identitätsdaten der betroffenen Person und die Daten zu deren Reisedokumenten. Das ETIAS kann jetzt noch nicht im Gesetzestext erwähnt werden, da die Übernahme dieser Weiterentwicklung vom Parlament noch nicht genehmigt worden ist (s. dazu Ziff. 8.1).

Der CIR soll die Identifizierung der Personen erleichtern, deren Daten in den erwähnten Schengen/Dublin-Informationssystemen enthalten sind, und das Aufdecken von Mehrfachidentitäten unterstützen. Er soll auch den Zugang der zur Verhütung, Aufdeckung oder Untersuchung terroristischer und anderer schwerer Straftaten benannten Behörden zu diesen Informationssystemen zu diesem Zweck erleichtern und vereinheitlichen. Die entsprechenden Zugriffsrechte auf den CIR werden in den Artikeln 110*b*–110*d* AIG geregelt. Geplant ist, dass die Abfrage des CIR über das ESP (vgl. Art. 110*e* E-AIG) ausgelöst wird. Die Inbetriebnahme des CIR erfolgt voraussichtlich Mitte 2022, während das ESP erst Mitte 2023 betriebsbereit sein wird. Daher muss noch geklärt werden, ob der CIR während einer Übergangszeit, bis beide Zentralkomponenten in Betrieb sind, auch ohne ESP abgefragt werden kann. Ausführliche Informationen zum CIR sind unter Ziffer 5.1 zu finden.

Abs. 2

Der CIR enthält für jeden Satz der gespeicherten Identitätsdaten, Daten zu den Reisedokumenten und biometrischen Daten einen Verweis auf das zugrundeliegende Schengen/Dublin-Informationssystem, aus welchem die entsprechenden Daten stammen, sowie einen Verweis auf den tatsächlichen Datensatz in dem entsprechenden Schengen/Dublin-Informationssystem.

Die detaillierten Regelungen zum CIR sind in Kapitel IV der beiden EU-Interoperabilitätsverordnungen enthalten.

Art. 110b Abfrage des CIR zwecks Identifikation

Abs. 1 und 2

Gemäss Artikel 20 Absatz 1 der EU-Interoperabilitätsverordnungen muss eine der folgenden Bedingungen für eine Abfrage zwecks Identifikation erfüllt sein (Abs. 1 Bst a und Abs. 2):

- Eine Polizeibehörde kann eine Person wegen des Fehlens eines Reisedokuments oder eines anderen glaubwürdigen Dokuments zum Nachweis der Identität nicht identifizieren.
- Es bestehen Zweifel an den von einer Person vorgelegten Identitätsdaten;
- Es bestehen Zweifel an der Echtheit eines Reisedokuments oder eines anderen glaubwürdigen, von einer Person vorgelegten Dokuments.
- Es bestehen Zweifel an der Identität der Inhaberin oder des Inhabers eines Reisedokuments oder eines anderen glaubwürdigen Dokuments.
- Eine Person ist zu einer Zusammenarbeit nicht in der Lage oder sie verweigert die Mitwirkung.

Im Falle von Naturkatastrophen, bei Unfallereignissen oder Terroranschlägen dürfen die nach Artikel 110*b* Absatz 3 E-AIG abfrageberechtigten Behörden ausschliesslich zur Identifikation unbekannter Personen, die sich nicht ausweisen können, oder nicht identifizierter menschlicher Überreste mit den biometrischen Daten der betroffenen Person Abfragen im CIR vornehmen (Abs. 1 Bst. b).

Abs. 3

Die Behörden, welche im konkreten Einzelfall den CIR zum Zweck der Identifikation von Drittstaatsangehörigen abfragen dürfen, werden in Absatz 3 definiert. Eine Abfrage darf nur zu folgenden Zwecken erfolgen: zur Bekämpfung der illegalen Einwanderung, zum Schutz der öffentlichen Sicherheit und Ordnung sowie zur Wahrung der inneren Sicherheit.

Es sind dies das Bundesamt für Polizei (fedpol), die Polizeibehörden der Kantone und Gemeinden sowie die Eidgenössische Zollverwaltung (EZV) zum Schutz der Bevölkerung und zur Wahrung der inneren Sicherheit. fedpol erhält den Zugriff für Identifizierungen auf dem Staatsgebiet, die es im Rahmen seiner Aktivitäten der öffentlichen Sicherheit und Ordnung durchführt. Die Polizeibehörden der Kantone und Gemeinden erhalten auch zur Verifizierung der Legalität des Aufenthalts einen Zugriff. Die EZV erhält den Zugriff zur Erfüllung der ihr übertragenen Aufgaben, insbesondere um den ordnungsgemässen Verkehr von Personen und Waren über die Zollgrenze zu gewährleisten und um zur inneren Sicherheit des Landes und zum Schutz der Bevölkerung beizutragen. Sie ist namentlich befugt, den Verkehr von Personen zu kontrollieren. Diese Kontrolle beinhaltet die Überprüfung der Identität, der Berechtigung zum Grenzübertritt und der Berechtigung zum Aufenthalt einer Person in der Schweiz.

Abs. 4 und 5

Die Abfrage im CIR erfolgt grundsätzlich auf der Grundlage direkt vor Ort erhobener und aktueller biometrischer Daten der betroffenen ausländischen Person. Das Verfahren zur Identifikation muss grundsätzlich im Beisein der betroffenen Person eingeleitet werden. Die Anwesenheit der betroffenen Person ist also nicht während des ganzen Verfahrens zur Identifikation notwendig. Ist eine Abfrage mittels biometrischer Daten nicht möglich oder nicht erfolgreich, ist die Abfrage anhand von Reisedokumentendaten oder Identitätsdaten vorzunehmen.

Art. 110c Abfrage des CIR zwecks Aufdeckung von Mehrfachidentitäten

Abs. 1

Wenn bei der Abfrage des CIR eine gelbe Verknüpfung (vgl. Ziff. 5.1.4) angezeigt wird, dürfen die in diesem Absatz bezeichneten Behörden für die manuelle Verifizierung verschiedener Identitäten ausschliesslich auf die im CIR enthaltenen biometrischen Personendaten, auf die Identitätsdaten, auf die Daten zu den Reisdokumenten und auf den Verweis zum Schengen/Dublin-Informationssystem, aus dem die Daten stammen, zugreifen. Das ETIAS kann jetzt noch nicht im Gesetzestext erwähnt werden, da die Übernahme dieser Weiterentwicklung vom Parlament noch nicht genehmigt worden ist (s. dazu Ziff. 8.1).

Abs. 2

Wenn bei der Abfrage des CIR eine rote Verknüpfung angezeigt wird (vgl. Ziff. 5.1.4), dürfen die Behörden, die auf der Grundlage des AIG oder des BPI Zugriff auf den CIR, das EES, das ETIAS, das C-VIS, Eurodac oder das SIS haben, zur Bekämpfung von Identitätsbetrug auf die im CIR enthaltenen Daten (vgl. Erläuterungen zu Abs. 1) sowie auf den Verweis auf das Schengen/Dublin-Informationssystem zugreifen. Das ETIAS kann jetzt noch nicht im Gesetzestext erwähnt werden, da die Übernahme dieser Weiterentwicklung vom Parlament noch nicht genehmigt worden ist (s. dazu Ziff. 8.1).

Art. 110d Abfrage des CIR zwecks Verhütung, Aufdeckung oder Ermittlung terroristischer oder sonstiger schwerer Straftaten

Abs. 1 und 2

Wenn bei einem konkreten Einzelfall Gründe dafür bestehen, dass die Abfrage eines Schengen/Dublin-Informationssystems zur Verhütung, Aufdeckung oder Untersuchung terroristischer oder anderer schwerer Straftaten beitragen kann, können fedpol, der NDB, die Bundesanwaltschaft und die kantonalen Polizei- und Strafverfolgungsbehörden sowie die Polizeibehörden der Städte Zürich, Winterthur, Lausanne, Chiasso und Lugano den CIR abfragen, um in Erfahrung zu bringen, ob im EES, im VIS, im ETIAS oder in Eurodac Daten zu der entsprechenden Person vorhanden sind. Die in diesem Absatz aufgeführten kommunalen Polizeibehörden (Zürich, Lugano usw.) sind abfrageberechtigt, da sie gleich wie die Kantonspolizeien kriminalpolizeiliche Aufgaben im Rahmen der Verhütung, Aufdeckung und Ermittlung

schwerer Straftaten wahrnehmen (vgl. so auch bereits die Regelung in Art. 109*a* Abs. 3 AIG). In der Botschaft des Bundesrates vom 22. Mai 2019[52] zum Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus wird der Begriff «schwere Straftaten» genauer definiert. Darunter fallen insbesondere Straftaten nach Artikel 286 Absatz 2 der Strafprozessordnung[53]. Im Rahmen der Gesetzesanpassungen zur Terrorismusbekämpfung werden im StGB auch die «terroristischen Straftaten» präzisiert.

Abs. 3 und 4

Der Zugang der benannten Behörden zum CIR erfolgt gemäss einem zweistufigen Verfahren. In einem ersten Schritt erhält die benannte Behörde nur die Information, ob in den jeweiligen Systemen Informationen zu einer Person vorhanden sind. Wenn eine Abfrage des CIR ergibt, dass Daten zu der betreffenden Person in einem der erwähnten Schengen/Dublin-Informationssysteme enthalten sind, zeigt der CIR den benannten Behörden nach Absatz 2 den entsprechenden Verweis auf das EES, das VIS, das ETIAS oder Eurodac an. In einem zweiten Schritt hat sie den Zugriff auf die betroffenen Daten über die Einsatzzentrale fedpol zu beantragen.

Falls eine benannte Behörde nach Absatz 2 trotz einem entsprechenden Hinweis auf eine Antragstellung verzichtet, sind die Gründe dafür in einer nationalen Datei rückverfolgbar festzuhalten.

3. Abschnitt: Europäisches Suchportal (ESP)

Art. 110e

Das ESP soll so geschaffen werden, dass damit die systemübergreifende, parallel erfolgende Abfrage aller einschlägigen Schengen/Dublin-Informationssysteme sowie der Interpol-Datenbanken und Europol-Daten ermöglicht wird. Es soll als einzige Schnittstelle für eine nahtlose Abfrage der erforderlichen Informationen in den verschiedenen Informationssystemen dienen. Dabei sollen die Zugriffsrechte und die Datenschutzanforderungen vollständig gewahrt werden.

Anhand von Identitätsdaten, Daten zu den Reisedokumenten und biometrischen Personendaten ist es möglich, mit dem ESP gleichzeitig das EES, das VIS, das ETIAS, Eurodac, das SIS, die Interpol-Datenbanken SLTD und TDAWN sowie Europol-Daten abzufragen (Art. 6 und 7 der EU-Interoperabilitätsverordnungen). Das ETIAS kann jetzt noch nicht im Gesetzestext erwähnt werden, da die Übernahme dieser Weiterentwicklung vom Parlament noch nicht genehmigt worden ist (s. dazu Ziff. 8.1).

Eine Suche mittels ESP wird dann eingeleitet, wenn:

– Daten in eine der genannten Datenbanken eingegeben werden;

52 BBl **2019** 4751
53 SR **312.0**

– Grenzübertrittskontrollen an den Schengen-Aussengrenzen oder Identitätskontrollen durchgeführt werden.

Eine Suche kann ferner eingeleitet werden, um den rechtmässigen Aufenthalt von Drittstaatsangehörigen in der Schweiz zu überprüfen.

Die Suche mittels ESP ist jedoch nur für diejenigen Behörden möglich, welche bereits auf eine der genannten Datenbanken zugriffsberechtigt sind (Art. 7 der EU-Interoperabilitätsverordnungen). Um die Nutzung des ESP zu ermöglichen, erstellt eu-LISA Kategorien von ESP-Nutzerprofilen, welche den Zugriffsberechtigungen Rechnung tragen (Art. 8 der EU-Interoperabilitätsverordnungen).

Es werden den Nutzerinnen und Nutzern nur diejenigen Daten angezeigt, auf welche sie zugriffsberechtigt sind, und die Verknüpfungen gemäss den Artikeln 30–33 der EU-Interoperabilitätsverordnungen. Es werden keine Angaben zu Daten geliefert, auf die die Nutzerin oder der Nutzer nicht zugreifen darf (Art. 9 der EU-Interoperabilitätsverordnungen).

Jeder Schengen-Staat hat Protokolle über die Abfragen des ESP durch die ermächtigten Behörden resp. deren Bediensteten zu führen.

Die nationalen Schnittstellen zu den verschiedenen Informationssystemen sollen aufrechterhalten werden, um eine technische Ausweichmöglichkeit zu haben.

4. Abschnitt: Detektor für Mehrfachidentitäten (MID)

Art. 110f Inhalt des Detektors für Mehrfachidentitäten

Der MID ist gleichzeitig ein Detektor und eine neue Datenbank, auf welche gewisse Behörden Zugriff haben. Diese Datenbank enthält Identitätsbestätigungsdateien nach Artikel 34 der EU-Interoperabilitätsverordnungen. Deren Inhalte werden gleich lang gespeichert wie die damit verbundenen Daten in mindestens zwei der Schengen/Dublin-Informationssysteme (Art. 35 der EU-Interoperabilitätsverordnungen).

Abs. 1

Absatz 1 legt die Ziele des MID fest: die Identitätskontrollen zu erleichtern und den Identitätsbetrug zu bekämpfen.

Abs. 2

Absatz 2 regelt, in Übereinstimmung mit den EU-Verordnungen, wann die Prüfung auf Mehrfachidentitäten automatisch ausgelöst wird. Bei jeder Neuerfassung eines individuellen Dossiers, bei einer Aktualisierung im EES, VIS, oder ETIAS oder wenn eine Ausschreibung im SIS erfasst oder aktualisiert wird, wird eine automatische Prüfung im CIR und im SIS ausgelöst. Das ETIAS kann noch nicht im Gesetztext erwähnt werden, da diese Übernahme noch nicht vom Parlament genehmigt worden ist (s. dazu Ziff. 8.1)

Abs. 3

Dieser Absatz legt fest, wie die Überprüfung von Mehrfachidentitäten im Rahmen der Interoperabilität der verschiedenen Schengen-Informationssysteme abläuft. Der CIR, das ETIAS, VIS, EES und zu einem späteren Zeitpunkt Eurodac nutzen wie das SIS den sBMS (Art. 110) und das ESP (Art. 110*e*) zur Aufdeckung von Mehrfachidentitäten. Der sBMS erlaubt einen biometrischen Abgleich (Art. 27 Abs. 2 der EU-Interoperabilitätsverordnungen). Das ESP ermöglicht eine Abfrage anhand der Identitätsdaten und Daten zu den Reisedokumenten (Art. 27 Ziff. 3 und 4 der EU-Interoperabilitätsverordnungen). Die Überprüfung findet jeweils nach der Erfassung oder Aktualisierung eines Dossiers in einem der verschiedenen Systeme statt (vgl. Art. 110*f* Abs. 2).

Abs. 4

Dieser Absatz präzisiert die Voraussetzungen für die Erstellung einer Identitätsbestätigungsdatei im MID nach Artikel 34 der EU-Interoperabilitätsverordnungen. Eine solche Datei wird erstellt, wenn die Prüfung auf Mehrfachidentitäten Verknüpfungen zwischen den Daten der verschiedenen Informationssysteme auslöst, welche mit derselben Person verbunden sind und möglicherweise zur selben Person gehören. Diese Verknüpfungen weisen insbesondere auf rechtmässig sowie unrechtmässig verwendete Mehrfachidentitäten hin. Der MID enthält zudem einen Verweis auf die betroffenen Informationssysteme, namentlich eine einmalige Kennnummer, welche es erlaubt, die verbundenen Daten aus den jeweiligen Systemen abzufragen. Schliesslich sind auch das Erstellungsdatum der Verknüpfung, ihre Aktualisierung sowie die für die Verifizierung der Verknüpfungen zuständige Behörde im MID aufgeführt.

Art. 110g Manuelle Verifizierung verschiedener Identitäten im MID

Abs. 1

Eine manuelle Verifizierung muss jedes Mal durchgeführt werden, wenn Verbindungen zwischen Daten aus verschiedenen Systemen bestehen und die Identitäten nicht übereinstimmen oder sich ähneln (gelbe Verknüpfung, Art. 28 Ziff. 4 der EU-Interoperabilitätsverordnungen). Zur Vornahme der manuellen Verifizierung erhalten die dafür zuständigen Behörden (Art. 110*c*) Zugriff auf den MID. Die zuständigen Behörden stimmen mit denjenigen überein, welche zur Aufdeckung möglicher Mehrfachidentitäten auf den CIR zugreifen dürfen. Aus diesem Grund ist es angezeigt, auf Artikel 110*c* Absatz 1 E-AIG zu verweisen, der die Behörden festlegt, die Zugriff auf den CIR haben.

Abs. 2

Dieser Absatz regelt, welche Behörden zur Verifizierung der gelben Verknüpfungen im MID zuständig sind. Dies ist grundsätzlich diejenige Behörde, die eine Abfrage in die Wege leitet, indem sie ein Dossier erfasst oder Daten im C-VIS, im EES oder im ETIAS (nach der Genehmigung der Übernahme dieser Weiterentwicklung)

aktualisiert. In Fällen, in denen polizeiliche Ausschreibungen vorliegen, ist das SIRENE-Büro von fedpol die für die Verifizierung zuständige Behörde.

Zur Unterstützung der manuellen Verifizierung von MID-Verknüpfungen soll eine zentrale MID-Expertenstelle (MES) geschaffen werden. Sie wird sich aus Personal der Bundesämter zusammensetzen, die Verknüpfungen verifizieren dürfen. Die MES soll den Behörden in besonders komplexen Fällen zur Unterstützung dienen, oder wenn einer Behörde das nötige Expertenwissen für die Verifizierung einer MID-Verknüpfung fehlt.

Abs. 3

Die Verifizierung von Mehrfachidentitäten wird in Anwesenheit der betroffenen Person eingeleitet (Art. 29 der Verordnung «IOP Grenzen»). Dies ist insbesondere der Fall, wenn die Verifizierung im Rahmen einer Grenzkontrolle stattfindet oder wenn Verknüpfungen auf Schweizer Territorium zu verifizieren sind. Im Falle von Verknüpfungen, welche in Zusammenhang mit einem Antrag für eine ETIAS-Reisebewilligung stehen, kann die Verifizierung nicht in Anwesenheit der betroffenen Person stattfinden.

Abs. 4

Wird eine unrechtmässige Mehrfachidentität (rote Verknüpfung, Art. 32 der EU-Interoperabilitätsverordnungen) entdeckt oder sind die Daten einer Person rechtmässig in mehreren Schengen-Informationssystemen vorhanden (weisse Verknüpfung, Art. 33 der EU-Interoperabilitätsverordnungen), ist die betroffene Person zu informieren. Die für die manuelle Verifizierung zuständige Behörde übermittelt diese Information mittels eines Standard-Formulars. Darüber hinaus informiert der MID, im Falle der Erstellung einer roten Verknüpfung, automatisch die für die verknüpften Daten zuständigen Behörden (Art. 32 Ziff. 6 der EU-Interoperabilitätsverordnungen).

5. Abschnitt: Datenbekanntgabe und Verantwortung für Datenbearbeitung

Art. 110h Bekanntgabe von Daten aus dem sBMS, dem CIR und dem MID

Grundsätzlich dürfen die Daten der Komponenten der Interoperabilität nicht an Drittstaaten, internationale Organisationen oder private Akteure weitergegeben werden. Die Vorschriften zur Datenbekanntgabe, welche in jedem System vorgesehen sind, bleiben bestehen (Art. 50 der EU-Interoperabilitätsverordnungen). Es handelt sich um den allgemeinen Artikel 111*d* AIG und die Artikel 103*d*[54] und 108*f*, welche die Vorschriften zur Datenbekanntgabe der Informationssysteme EES und ETIAS regeln. Die Daten aus diesen Systemen können jederzeit in Übereinstimmung mit den Bestimmungen, welche in Kraft sind oder zukünftig in Kraft treten werden, weitergegeben werden. Diese Bestimmungen sehen vor, dass die Daten aus

54 BBl **2019** 4573

den verschiedenen Systemen, darin inbegriffen der Inhalt des CIR, in gewissen Fällen weitergeleitet werden können.

Art. 110i Verantwortung für die Datenbearbeitung im sBMS, im CIR und im MID

Diese Bestimmung verweist hinsichtlich der Verantwortung für die Datenbearbeitung in den drei Interoperabilitätskomponenten sBMS, CIR und MID auf Artikel 40 der beiden EU-Interoperabilitätsverordnungen (vgl. dazu Ziff. 3.2, Datenschutz).

14c. Kapitel: Datenschutz im Rahmen der Schengen-Assoziierungsabkommen

Es bietet sich an, das aktuelle Kapitel 14*b* in 14*c* umzunummerieren. Folglich werden alle Bestimmungen, welche den Datenschutz im Rahmen des Schengen-Assoziierungsabkommens betreffen, nach dem neuen Kapitel 14*b* aufgeführt, welches die Interoperabilität betrifft.

Die Bestimmungen in diesem Kapitel bleiben materiell unverändert.

Artikel 111*c* Absatz 3 verweist auf den neuen Artikel 109*l*, sowie auf die Artikel 111*a* und 111*d*. Er erfährt keine materielle Änderung.

Artikel 111*d* Absatz 5 wird aufgehoben und wird zum neuen Artikel 109*l* E-AIG.

Das Auskunftsrecht, welches in Artikel 111*f* vorgesehen ist, nimmt insbesondere Bezug auf das DSG und die kantonalen Gesetze zum Datenschutz. Diese Bestimmung gilt ebenfalls für die Informationen, welche in den verschiedenen Schengen/Dublin-Informationssystemen enthalten sind. Da dieser Artikel Artikel 8 DSG übernimmt, wird seine Aufhebung vorgeschlagen.

Auf ähnliche Weise ist das Recht auf die Abänderung oder Löschung der Daten im DSG geregelt. Dasselbe gilt bezüglich des Informationsrechts. Gewisse Punkte, welche den Datenschutz bezüglich der verschiedenen Schengen/Dublin-Informationssysteme und bezüglich der Interoperabilität betreffen, sind oder werden in den Ausführungsverordnungen konkretisiert. Daher werden die verschiedenen Datenschutzrechte in diesem Kapitel nicht aufgeführt.

Das aktuelle Kapitel 14*c* zu Eurodac wird verschoben und vor dem Kapitel zur Interoperabilität geregelt. Dieses Kapitel wird daher aufgehoben.

Art. 120d Zweckwidriges Bearbeiten von Personendaten in Informationssystemen

Artikel 45 der beiden EU-Interoperabilitätsverordnungen verpflichtet die Schengen-Staaten dazu, Sanktionen für den Missbrauch von Daten sowie die unrechtmässige Verarbeitung oder den Austausch von Daten vorzusehen. Die Ahndung soll wirksam, verhältnismässig und abschreckend sein. Ähnliche Bestimmungen gibt es in der Verordnung (EG) Nr. 767/2008 zu VIS (Art. 36) und in der Verordnung (EU) 2017/2226 (Art. 48).

Entsprechend muss der bestehende Artikel 120*d*, welcher im Rahmen des Projekts EES abgeändert wurde, im Hinblick auf die Interoperabilität erneut angepasst werden.

Das Projekt ETIAS ändert die vorliegende Bestimmung ebenfalls. Diese Vorlage wird derzeit im Parlament beraten.

Der Titel der Bestimmung wird angepasst. Es wird nicht genauer darauf eingegangen, dass es sich nur um Informationssysteme des SEM handelt. Bei einigen der Systeme handelt es sich um Schengen/Dublin-Informationssysteme (CIR und MID), welche nicht ausschliesslich in die Zuständigkeit des SEM fallen. Beim VIS, EES und zukünftig ETIAS handelt es sich um Schengen/Dublin-Informationssysteme, welche in die Zuständigkeit des SEM fallen.

Absatz 1, der im Rahmen des Projekts EES eingefügt wurde und noch nicht in Kraft getreten ist, wird mit der vorliegenden Vorlage angepasst und neu in Artikel 101 Absatz 2 eingefügt. Er erfährt materiell keine Änderung.

Da Absatz 1 neu in Artikel 101 Absatz 2 eingefügt wurde, ist Artikel 120*d* (Stand: Verabschiedung Projekt EES durch das Parlament) dahingehend systematisch anzupassen, als es neu keine Absätze mehr gibt.

Absatz 2 Buchstabe a, welcher im Rahmen des Projekts EES eingefügt wurde und noch nicht in Kraft getreten ist, ist neu Buchstabe a (ohne Absatz). Er sieht Bussen vor im Falle der zweckwidrigen Bearbeitung von Daten des C-VIS.

Buchstabe b des Absatzes 2, welcher im Rahmen des Projekts EES eingefügt wurde und noch nicht in Kraft getreten ist, ist neu Buchstabe b (ohne Absatz) und regelt dasselbe für das EES.

Zukünftig soll auch das ETIAS hier aufgeführt werden. Dies ist jedoch Gegenstand einer separaten Vorlage, welche derzeit im Parlament behandelt wird.

Es bietet sich an, neu zwei Buchstaben c und d vorzusehen, welche die Bestimmungen für den CIR und den MID festlegen. Jede Datenbearbeitung, welche gegen die Artikel 110*a*–110*d*, 110*f* oder 110*g* E-AIG verstösst, ist mit einer Busse zu bestrafen, welche gemäss Artikel 106 Absatz 1 StGB bis zu 10 000 Franken betragen kann, wenn Mitarbeitende der zuständigen Behörden vorsätzlich Personendaten zweckwidrig bearbeiten.

Die strafrechtliche Verfolgung liegt gemäss aktuellem Artikel 120*e* AIG in kantonaler Kompetenz.

Art. 122b Abs. 2

Vgl. Kommentar zu Artikel 92*a*.

Art. 122c Abs. 3 Bst. b

Vgl. Kommentar zu Artikel 92*a*.

Art. 126 Abs. 5

Vgl. Kommentar zu Artikel 102*e*.

7.2 Bundesgesetz vom 20. Juni 2003 über das Informationssystem für den Ausländer- und den Asylbereich

Art. 1 Abs. 2

Vgl. Kommentar zu Artikel 92*a* E-AIG.

Art. 15 Bekanntgabe ins Ausland

Die Artikel 105–107 AIG werden ersetzt durch die Artikel 102*c*–102*e* E-AIG. Der entsprechende Verweis in Artikel 15 BGIAA muss angepasst werden. Der heutige Verweis auf die Artikel 111*d* Absatz 5 und 111*i* AIG wird mit einem Verweis auf die Artikel 109*k* und 109*l* E-AIG ersetzt.

7.3 Verantwortlichkeitsgesetz vom 14. März 1958 (VG)

Gliederungstitel Va. Abschnitt

Im VG soll die Haftung für Schaden, der durch widerrechtliche Datenbearbeitung erfolgt ist, die im Dienste des Bundes oder eines Kantons steht, auf alle Schengen/Dublin-Informationssysteme und deren Komponenten ausgedehnt werden. Entsprechend ist der Gliederungstitel des Abschnittes V*a* anzupassen und hat neu wie folgt zu lauten: *Va. Abschnitt: Haftung für Schäden im Zusammenhang mit dem Betrieb oder der Nutzung der Schengen/Dublin-Informationssysteme oder deren Komponenten.*

Art. 19a

Artikel 19*a* VG regelt aktuell die Haftung bezüglich des SIS. Nach diesem Artikel haftet der Bund für den Schaden, den eine Person, die im Dienste des Bundes oder eines Kantons steht, bei dessen Betrieb einer Drittperson widerrechtlich zufügt. Absatz 2 legt ferner fest, dass dem Bund Rückgriff auf den Kanton zusteht, in dessen Dienst die Person steht, die den Schaden verursacht hat, wenn der Bund Ersatz geleistet hat.

Vorliegender Artikel soll auf alle Schengen/Dublin-Informationssysteme sowie deren Komponenten ausgedehnt werden. Die verschiedenen EU-Rechtsgrundlagen dazu sehen nämlich ebenfalls vor, dass eine Person, die durch eine rechtswidrige Datenverarbeitung einen materiellen oder immateriellen Schaden erlitten hat, das Recht hat, von dem für den Schaden verantwortlichen Schengen-Staat Schadenersatz zu verlangen. Bezüglich EES findet sich die Haftungsbestimmung in Artikel 45 der Verordnung (EU) 2017/2226, bezüglich VIS in Artikel 33 der Verordnung (EG) Nr.

767/2008, bezüglich ETIAS in Artikel 63 der Verordnung (EU) 2018/1240, bezüglich Eurodac in Artikel 37 der Verordnung (EU) Nr. 603/2013 und bezüglich der Zentralkomponenten in Artikel 46 der EU-Interoperabilitätsverordnungen.

Entsprechend werden neu in die Bestimmung aufgenommen das EES (Bst. b), das VIS (Bst. c), der CIR (Bst. d), das ESP (Bst. e), der MID (Bst. f) und Eurodac (Bst. g). Das ETIAS kann noch nicht im Gesetzestext erwähnt werden, da die Übernahme dieser Weiterentwicklung vom Parlament noch nicht genehmigt worden ist (s. dazu Ziff. 8.1).

Es erfolgt zudem eine kleine formelle Anpassung der Bestimmung: Aus Gründen der Klarheit wird der Begriff «Betrieb» ersetzt durch «Betrieb und Nutzung». In der französischen Fassung von Artikel 19*b* wird der Begriff «Nutzung» («utilisation») bereits verwendet.

Art. 19b

Auch vorliegender Artikel ist anzupassen. Er erhält neu zwei Absätze. Anstelle des Verweises auf das SIS in Buchstabe a soll neu die Formulierung «eines der Schengen/Dublin-Informationssysteme oder einer seiner Komponenten» verwendet werden. Auch Buchstabe b ist anzupassen. Aktuell nimmt er Bezug auf eine Ausschreibung im SIS, die zu einem Schaden geführt hat. Allgemeiner und damit in Einklang mit allen Schengen/Dublin-Informationssystemen und deren Komponenten soll von «Datenbearbeitung» gesprochen werden.

Zudem sind neu die Schengen- und die Dublin-Assoziierungsabkommen in einem Anhang festzulegen. Dies sieht Absatz 2 vor.

7.4 Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes (BPI)

Anpassung der Gliederung

Im BPI sollen mehrere Artikel ergänzt werden, die Schengen/Dublin-Informationssysteme oder deren Komponenten regeln. Daher müssen mehrere Gliederungstitel angepasst oder eingefügt werden.

Art. 2

Vorliegender Artikel zählt die Informationssysteme auf, die im BPI geregelt sind. Wie unter Ziffer 6.2 erwähnt, sollen die Zentralkomponenten, die das SIS betreffen, auch im BPI geregelt werden. Sie sind entsprechend in vorliegendem Artikel zu ergänzen.

Neu wird eine Unterteilung vorgenommen in die polizeilichen Informationssysteme (Buchstabe a) und die Schengen/Dublin-Informationssysteme und deren Komponenten (Buchstabe b).

In Buchstabe a werden aufgeführt: der Polizeiliche Informationssystem-Verbund (Art. 9–14): neu Ziffer 1, das automatisierte Polizeifahndungssystem (Art. 15): neu Ziffer 2, der Nationale Polizeiindex (Art. 17): neu Ziffer 3, das Geschäfts- und Aktenverwaltungssystem von fedpol (Art. 18): neu Ziffer 4.

Als Schengen/Dublin-Informationssysteme und deren Komponenten werden in Buchstabe b erwähnt: der nationale Teil des Schengener Informationssystems (N-SIS; Art. 16): neu Ziffer 1. Zu ergänzen sind ferner in den Ziffern 2–4 entsprechend ihrer voraussichtlichen Inbetriebnahme die Zentralkomponenten sBMS (geregelt in Art. 16*a*), das ESP (zu finden in Art. 16*b*) sowie der MID (in Art. 16*c* geregelt).

Art. 16a Gemeinsamer Dienst für den Abgleich biometrischer Daten (sBMS)

Da der sBMS auch ans SIS angeschlossen ist, soll er entsprechend Artikel 110 E-AIG auch im BPI geregelt werden. Dies geschieht in vorliegendem Artikel. Der sBMS wird, trotz direkter Anwendbarkeit der beiden EU-Interoperabilitätsverordnungen, der Vollständigkeit halber ergänzt, damit einfacher auf ihn verwiesen werden kann. Beim sBMS handelt es sich nicht um eine Datensammlung im Sinne von Artikel 3 Buchstabe g DSG, da die biometrischen Merkmalsdaten nicht nach betroffenen Personen erschliessbar sind.

Abs. 1

Im sBMS sind die biometrischen Merkmalsdaten (Templates) gespeichert, die aus dem Gesichtsbild und den Fingerabdrücken aus dem SIS und dem CIR generiert werden. Die entsprechenden Angaben im CIR stammen aus dem EES, dem VIS und Eurodac. Dies erläutert der vorliegende Absatz.

Abs. 2

Der Verweis nach Absatz 2 weist auf das Schengen/Dublin-Informationssystem hin, aus dem die biometrischen Merkmalsdaten ursprünglich generiert wurden, und auf die eigentlichen Datensätze darin. Die enthaltenen Daten sind logisch voneinander getrennt gespeichert nach den Informationssystemen, aus denen sie stammen.

Abs. 3

Der sBMS dient der systemübergreifenden Abfrage mittels biometrischer Daten. Werden neue Datensätze angelegt oder aktualisiert, erfolgt ein automatisierter Datenabgleich über im CIR und im SIS erfasste Personen.

Eine Löschung der dazugehörigen Daten im CIR oder im SIS hat auch die Löschung der Daten im sBMS zur Folge.

Art. 16b Europäisches Suchportal (ESP)

Das ESP soll neben dem AIG (Art. 110*e*) auch im BPI geregelt werden, da es das SIS mitumfasst.

Abs. 1

Wie zu Artikel 110*e* E-AIG ausgeführt, wird es das ESP ermöglichen, mit nur einer einzigen Abfrage alle einschlägigen Schengen/Dublin-Informationssysteme und deren Komponenten (SIS, EES, VIS, ETIAS, Eurodac und CIR) und die Interpol-Datenbanken sowie Europol-Daten abzufragen. Das ETIAS kann jetzt noch nicht im Gesetzestext erwähnt werden, da die Übernahme dieser Weiterentwicklung vom Parlament noch nicht genehmigt worden ist (s. dazu Ziff. 8.1).

Abs. 2

Der Zugriff auf das ESP ist beschränkt auf diejenigen Behörden, die für mindestens eines der Schengen/Dublin-Informationssysteme und deren Komponenten (SIS, EES, VIS, ETIAS, Eurodac und CIR) oder die Interpol-Datenbanken sowie Europol-Daten bereits zugriffsberechtigt sind.

Abs. 3

Die Abfrage durch zugriffsberechtigte Behörden kann mittels Identitätsdaten, Daten zu den Reisedokumenten oder biometrischer Daten erfolgen. Gesucht werden kann nach Personen oder Reisedokumenten.

Abs. 4

Das Abfrageergebnis beschränkt sich auf die Schengen/Dublin-Informationssysteme und die Interpol-Datenbanken bzw. Europol-Daten, auf welche die betreffende Behörde ein Zugriffsrecht besitzt. Bei der Antwort ebenfalls angezeigt wird, aus welchem zugrundeliegenden System die betreffenden Daten stammen, wie auch bestehende Verknüpfungen.

Zusammen mit den Schengen-Staaten wird eu-LISA die für die Datenabfrage zu verwendenden Suchfelder, die spezifischen Daten, die abgefragt werden dürfen, und die Kategorien von Daten, die als Abfrageergebnis ausgegeben werden dürfen, in einem Durchführungsrechtsakt festlegen. Diese Elemente werden teilweise in den Ausführungsverordnungen zu regeln sein.

Art. 16c Detektor für Mehrfachidentitäten

Auch der MID betrifft das SIS und soll neben dem AIG (Art. 110*f*) auch im BPI geregelt werden.

Abs. 1

Absatz 1 regelt die Zwecke des MID. Er soll der Prüfung der Identität dienen und dem Identitätsbetrug entgegenwirken.

Abs. 2

In gewissen Fällen erfolgt automatisiert eine Prüfung auf Mehrfachidentitäten im SIS und im CIR. Dies ist dann der Fall, wenn im SIS, EES, ETIAS, VIS und später auch in Eurodac Daten neu erfasst oder aktualisiert werden. Das ETIAS kann jetzt

noch nicht im Gesetzestext erwähnt werden, da die Übernahme dieser Weiterentwicklung vom Parlament noch nicht genehmigt worden ist (s. dazu Ziff. 8.1).

Abs. 3

Dieser Absatz erläutert, wie die automatisierte Prüfung auf Mehrfachidentitäten konkret abläuft. Um zu prüfen, ob bereits Daten zu einer Person im SIS oder im CIR gespeichert sind, werden einerseits die neu erfassten oder aktualisierten Daten mit bereits im sBMS vorhandenen biometrischen Merkmalsdaten abgeglichen. Andererseits werden über das ESP die Identitätsdaten und die Daten zu den Reisedokumenten mit den bereits vorhandenen alphanumerischen Daten abgeglichen.

Ergibt sich eine oder ergeben sich mehrere Übereinstimmungen, erstellen das SIS und der CIR eine Verknüpfung zwischen den für die Abfrage verwendeten Daten und den Daten, die zu der Übereinstimmung geführt haben.

Abs. 4

Im Falle einer Verknüpfung wird eine Identitätsbestätigungsdatei (s. Art. 34 der beiden EU-Interoperabilitätsverordnungen) erstellt. Darin enthalten sind die folgenden Angaben: die Art der Verknüpfungen zwischen den Daten, sofern eine Übereinstimmung vorliegt, der Verweis auf die Schengen/Dublin-Informationssysteme, in denen die verknüpften Daten verzeichnet sind, eine einmalige Kennnummer, die das Abrufen der verknüpften Daten aus den entsprechenden Schengen/Dublin-Informationssystemen ermöglicht, die Behörde, die für die manuelle Verifizierung verschiedener Identitäten zuständig ist, und das Datum der Erstellung oder der Aktualisierung der Verknüpfung.

Artikel 16d Manuelle Verifizierung von Verknüpfungen im MID

Vorliegender Artikel regelt, welche Behörden zuständig sind für die manuelle Verifizierung bei Verknüpfungen zwischen den Schengen/Dublin-Informationssystemen (vgl. dazu Art. 110 Abs. 1 E-AIG).

Abs. 1

Die Zugriffsberechtigung dient der manuellen Verifizierung gelber Verknüpfungen.

Abs. 2

Grundsätzlich hat diejenige Behörde eine manuelle Verifizierung vorzunehmen, die einen Eintrag oder eine Änderung an einem Dossier in einem der Schengen/Dublin-Informationssysteme vornimmt.

Betrifft eine Verknüpfung eine Ausschreibung im SIS, ausser wenn es um eine Einreiseverweigerung geht, ist das SIRENE-Büro für die manuelle Verifizierung zuständig. Betrifft die Verifizierung das EES, ist die EZV oder die kantonale Polizei zuständig. Das SEM und weitere Visa-Behörden haben die manuelle Verifizierung vorzunehmen, wenn die Verknüpfung das C-VIS betrifft, und das SEM, wenn die Verknüpfung das ETIAS betrifft.

Die für die manuelle Verifizierung zuständige Behörde erhält Zugriff auf die Daten, die sie für die Prüfung der Identität benötigt. Dies sind einerseits die in der betreffenden Identitätsbestätigungsdatei enthaltenen verknüpften Daten und andererseits die im CIR und SIS verknüpften Identitätsdaten. Die Prüfung der verschiedenen Identitäten hat unverzüglich zu erfolgen. Dabei ist die Verknüpfung wie folgt zu aktualisieren: auf Grün (Identitätsdaten der verknüpften Dateien gehören nicht zu derselben Person), auf Rot (unrechtmässige Mehrfachidentität oder Identitätsbetrug liegt vor) oder auf Weiss (es handelt sich um ein und dieselbe Person) und die Identitätsbestätigungsdatei zu ergänzen. Jede Verknüpfung ist einzeln zu prüfen.

Abs. 4

Ergibt die manuelle Verifizierung, dass entweder eine illegale Mehrfachidentität vorliegt (rote Verknüpfung) oder dass eine Person in verschiedenen Schengen/Dublin-Informationssystemen verzeichnet ist (weisse Verknüpfung), ist sie mittels eines Standardformulars über diesen Sachverhalt zu informieren. Auf eine entsprechende Information kann verzichtet werden, wenn dies einer Ausschreibung im SIS entgegenstehen würde sowie wenn dies aus Gründen der Sicherheit und der öffentlichen Ordnung, zur Verhinderung von Kriminalität und zur Gewährleistung, dass keine nationalen Ermittlungen beeinträchtigt werden, nötig ist.

Der MID unterrichtet automatisch die Behörden, die für die Daten einer roten Verknüpfung zuständig sind.

Die manuelle Verifizierung von Mehrfachidentitäten hat, soweit möglich, in Anwesenheit der betroffenen Person zu erfolgen. Zu denken ist insbesondere an Fälle der Kontrolle bei der Einreise ins schweizerische Staatsgebiet, wenn die Schweiz der erste Schengen-Staat ist.

Artikel 16e Bekanntgabe von Daten des sBMS, des CIR und des MID

Vorliegender Artikel regelt, dass personenbezogene Daten, die in den Interoperabilitätskomponenten gespeichert sind, verarbeitet werden oder auf die über die Interoperabilitätskomponenten zugegriffen wird, grundsätzlich nicht an Drittstaaten, internationale Organisationen oder private Stellen übermittelt oder diesen zur Verfügung gestellt werden dürfen. Es gelten weiterhin die Vorschriften zur Datenbekanntgabe, welche für jedes System vorgesehen sind.

Artikel 16f Verantwortung für die Datenbearbeitung im sBMS, im CIR und im MID

Auch die Verantwortung für die Datenbearbeitung ist zu regeln. Sie richtet sich nach Artikel 40 der beiden EU-Interoperabilitätsverordnungen.

8 Koordinationsbedarf

8.1 Koordination mit der ETIAS-Vorlage

Die der Interoperabilität gewidmeten Formulierungen der Artikel 110*a* Absatz 1, 110*c*, 110*e* Absatz 1 und 110*f* Absatz 2 AIG im vorliegenden Entwurf des Bundesbeschlusses sollten das ETIAS-System erwähnen. Die ETIAS-Vorlage[55] wird jedoch voraussichtlich erst in der Herbstsession 2020 vom Parlament genehmigt werden, und vor diesem Zeitpunkt kann man nicht auf das ETIAS verweisen. Sobald diese Schlussabstimmung stattgefunden hat, müssen die genannten Artikel im vorliegenden Entwurf entsprechend ergänzt werden und auf das ETIAS Bezug nehmen. Darüber hinaus muss auch Artikel 19*a* Absatz 1bis VG, der aktuell die Haftung bezüglich der EU-Systeme regelt, neu das ETIAS erwähnen. Zudem müssen auch die Artikel 16*b* Absatz 1 und 16*c* Absatz 2 BPI, die sich mit dem ESP und dem MID befassen, das System ETIAS erwähnen. Entsprechend müssen diese Artikel des vorliegenden Entwurfs nach der Schlussabstimmung zur ETIAS-Vorlage ebenfalls mit dem ETIAS ergänzt werden.

Das Eidgenössische Justiz- und Polizeidepartement (EJPD) wird dem Parlament im Rahmen der parlamentarischen Beratungen zum vorliegenden Entwurf einen entsprechenden Antrag stellen.

Einige Bestimmungen der ETIAS-Vorlage, die sich derzeit in den parlamentarischen Beratungen befinden, werden aufgrund der Interoperabilität ebenfalls geändert werden müssen, nämlich die Artikel 5 Absatz 1 Buchstabe a^{bis}, 108*a*, 108*f* und 120*d* AIG in der Fassung der ETIAS-Vorlage. Diese Artikel müssen wie folgt angepasst werden:

Die Fussnote von Artikel 5 Absatz 1 Buchstabe a^{bis} in der Fassung der ETIAS-Vorlage muss angepasst werden. Da die Verordnung (EU) 2018/1240 durch die Verordnung «IOP Grenzen» angepasst wird, muss die Fussnote AIG entsprechend aktualisiert werden.

Der Abschnitt mit den Regelungen zum ETIAS (Art. 108*a*–108*g*) muss in die neue Gliederungsstruktur eingepasst werden, die der vorliegende Entwurf vorsieht (vgl. dazu die Erläuterungen zum 14*a*. Kapitel in Ziff. 7). Dazu müssen der Abschnittstitel vor Artikel 108*a* sowie alle folgenden Abschnittstitel umnummeriert werden.

Artikel 108*a* AIG in der Fassung der ETIAS-Vorlage regelt die Daten des ETIAS. Diese werden teilweise neu im CIR gespeichert. Ein neuer Absatz 3 muss präzisieren, welche Daten im CIR gespeichert werden. Die Identitätsdaten und die Daten zu den Reisedokumenten (Art. 108*a* Abs. 1 Bst. a in der Fassung der ETIAS-Vorlage) werden im CIR gespeichert. Die Informationen zu den bewilligten oder abgelehnten Gesuchen um eine ETIAS-Reisegenehmigung sowie die Daten der Überwachungsliste sind von einer Speicherung im CIR ausgenommen; sie bleiben nach wie vor nur im ETIAS gespeichert.

55 Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustauschs zwischen der Schweiz und der EU betreffend die Übernahme der Verordnung (EU) 2018/1240 über das Europäische Reiseinformations- und -genehmigungssystem (ETIAS) (Weiterentwicklung des Schengen-Besitzstands), Entwurf in BBl *2020* 2955.

Artikel 108*f* AIG in der Fassung der ETIAS-Vorlage, der gegenwärtig dem Parlament unterbreitet wird, muss im Rahmen der Interoperabilität ebenfalls angepasst werden. Dieser Artikel regelt die Bekanntgabe von ETIAS-Daten. Ein neuer Absatz 3 wird eingeführt. Da der CIR neu ein Bestandteil des ETIAS wird, gelten die Bestimmungen für die Bekanntgabe von ETIAS-Daten auch für diejenigen ETIAS-Daten, die im CIR gespeichert sind (Identitätsdaten, Daten zu den Reisedokumenten und biometrische Daten). Hinsichtlich der Weitergabe von ETIAS-Daten, welche im CIR gespeichert sind, soll ein neuer Absatz 3 auf Artikel 110*h* verweisen. Dieser verweist wiederum auf Artikel 40 der beiden EU-Interoperabilitätsverordnungen. Diese Regelung ist analog zur Regelung, die für das EES gilt (Art. 103*d* Abs. 3 AIG im vorliegenden Entwurf).

Schliesslich muss der Inhalt von Artikel 120*d* Absatz 2 AIG in der dem Parlament derzeit im Rahmen der ETIAS-Vorlage vorgelegten Fassung in den Wortlaut von Artikel 120*d* des vorliegenden Entwurfs aufgenommen werden. Entsprechend müssen diese Artikel nach der Schluss-Abstimmung zur ETIAS-Vorlage noch angepasst werden.

8.2 Koordination mit der Änderung des AIG vom 14. Dezember 2018 zur Umsetzung der Verfahrensregelungen und Informationssysteme

Ein allfälliger Koordinationsbedarf besteht zudem hinsichtlich Artikel 111 AIG (Informationssysteme für Reisedokumente). Diese Bestimmung soll im Rahmen der Vorlage «Verfahrensregelungen und Informationssysteme»[56] aufgehoben werden. Im Gegensatz zu allen anderen Bestimmungen dieser Vorlage wurde die Aufhebung von Artikel 111 AIG noch nicht in Kraft gesetzt, weil das SEM für eine Übergangszeit noch auf die Nutzung des bisherigen Systems zur Ausstellung von Reisedokumenten angewiesen ist. Sollte Artikel 111 AIG bei der Inkraftsetzung des vorliegenden Bundesbeschlusses noch nicht aufgehoben worden sein, müsste diese Bestimmung neu nummeriert werden, da sie nicht in den neuen Abschnitt «Datenbekanntgabe und Verantwortung für die Datenbearbeitung» passt.

8.3 Koordination mit der SIS-Vorlage

Die Interoperabilität ist mit der laufenden Revision des AIG und des BPI im Rahmen der SIS-Vorlage zu koordinieren. Zurzeit prüft das Parlament den Entwurf des Bundesbeschlusses zum SIS. Dieser Bundesbeschluss wird voraussichtlich in der Herbst- oder Wintersession 2020 vom Parlament verabschiedet werden. Unabhängig davon, ob vorliegende Änderung des BPI nach oder gleichzeitig mit dem Bundesbeschluss zum SIS in Kraft tritt, ist Artikel 16 BPI anzupassen, indem in Absatz 1 erster Satz in der französischen Fassung die Formulierung aus dem vorliegenden

56 AS **2019** 1413

Entwurf übernommen wird. Absatz 2 Buchstabe b des vorliegenden Entwurfs ist als Buchstabe c in der SIS-Fassung zu übernehmen.

Die Fussnote von Artikel 68*a* Absatz 2 AIG in der Fassung der SIS-Vorlage muss angepasst werden. Da die Verordnung (EU) 2018/1861 durch die Verordnung «IOP Polizei» angepasst wird, ist die Fussnote in Artikel 68*a* Absatz 2 entsprechend anzupassen.

8.4 Koordination mit der EES-Vorlage

Der Bundesbeschluss zum EES[57] wurde am 21. Juni 2019 vom Parlament genehmigt. Die Vorlage beinhaltet eine Änderung des AIG, indem neue Bestimmungen für das Informationssystem EES aufgenommen werden.

Die Änderung des AIG durch die vorliegende Interoperabilitätsvorlage bezieht sich auf die Bestimmungen des AIG, die durch den verabschiedeten Bundesbeschluss zum EES angepasst wurden, da diese endgültig feststehen.

Der Bundesbeschluss zur Interoperabilität übernimmt den vom Parlament genehmigten Inhalt des Bundesbeschlusses zum EES und fügt die für die Interoperabilität erforderlichen Ergänzungen hinzu (2. Abschnitt: Einreise- und Ausreisesystem (EES) und automatisierte Grenzkontrolle). Sollte der Bundesbeschluss zur Interoperabilität gleichzeitig mit dem Bundesbeschluss zum EES in Kraft treten, sollten daher die Bestimmungen in der Fassung Interoperabilität (und nicht diejenigen in der Fassung EES) gelten.

9 Auswirkungen

9.1 Finanzielle und personelle Auswirkungen auf den Bund

Für den Bund ergeben sich sowohl in der Projektphase als auch in der Anwendung der EU-Interoperabilitätsverordnungen ab Inbetriebnahme finanzielle und personelle Auswirkungen. Der Nutzen der Interoperabilität wird sowohl für den Bund als auch für die Kantone beträchtlich sein.

9.1.1 Finanzielle und personelle Auswirkungen in der Projektphase

Die Gesamtkosten der Interoperabilitätsprojekte für den Bund belaufen sich für die gesamte Zeitspanne von 2020 bis 2025 geschätzt auf 21 Millionen Franken.

57 Bundesbeschluss über die Genehmigung und die Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Rechtsgrundlagen zur Errichtung und Nutzung des Einreise- und Ausreisesystems (EES) (Verordnungen [EU] 2017/2226 und 2017/2225) (Weiterentwicklungen des Schengen-Besitzstands), BBl **2019** 4573.

Kosten (in Mio.) Interoperabilitäts-Projekte	Total	2020	2021	2022	2023	2024	2025
Interoperabilität fedpol	**11,3**	2,9	3,1	1,4	1,5	1,2	1,2
Interoperabilität SEM	**7,7**	2,1	2,2	2,4	1,0		
IOP-Weiterentwicklung (SEM)	**2,0**					1,0	1,0
Total	**21,0**	**5,0**	**5,3**	**3,8**	**2,5**	**2,2**	**2,2**

Die Projekte bei fedpol und beim SEM sind Bestandteil eines Verpflichtungskredites zur Weiterentwicklung des Schengen/Dublin-Besitzstands, der in einem Programm des Generalsekretariats des EJPD (GS-EJPD) geführt wird. Dieses Programm wird als IKT-Schlüsselprojekt geführt. Der Bundesbeschluss zum Verpflichtungskredit[58] wurde vom Nationalrat am 21. Dezember 2019 und vom Ständerat am 11. Juni 2020 gutgeheissen. Der Mittelbedarf der Projekte für die Jahre 2020–2022 beträgt insgesamt 14,1 Millionen Franken. 9,8 Millionen davon stammen aus der ersten Tranche des Verpflichtungskredits und werden durch vom Bund zugewiesene zentrale IKT-Mittel und Eigenmittel des EJPD gedeckt. Die Finanzierung der Projektkosten ab 2023 erfolgt voraussichtlich im Rahmen der Freigabe der zweiten Tranche des Verpflichtungskredits.

Aus der Übernahme und Umsetzung der Interoperabilität werden sich auch technische Anpassungen ergeben. Eine zusätzliche technische nationale Komponente soll die Anbindung der Schweizer Systeme an das ESP sicherstellen. Für die Verifizierung von MID-Verknüpfungen (vgl. 5.1) wird zudem ein nationaler MID-Client benötigt. Diese Komponenten werden durch das Informatik Service Center des EJPD (ISC-EJPD) bereitgestellt. Die Kosten für die Entwicklung sind in den oben aufgeführten Projektkosten enthalten. Die technischen Anforderungen werden von eu-LISA vorgegeben. Es ist zu erwarten, dass die nationalen Komponenten aufgrund von Weiterentwicklungen der EU-Komponenten ebenfalls angepasst werden müssen. Diese Anpassungen werden nach der geplanten Betriebsaufnahme 2023 im Projekt IOP-Weiterentwicklungen des SEM durchgeführt. Für dieses Projekt sind für 2024 und 2025 Kosten von je einer Million Franken eingeplant.

Für fedpol verursacht die Umsetzung der Projektphase zwischen 2020 und 2023 voraussichtlich einen personellen Aufwand von 2800 Personentagen. Das SEM rechnet mit 3960 Personentagen. Die entsprechenden personellen Mittel werden intern kompensiert.

58 Bundesbeschluss vom 11. Juni 2020 über einen Verpflichtungskredit zur Weiterentwicklung des Schengen/Dublin-Besitzstands, BBl **2020** 6471.

Für die EZV dürften sich der Mehraufwand für die Projektleitung und der Entwicklungsaufwand für die Anpassungen der mobilen und stationären Grenzkontrolllösungen im unteren einstelligen Millionenbereich bewegen. Die Kosten sind nach heutigem Kenntnisstand Bestandteil des Programms DaziT der EZV. Die sich daraus ergebenden finanziellen Verpflichtungen werden dem entsprechenden Gesamtkredit angerechnet.

9.1.2 Finanzielle und personelle Auswirkungen ab Inbetriebnahme

Betriebskosten

2023 entstehen voraussichtlich Betriebskosten von 0,2 Millionen Franken und ab 2024 von jährlich circa 2 Millionen Franken für den Betrieb von zwei nationalen Interoperabilitätskomponenten. Diese werden benötigt, um den Anschluss der nationalen Systeme an die Interoperabilität sicherzustellen und die Verifizierung von MID-Verknüpfungen zu ermöglichen. Auf nationaler Ebene ist die Interoperabilität kein reines Organisationsprojekt, sondern beinhaltet auch die Erstellung und den Betrieb von nationalen technischen Komponenten. Die Grössenordnung der Umsetzung war zum Zeitpunkt der Erarbeitung der Botschaft zum Verpflichtungskredit zur Weiterentwicklung des Schengen/Dublin-Besitzstands noch nicht bekannt, weil diese Informationen seitens der EU damals noch nicht zur Verfügung standen. Aus diesem Grund werden die jährlich wiederkehrenden Betriebskosten der Interoperabilitätskomponenten ab Inbetriebnahme nun auf jährlich circa 2 Millionen Franken, anstelle der in der Botschaft zum Verpflichtungskredit[59] genannten 0,2 Millionen Franken, geschätzt. Diese Schätzung ergibt sich aus einem Vergleich mit dem Projekt EES, wo ebenfalls zwei nationale Komponenten durch das ISC-EJPD bereitgestellt und betrieben werden müssen und Betriebskosten in ähnlicher Höhe erwartet werden. In der Konzeptphase des Projekts werden die nötigen finanziellen Mittel für den Betrieb präzisiert und im Rahmen der Erarbeitung des Voranschlags 2024 in notwendiger Höhe beantragt.

Personelle Auswirkungen der Verifizierung von MID-Verknüpfungen

Die Inbetriebnahme der Interoperabilität 2023 wird zu einer erhöhten Anzahl Treffer führen, die nachgelagerte manuelle Abklärungen erforderlich machen werden. MID-Verknüpfungen, die Unterschiede zwischen den Daten aufweisen (gelb gekennzeichnet), müssen immer manuell überprüft werden. Die beiden EU-Interoperabilitätsverordnungen sehen vor, dass die manuelle Verifizierung von MID-Verknüpfungen von jener Behörde durchgeführt wird, welche Daten erfasst oder aktualisiert, die zu der MID-Verknüpfung geführt haben. Für die Schweiz sind dafür das fedpol, SEM, die EZV, die Auslandsvertretungen des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA) sowie die kantonalen Polizei- und Migrationsbehörden zuständig. Eine gelbe MID-Verknüpfung entsteht beispielswei-

59 Botschaft vom 4. September 2019 zu einem Verpflichtungskredit zur Weiterentwicklung des Schengen/Dublin-Besitzstands, BBl **2019** 6189.

se, wenn ein Drittstaatsangehöriger im SIS zwecks Einreiseverbot ausgeschrieben ist und dann mit einem gefälschten Reisepass ein Schengen-Visum beantragt. Die Fingerabdrücke im SIS und im VIS sind identisch, aber die Identitätsdaten nicht. Diese MID-Verknüpfung gilt es manuell zu verifizieren. Dafür sind zusätzliche Abklärungen nötig, um die Identität der Person eindeutig feststellen zu können. Damit wird einerseits die Mobilität von rechtmässig reisenden Personen erleichtert, andererseits kann mit der manuellen Verifizierung Identitätsbetrug aufgedeckt und künftig verhindert werden. Für diese zusätzliche Aufgabe benötigen die zuständigen Behörden zusätzliche personelle Ressourcen. Nach heutigem Kenntnisstand wird davon ausgegangen, dass die Schweizer Behörden künftig jährlich ca. 10 000 gelbe MID-Verknüpfungen manuell verifizieren werden müssen. Ungefähr 60% davon werden voraussichtlich SIS-Daten betreffen. Diese werden zugunsten der Kantone und anderer Behörden durch das SIRENE-Büro bei fedpol verifiziert. Ungefähr 40% der gelben MID-Verknüpfungen werden durch das SEM, die EZV, das EDA und die kantonalen Polizei- und Migrationsbehörden zu bearbeiten sein.

Die Evaluation verschiedener Organisationsvarianten ergab, dass die zuständigen Behörden im Migrationsbereich bei der Verifizierung von MID-Verknüpfungen durch eine zentrale, durch den Bund betriebene und finanzierte MID-Expertenstelle (MES) unterstützt werden sollen. Die MES ist voraussichtlich beim SEM anzusiedeln. Mit dieser Stelle sollen die zuständigen Behörden in komplexen Fällen Unterstützung in Anspruch nehmen können, um ihr Tagesgeschäft nicht zusätzlich zu belasten. Gleichzeitig dient die MES denjenigen Behörden zur Unterstützung, die zum Beispiel nur sehr selten eine MID-Verknüpfung verifizieren müssen, und daher nicht über das nötige Expertenwissen verfügen (z.B. eine Schweizer Botschaft im Ausland). Durch diese begrenzte Zentralisierung können Synergieeffekte genutzt und damit Kosteneinsparungen realisiert werden. Als Kompetenzzentrum setzt die MES qualitative Synergieeffekte frei, indem Wissen aus verschiedenen Bereichen zusammengetragen wird und sich so die Qualität der Verifizierungen verbessert sowie Kommunikationswege verkürzt werden. In der MES wird voraussichtlich Personal der verschiedenen zuständigen Bundesstellen tätig sein. Die genaue Organisation und Zusammensetzung der MES wird in der Konzeptphase des Projektes ausgearbeitet. Die MES darf die Verifizierung der Verknüpfungen allerdings nicht selbstständig wahrnehmen, sondern gibt ihre Ergebnisse nach erfolgter Prüfung der MID-Verknüpfung an die zuständige Behörde zurück. Letztere entscheidet anschliessend, ob es sich um rechtmässige Unterschiede handelt oder ob ein Identitätsbetrug vorliegt. MID-Verknüpfungen, die SIS-Daten beinhalten, müssen immer durch das SIRENE-Büro Schweiz verifiziert werden. Der für die MES benötigte personelle Mehrbedarf ist in der nachfolgenden Tabelle zum personellen Mehraufwand enthalten.

Bei der Inbetriebnahme der Interoperabilität 2023 müssen die entsprechenden Mitarbeitenden einsatzbereit sein. Das EJPD prüft bis Mitte 2021, wie viele zusätzliche Stellen ab 2023 unter Berücksichtigung der im EJPD laufenden Aufgabenüberprüfung und entsprechenden internen Kompensationen effektiv beantragt werden. Ein allfälliger Ressourcenmehrbedarf wird dem Parlament im Rahmen der Botschaft zum Voranschlag mit integriertem Aufgaben- und Finanzplan 2022 unterbreitet werden.

Der personelle Mehraufwand verteilt sich gemäss vorläufiger Schätzung des EJPD wie folgt und wird in den nachfolgenden Unterkapiteln ausführlich dargelegt:

Personeller Mehraufwand (Schätzung)

	ab 2023
Vollzeitstellen (FTE)	
fedpol	11
SEM	6
EZV	1
EDA	0,9
Kantone (Kantonspolizei und Migrationsbehörden)	1,1
Total	**20**

Personelle Auswirkungen für fedpol

MID-Verknüpfungen, welche SIS-Ausschreibungen betreffen, sind zwingend durch das SIRENE-Büro zu verifizieren. Dies bedingt teilweise aufwändige Abklärungen und Konsultationen im Inland und mit anderen Schengen-Staaten. Mit der Weiterentwicklung des SIS kommen auf das SIRENE-Büro bereits neue Ausschreibungskategorien sowie eine obligatorische Bearbeitungsfrist von 12 Stunden zu. Für den Informationsaustausch muss das SIRENE-Büro einen 24/7-Schichtbetrieb sicherstellen, weshalb es den personellen Einsatz auch nachts, an den Wochenenden und an Feiertagen erhöhen müssen wird.

Die Verifizierung von MID-Verknüpfungen auf SIS-Ausschreibungen beinhaltet auch die Kontrolle der Übereinstimmung biometrischer Daten. Der Vergleich von biometrischen Daten wird durch die Abteilung Biometrische Identifikation im 24/7-Schichtbetrieb wahrgenommen.

Durch die Interoperabilität werden polizeiliche Daten automatisiert mit Daten aus anderen EU-Informationssystemen abgeglichen. Folglich werden die Polizeibehörden vermehrt über polizeilich relevante Informationen verfügen, die im Anschluss zu Ermittlungen führen können. Mit der Interoperabilität wird somit auch der Koordinations- und Vorbereitungsaufwand für die Bundeskriminalpolizei zunehmen.

Alle vorstehend beschriebenen Aufgaben lösen in den betroffenen Bereichen Mehraufwand aus, welcher ohne zusätzliche Ressourcen nicht zu bewältigen sein wird. fedpol geht ab Inbetriebnahme der Interoperabilität von einem personellen Mehraufwand im Umfang von insgesamt 11 FTE aus.

Personelle Auswirkungen für das SEM

Beim SEM wird für die Verifizierung der MID-Verknüpfungen der Direktionsbereich Zuwanderung und Integration zuständig sein. Dort sind die gemäss den EU-Verordnungen definierten zuständigen Behörden des SEM angesiedelt. Für die

Verifizierung von MID-Verknüpfungen ergibt sich beim SEM insgesamt ein Mehraufwand von 5 FTE. Ein Teil davon wird in der MES anfallen, welche die komplexen MID-Verknüpfungen im Migrationsbereich bearbeiten wird.

Die Aufwände für die Management- und Supportaufgaben sind in den 5 FTE bereits enthalten. Zusätzlich fallen im SEM Aufgaben im Zusammenhang mit der Anwendungs- und Produkteverantwortung für die nationalen technischen Komponenten an.

Zusammen ergibt dies einen personellen Mehraufwand im SEM von insgesamt 6 FTE.

Personelle Auswirkungen für die EZV

Die vorliegende Weiterentwicklung hat finanzielle, prozessuale und personelle Auswirkungen auf die EZV. Einerseits müssen bei bereits bestehenden Systemen Anpassungen an den Schnittstellen vorgenommen und andererseits diverse neue Systeme, wie das für Kontrollen an Schengen-Aussengrenzen obligatorische ESP, implementiert werden. Allfällige Anpassungen, welche sich aus der Schaffung einer nationalen Abfrageplattform (NAP) ergeben sollten, müssen ergänzend berücksichtigt werden (s. Ziff. 9.2.2).

Das für die Personenkontrolle an der Schengen-Aussengrenze obligatorische ESP wird zu Anpassungen der operationellen Prozesse führen, insbesondere bei der Erkennung von Mehrfach- und Falschidentitäten. Aus heutiger Sicht wird davon ausgegangen, dass sich die Effizienzgewinne durch eine höhere Automatisierung und die Aufwände durch die Aufdeckung von falschen Identitäten in etwa die Waage halten. Für die Verifizierung von MID-Verknüpfungen, inklusive Schulungs- und Ausbildungsmassnahmen, ergibt sich bei der EZV ein geringer Mehraufwand, welcher intern kompensiert wird.

Personelle Auswirkungen für die Konsularische Direktion und die Schweizer Vertretungen im Ausland (EDA)

Die Konsularische Direktion des EDA unterstützt die Vertretungen im Ausland in der Erbringung der konsularischen Dienstleistungen. Sie stellt zweckdienliche Arbeitsinstrumente zur Verfügung und koordiniert die Zusammenarbeit mit nationalen und internationalen Partnern. Die Auslandvertretungen werden für die Verifizierung von MID-Verknüpfungen zuständig sein, wenn Daten aus einem Visumsantrag, der in der jeweiligen Auslandvertretung eingereicht wurde, zu einer MID-Verknüpfung mit Daten in einem anderen EU-Informationssystem führen. Nach aktuellem Wissensstand kann davon ausgegangen werden, dass der personelle Mehraufwand für die Konsularische Direktion und die Auslandsvertretungen departementsintern kompensiert werden kann. Die Unterstützung durch die MES entlastet die Auslandvertretungen in komplexen Fällen, die aufwändigere Abklärungen bedingen.

9.2 Auswirkungen auf Kantone

Die EU-Interoperabilitätsverordnungen werden es auch kantonalen Polizei- und Migrationsbehörden ermöglichen, stets über die für sie relevanten Informationen zu verfügen. Der zu erwartende Nutzen ist gross, ein gewisser Mehraufwand für die Kantone kann allerdings nicht ausgeschlossen werden.

9.2.1 Finanzielle und personelle Auswirkungen

Die Interoperabilität wird es auch kantonalen Polizei- und Migrationsbehörden ermöglichen, vorhandene Informationen effizienter und gezielter nutzen zu können. Das Risiko, dass Mehrfachidentitäten unerkannt bleiben, wird reduziert und die Anzahl Treffer erhöht. Es ist vorgesehen, dass die Polizeibehörden der Kantone und Gemeinden zur Identifizierung von Personen, die sich schon im Schengen-Raum befinden, auf die Daten im CIR zugreifen können. Bei ihrer Arbeit zur Verhütung, Ermittlung, Feststellung oder Verfolgung von terroristischen oder sonstigen schweren Straftaten werden die kantonalen Polizeibehörden vom Zugriff der Strafverfolgungsbehörden profitieren können. Damit können sie mittels einer Abfrage im CIR feststellen, ob Daten zu einer Person in einem der EU-Informationssysteme vorhanden sind. Als zentrale Zugangsstelle für Abfragen von Strafverfolgungsbehörden in nicht-polizeilichen Informationssystemen ist fedpol dafür zuständig, den Strafverfolgungsbehörden in einem zweiten Schritt den Zugang zu den benötigten Daten zu erteilen. Dieser Prozess wird bereits im Fall des VIS angewandt und ist für das EES vorgesehen.

Das ESP wird bei der Grenzkontrolle an den Schengen-Aussengrenzen zwingend zu nutzen sein. Nebst der EZV betrifft dies die kantonalen Polizeibehörden, welche für die Kontrolle der Schengen-Aussengrenzen zuständig sind. Sie werden MID-Verknüpfungen verifizieren, die EES-Daten betreffen. Dies stellt eine neue Aufgabe dar, die zu einem Mehraufwand führen wird. Die Unterstützung durch die MES entlastet die kantonalen Polizei- und Migrationsbehörden in komplexen Fällen, die aufwändigere Abklärungen bedingen.

Der Bund wird für die Verifizierung der MID-Verknüpfungen einen Client (nationale Komponente) zur Verfügung stellen. Die Einbindung dieses Clients in die entsprechenden kantonalen Systeme liegt in der Verantwortung der Kantone. Die Anbindung der nationalen Abfragesysteme ans ESP wird auch technische Anpassungen bei den kantonalen Abfragesystemen nötig machen. Diese Anpassungen liegen in der Zuständigkeit der Kantone. Weitere Anpassungen sind möglich, können aber zum jetzigen Zeitpunkt noch nicht abschliessend benannt werden. Die Kantone werden frühzeitig in Arbeitsgruppen einbezogen, um in der Umsetzung eine enge Zusammenarbeit zu gewährleisten.

9.2.2 Nationale Abfrageplattform

Die Interoperabilität auf EU-Ebene und die Motion Eichenberger[60] gaben in der Schweiz den Anstoss, auch die kantonalen Informationssysteme untereinander und mit denen des Bundes interoperabel zu machen. Es handelt sich bei der nationalen Abfrageplattform um ein von der Übernahme der EU-Interoperabilitätsverordnungen getrenntes Projekt unter der Führung der Kantone. Grundsätzlich haben die Kantone auf ihrem Hoheitsgebiet für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung zu sorgen. Ihre Zuständigkeit in Polizeiangelegenheiten ist vorrangig. Dem Bund sind einzelne polizeiliche Aufgabenbereiche übertragen. Mit einer nationalen Abfrageplattform sollen bei der Abfrage Synergien zwischen den nationalen und kantonalen Informationssystemen genutzt und die Suchresultate für die Benutzenden übersichtlicher und einheitlicher dargestellt werden. Im Rahmen der Harmonisierung der Schweizer Polizeiinformatik (Kompetenzzentrum Polizeitechnik und Informatik) wurde dazu ein Projekt initialisiert, da der Nutzen und die Machbarkeit einer nationalen Abfrageplattform klar gegeben sind. Das Projekt sieht voraussichtlich einen zentralen Betrieb der Abfrageplattform vor, während die Datenhaltung und der Betrieb der Informationssysteme weiterhin bei den jeweiligen Behörden bleiben soll. Die Zugriffsrechte der Behörden würden unverändert bleiben (vgl. Erläuterung zu Artikel 16*b* Abs. 5 E-BPI). Da das Projekt zur technischen Umsetzung der NAP erst initialisiert wurde, sind die technischen Vorgaben aktuell noch zu unbestimmt, um den rechtlichen Handlungsbedarf bestimmen zu können. Die rechtliche Grundlage der NAP wird zu einem späteren Zeitpunkt in einer separaten Vorlage vorgeschlagen.

9.3 Auswirkungen in weiteren Bereichen

In den Bereichen Volkswirtschaft, Gesellschaft und Umwelt sind keine direkten Auswirkungen zu erwarten. Durch die Interoperabilität wird sich die Sicherheit im Schengen-Raum erhöhen, was einen positiven Einfluss auf die Volkswirtschaft und die Gesellschaft hat.

10 Rechtliche Aspekte

10.1 Verfassungsmässigkeit

Die Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der EU-Interoperabilitätsverordnungen stützen sich auf Artikel 54 Absatz 1 BV. Demnach sind die auswärtigen Angelegenheiten Sache des Bundes. Gestützt auf Artikel 184 Absatz 2 BV unterzeichnet und ratifiziert der Bundesrat völkerrechtliche Verträge. Die Bundesversammlung ist nach Artikel 166 Absatz 2 BV für die Genehmigung völkerrechtlicher Verträge zuständig; ausgenommen sind die Verträge, für deren Abschluss auf Grund von Gesetz oder völkerrechtlichem Vertrag der Bundesrat zuständig ist. Auf eine solche Abschlusszuständigkeit kann sich der Bundesrat hier nicht berufen (vgl. Art. 7*a* Abs. 1 und 2 des Regierungs- und Verwal-

60 Motion 18.3592, Nationaler polizeilicher Datenaustausch.

tungsorganisationsgesetzes vom 21. März 1997[61] sowie Art. 24 Abs. 2 des Parlamentsgesetzes vom 13. Dezember 2002[62] [ParlG]). Dementsprechend ist die Bundesversammlung für die Genehmigung der beiden Notenaustausche zuständig.

10.2 Vereinbarkeit mit anderen internationalen Verpflichtungen der Schweiz

Mit der Übernahme der zwei Schengen-Weiterentwicklungen erfüllt die Schweiz ihre Verpflichtungen aus dem SAA. Sie trägt ausserdem zur uniformen Anwendung der Schengen/Dublin-Informationssysteme bei. Somit sind die Übernahme der beiden EU-Verordnungen und die damit verbundenen gesetzlichen Anpassungen mit den internationalen Verpflichtungen der Schweiz vereinbar.

10.3 Erlassform

Die Übernahme der zwei EU-Verordnungen stellt keinen Beitritt der Schweiz zu einer Organisation für kollektive Sicherheit oder zu einer supranationalen Gemeinschaft dar. Der Bundesbeschluss über die Genehmigung der entsprechenden Notenaustausche ist deshalb nicht dem obligatorischen Referendum nach Artikel 140 Absatz 1 Buchstabe b BV zu unterstellen.

Nach Artikel 141 Absatz 1 Buchstabe d Ziffer 3 BV unterliegen völkerrechtliche Verträge dem fakultativen Referendum, wenn sie wichtige rechtsetzende Bestimmungen enthalten oder wenn deren Umsetzung den Erlass von Bundesgesetzen erfordert. Nach Artikel 22 Absatz 4 ParlG sind unter rechtsetzenden Normen jene Bestimmungen zu verstehen, die in unmittelbar verbindlicher und generell-abstrakter Weise Pflichten auferlegen, Rechte verleihen oder Zuständigkeiten festlegen. Als wichtig gelten schliesslich Bestimmungen, die im innerstaatlichen Recht auf der Grundlage von Artikel 164 Absatz 1 BV in der Form eines Bundesgesetzes erlassen werden müssten.

Die vorliegend mittels Notenaustausch übernommenen EU-Verordnungen enthalten wichtige rechtsetzende Bestimmungen wie Abfrage- und Zugriffsrechte auf Informationssysteme. Die Übernahme bedingt zudem Anpassungen auf Gesetzesstufe (vgl. Ziff. 6.2). Demzufolge muss der Bundesbeschluss über die Übernahme der EU-Interoperabilitätsverordnungen dem fakultativen Referendum nach Artikel 141 Absatz 1 Buchstabe d Ziffer 3 BV unterstellt werden.

Die Bundesversammlung genehmigt völkerrechtliche Verträge, die dem Referendum unterliegen, in der Form eines Bundesbeschlusses (Art. 24 Abs. 3 ParlG).

Nach Artikel 141*a* Absatz 2 BV können die Gesetzesänderungen, die der Umsetzung eines völkerrechtlichen Vertrags dienen, der dem fakultativen Referendum untersteht, in den Genehmigungsbeschluss aufgenommen werden.

61 SR **172.010**
62 SR **171.10**

Die im Entwurf vorgeschlagenen Gesetzesbestimmungen dienen der Umsetzung der Rechtsgrundlagen für die Interoperabilität zwischen EU-Informationssystemen und ergeben sich unmittelbar aus den darin enthaltenen Verpflichtungen. Der Entwurf des Umsetzungserlasses kann deshalb in den Genehmigungsbeschluss aufgenommen werden.

10.4 Unterstellung unter die Ausgabenbremse

Mit der Vorlage werden keine neuen Verpflichtungskredite oder Zahlungsrahmen beschlossen, die einmalige Ausgaben von mehr als 20 Millionen Franken nach sich ziehen. Die Vorlage ist somit nicht der Ausgabenbremse (Art. 159 Abs. 3 Bst. b BV) unterstellt.

Abkürzungsverzeichnis

AIG	Ausländer- und Integrationsgesetz vom 16. Dezember 2005, SR *142.20*
AsyLex	Verein für Rechtsberatung zum Schweizer Asylrecht
BGIAA	Bundesgesetz vom 20. Juni 2003 über das Informationssystem für den Ausländer- und den Asylbereich, SR *142.51*
BPI	Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes, SR *361*
BV	Bundesverfassung, SR *101*
CIR	gemeinsamer Speicher für Identitätsdaten
COREPER	Ausschuss der Ständigen Vertreter der EU-Mitgliedstaaten
C-VIS	zentrales Visa-Informationssystem
DAA	Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags, SR *0.142.392.68*
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz, SR *235.1*
ECRIS-TCN	Europäisches Strafregisterinformationssystem für Drittstaatsangehörige (*European Criminal Records Information System on Third-Country Nationals*)
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EES	Europäisches Ein- und Ausreisesystem
EJPD	Eidgenössisches Justiz- und Polizeidepartement
ESP	Europäisches Suchportal
ETIAS	Europäisches Reiseinformations- und -genehmigungssystem
eu-LISA	Europäische Agentur für das Betriebsmanagement von IT-Grosssystemen im Raum der Freiheit, der Sicherheit und des Rechts
Eurodac	zentrale Datenbank der Europäischen Union, in der Fingerabdrücke von Personen gespeichert sind, die in

	einem Dublin-Staat ein Asylgesuch einreichen oder bei der illegalen Einreise aufgegriffen werden
Europol	Europäisches Polizeiamt
EZV	Eidgenössische Zollverwaltung
fedpol	Bundesamt für Polizei
FTE	Vollzeitstelle (*Full time equivalent*)
GS-EJPD	Generalsekretariat des Eidgenössischen Justiz- und Polizeidepartements
Interpol	Internationale Kriminalpolizeiliche Organisation (*International Criminal Police Organization*)
EU-Interoperabilitätsverordnungen	Verordnung (EU) 2019/817 (Verordnung «IOP Grenzen») und Verordnung (EU) 2019/818 (Verordnung «IOP Polizei»)
ISC-EJPD	Informatik Service Center des EJPD
i.V.m.	in Verbindung mit
LIBE-Ausschuss	Ausschuss des Europäischen Parlaments, der sich mit Fragen zu den Themen bürgerliche Freiheiten, Justiz und Inneres beschäftigt
MES	MID-Expertenstelle
MID	Detektor für Mehrfachidentitäten
NAP	Nationale Abfrageplattform
NDB	Nachrichtendienst des Bundes
N-SIS	nationaler Teil des Schengener Informationssystems
NUI	nationale Schnittstelle zwischen den nationalen Systemen der Schengen-Staaten und den EU-Zentralkomponenten (*National Uniform Interface*)
ORBIS	nationales Visumsystem
ParlG	Parlamentsgesetz vom 13. Dezember 2002, SR *171.10*
SAA	Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, SR *0.362.31*
sBMS	gemeinsamer Dienst für den Abgleich biometrischer Daten
SDSG	Schengen-Datenschutzgesetz vom 28. September 2018, SR *235.3*
SEM	Staatssekretariat für Migration

SFH	Schweizerische Flüchtlingshilfe
SGB	Schweizerischer Gewerkschaftsbund
SIRENE-Büro	nationale Kontaktstelle für alle Fahndungen via das SIS (SIRENE = *Supplementary Information Request at the National Entries*)
SIS	Schengener Informationssystem
SLTD	Interpol-Datenbank für gestohlene und verlorene Reisedokumente (*Stolen and Lost Travel Documents Database*)
SP	Sozialdemokratische Partei Schweiz
StGB	Strafgesetzbuch, SR *311.0*
TDAWN	Interpol-Datenbank zur Erfassung von Reisedokumenten, die Ausschreibungen zugeordnet sind (*Travel Documents Associated with Notices Database*)
Verordnung «IOP Grenzen»	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
Verordnung «IOP Polizei»	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
VG	Verantwortlichkeitsgesetz vom 14. März 1958, SR *170.32*
VIS	Visa-Informationssystem
VKM	Vereinigung der kantonalen Migrationsbehörden