19.xxx

Erläuternder Bericht

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

«Weiterentwicklung des Schengen-Besitzstands»

vom …

Übersicht

Die Interoperabilität wird den Informationsaustausch zwischen den verschiedenen EU-Informationssystemen ermöglichen. Mit einer Abfrage erhalten Grenzkontroll-, Migrations- und Strafverfolgungsbehörden künftig umfassende Informationen zu einer überprüften Person. Die Interoperabilität soll die Sicherheit im Schengen-Raum verbessern, effizientere Kontrollen an den Aussengrenzen ermöglichen und einen Beitrag zur Migrationssteuerung leisten. Der vorliegende Bericht führt die für die Übernahme und Umsetzung der 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 untereinander nicht verbunden. Um Informationen über eine Person zu erlangen, muss daher jedes Informationssystem separat abgefragt werden. Damit werden Synergien nicht genutzt. Wichtige Informationen können unentdeckt bleiben. 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 durchgeführt werden. Die Interoperabilität ermöglicht die Erkennung von Verknüpfungen zwischen bestehenden Daten. Die Zugriffsrechte der jeweiligen Behörden auf die einzelnen Systeme bleiben unverändert.

Die beiden EU-Interoperabilitätsverordnungen wurden der Schweiz am 21. Mai 2019 als Weiterentwicklungen des Schengen-Besitzstands notifiziert. Die Schweiz hat sich mit dem Schengen-Assoziierungsabkommen zur Übernahme aller Weiterentwicklungen des Schengen-Besitzstands verpflichtet. Innert zwei Jahren muss die Schweiz nun die rechtlichen Grundlagen für die Umsetzung der EU-Interoperabilitätsverordnungen schaffen.

Inhalt der Vorlage

Mit der Interoperabilität wird ein europäisches Suchportal geschaffen, das die gleichzeitige Abfrage in allen relevanten Informationssystemen ermöglicht. Die Interoperabilität sieht auch den automatisierten Abgleich biometrischer Daten einer Person vor, ermöglicht die Sammlung der biographischen und biometrischen Daten von Drittstaatsangehörigen in einem gemeinsamen Speicher und schafft neue Möglichkeiten, die wahre Identität von Personen aufzudecken, die in mehreren Informationssystemen unter falschen Identitäten oder Mehrfachidentitäten registriert sind.

In der Schweiz sind die Anpassung von Bundesgesetzen und deren Ausführungsrecht nötig, um die beiden EU-Verordnungen umzusetzen. Die Umsetzung der EU-Interoperabilitätsverordnungen ist mit einem finanziellen und personellen Mehraufwand für die Bundesverwaltung und die Kantone verbunden. Schweizer Systeme und

bestehende Prozesse müssen angepasst werden, um von den Möglichkeiten der Interoperabilität zu profitieren. Gleichzeitig soll ein nationales Abfrageinstrument bereitgestellt werden, um die Interoperabilität der nationalen und kantonalen Informationssysteme in der Schweiz zu verbessern und diese an das europäische Suchportal anzubinden.

Inhaltsverzeichnis

Erläuternder Bericht

1 Ausgangslage

1.1 Handlungsbedarf und Ziele

Die Schweiz hat sich mit dem Schengen-Assoziierungsabkommens (SAA)[1] 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.

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

- Die Verordnung (EU) 2019/817[2] betrifft den Bereich Grenzen und Visa (nachfolgend Verordnung «IOP Grenzen»).

- Die Verordnung (EU) 2019/818[3] betrifft den Bereich polizeiliche und justizielle Zusammenarbeit, Asyl und Migration (nachfolgend Verordnung «IOP Polizei»).

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. Allfällige Synergien können nicht genutzt werden und wichtige Informationen und Zusammenhänge können unentdeckt bleiben, wenn das Informationssystem, in dem sie erfasst sind, nicht abgefragt wird. Das Risiko besteht, dass die Behörden relevante Informationen verpassen. Folgendes Beispiel zeigt eine heute bestehende Sicherheitslücke und wie diese mit der Interoperabilität künftig geschlossen werden kann:

Eine kriminelle Person ist in der Schweiz im Schengener Informationssystem (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

1 SR **0.362.31**

2 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.

3 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.

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 Reisedokumenten und biometrische Daten (Fingerabdrücke und Gesichtsbilder) automatisiert abgeglichen und kriminelle Personen, welche falsche Identitäten benutzen, können identifiziert werden. Über das gemeinsame europäische Suchportal (ESP) können dann 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.[4]

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

Interoperabilität bedeutet also, die EU-Informationssysteme so miteinander zu vernetzen, dass vorhandene Informationen effizienter und gezielter genutzt werden können. Mittels einer Abfrage 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, so dass – in Situationen wie im vorher erwähnten Beispiel kein Visum an eine kriminelle Person ausgestellt wird. Zu diesem Zweck hat die EU zwei Verordnungstexte verabschiedet. Nebst der Schaffung des ESP sollen mit der Interoperabilität auch biometrische Daten (Fingerabdrücke und Gesichtsbilder) einer Person mit den Daten anderer Datenbanken automatisiert abgeglichen werden können. Weiter sollen Identitätsdaten und Reisedokumentdaten von Drittstaatsangehörigen in einer gemeinsamen Datenbank gespeichert werden. Schliesslich wird mit den beiden EU-Verordnungen die Möglichkeit geschaffen, Mehrfachidentitäten in den EU-Informationssystemen besser zu erkennen und Identitätsbetrug aufzudecken. Mit der Interoperabilität werden keine neuen Daten erhoben, sondern lediglich

[4] Unter «etc.» sind in der Grafik die Informationssysteme und Datenbanken zusammengefasst, zu denen die Schweiz momentan über keinen direkten Zugang verfügt, einen solchen jedoch zurzeit prüft (ECRIS-TCN) oder anstrebt (Europol-Daten, Interpol-Datenbanken).

zusätzliche Funktionen für die bestehenden und zukünftigen Informationssysteme geschaffen. Für die Behörden ändert sich dadurch nichts an den bestehenden Zugriffsrechten auf die zugrundeliegenden Systeme.

Die zwei EU-Verordnungen zur Interoperabilität wurden im Nachgang an die seit 2015 verübten terroristischen Anschläge im Schengen-Raum und die gesteigerten Herausforderungen im Migrationsbereich erarbeitet. Die Weiterentwicklung und der Ausbau der IT-Struktur der EU werden als zentrale Elemente zur Verbesserung der Sicherheit im Schengen-Raum angesehen. 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 Grenzkontroll-, Migrations- und Strafverfolgungsbehörden darstellt.

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 Weiterentwicklung fristgerecht zu übernehmen und die notwendigen rechtlichen Grundlagen für deren Umsetzung zu schaffen.

1.2 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 Juni 2018. 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 Kontrollen an den Aussengrenzen.
- Personeller Mehrbedarf: Wiederholt traktandiert war der zusätzliche Personalaufwand für die Schengen-Staaten und die Zusatzbelastung für bestehende Stellen wie die SIRENE-Büros[5].

5 SIRENE steht für «*Supplementary Information Request at the National Entries*». Jeder am Schengen-System teilnehmende Staat verfügt über ein nationales Büro, welches den Informationsaustausch und die Koordination des Vorgehens im Falle eines SIS-Treffers zuständig ist und rund um die Uhr operationell ist.

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

Der COREPER[6] definierte am 14. Juni 2018 die Verhandlungsrichtlinien für den Trilog mit dem Europäischen Parlament. Aufgrund von Nachbesserungen am ursprünglichen Kompromisstext hiess der COREPER die geänderten Texte am 12. September 2018 erneut gut und erteilte das Verhandlungsmandat für den Trilog. Der LIBE-Ausschuss[7] des Europäischen Parlaments verabschiedete seinen Bericht am 15. Oktober 2018. Der Trilog dauerte von Oktober 2018 bis Februar 2019 und wurde von technischen Meetings und Treffen der JI-Referenten begleitet. In den Trilogverhandlungen standen andere Themen im Vordergrund als zuvor auf Expertenstufe, beispielsweise der Zugriff auf den gemeinsamen Speicher für Identitätsdaten zu Identifikationszwecken bzw. zu Zwecken der Strafverfolgung oder die Informationspflicht der Staaten via Webportal. Auch die rechtliche Grundlage für eine Abfrage von Interpol Datenbanken als Teil der Interoperabilität war – und bleibt – Gegenstand von Diskussionen. Die offenen Fragen sollen in einem Abkommen zwischen der EU und Interpol geregelt werden. Die Experten der Schweiz haben an allen Sitzungen teilgenommen, konnten technische Fragen klären und ihre Lösungsvorschläge in allen Verhandlungsetappen einbringen.

Am letzten Trilog vom 5. Februar 2019 einigten sich die Rumänische Präsidentschaft und Vertreter des Europäischen Parlaments auf einen Kompromiss betreffend die Verordnungstexte. Die beiden Verordnungstexte wurden am 13. Februar 2019 vom COREPER und am 19. Februar 2019 vom LIBE-Ausschuss des Europäischen Parlamentes gutgeheissen. 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.

1.3 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

6 Ausschuss, der sich aus den Ständigen Vertretern der Regierungen der Mitgliedstaaten zusammensetzt und für die Vorbereitung der Arbeiten des Rates der EU zuständig ist.
7 Ausschuss des Europäischen Parlaments, der sich mit Fragen zu den Themen bürgerliche Freiheiten, Justiz und Inneres beschäftigt.

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. 7.1). 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[8]).

Ausgehend vom Datum der Notifikation durch die EU (21. Mai 2019) endet die Frist für die Übernahme und Umsetzung der EU-Verordnungen somit am 21. Mai 2021. Dabei ist zu bemerken, dass die übliche Zweijahresfrist pragmatisch verlängert wird,

8 Abkommen 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.

wenn die Anwendung des Rechtsakts innerhalb des Schengen-Raums erst ab einem späteren Datum vorgesehen ist. Dies ist bei einzelnen Zentralkomponenten der EU-Interoperabilitätsverordnungen der Fall, da sie zu einem unterschiedlichen Zeitpunkt in Betrieb genommen werden und die vollständige Umsetzung nicht vor 2023 geplant ist.

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

Die Vorlage ist weder in der Botschaft vom 27. Januar 2016[9] zur Legislaturplanung 2015–2019 noch im Bundesbeschluss vom 14. Juni 2016[10] über die Legislaturplanung 2015–2019 explizit angekündigt.

Die vorliegende Übernahme der Schengen-Weiterentwicklungen leistet aber einen Beitrag zur Umsetzung der Leitlinie 1, Ziel 4 sowie der Leitlinie 3, Ziele 13–15 für die Legislaturperiode 2015-2019. Mit der korrekten, 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 inneren und äusseren Sicherheitsbedrohungen kennen und über die notwendigen Instrumente verfügen, um diesen wirksam entgegenzutreten. Die Interoperabilität unterstützt dies, indem sie bestehende Sicherheitslücken schliesst und effizientere Kontrollen an den Aussengrenzen 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 Übernahme und Umsetzung der EU-Interoperabilitätsverordnungen stehen mit keiner Strategie des Bundesrats in Konflikt. Sie sind angezeigt, um den Verpflichtungen der Schweiz aus dem SAA nachzukommen.

2 Grundzüge der EU-Verordnungen

2.1 Übersicht

Die Interoperabilität schafft keine zusätzlichen Datenbanken, sondern integriert neue Funktionen in existierende und zukünftige Informationssysteme.

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

9 BBI **2016 1105**
10 BBI **2016 5183**

- das Europäische Suchportal (*European Search Portal*, nachfolgend „ESP“), das es den zuständigen Behörden erlaubt, 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 macht;
- der gemeinsame Speicher für Identitätsdaten (*Common Identity Repository*, nachfolgend „CIR“), der die Identitätsdaten (bspw. Name und Geburtsdatum), die Daten zu Reisedokumenten und die biometrischen Daten von Drittstaatenangehörigen enthält und deren Identifizierung erleichtert; und
- der Detektor für Mehrfachidentitäten (*Multiple Identity Detector*, nachfolgend „MID“) der Zusammenhänge zwischen neuen und bestehenden Daten in verschiedenen EU-Informationssystemen aufdeckt und so zur Bekämpfung von Identitätsbetrug beiträgt.

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

- 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 (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 Strafregisterauskünfte zwischen den EU-Staaten;
- das Einreise-/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 müssen, bevor sie in den Schengen-Raum einreisen;
- die Europol-Daten; 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 an den Informationssystemen SIS, VIS, Eurodac, EES und ETIAS, welche alle Teil des Schengen-Besitzstandes sind. Die EES-Verordnung und die ETIAS-Verordnung wurden der Schweiz 2018 als Weiterentwicklungen des Schengen-Besitzstandes notifiziert. Bis November 2020 hat die Schweiz auch die

Weiterentwicklungen des Schengen-Informationssystems (SIS) zu übernehmen, wodurch zusätzliche Möglichkeiten für die Polizei- und Migrationskooperation geschaffen werden, u.a. durch die Einführung einer neuen Rückkehrausschreibung.

Das ECRIS-TCN stellt hingegen keine Weiterentwicklung des Schengen-Besitzstandes dar und die Schweiz hat vorerst keinen Zugang dazu[11]. Es wird daher in den EU-Verordnungen von der Interoperabilität der «EU-Informationssysteme» gesprochen. Diese Formulierung wird im vorliegenden erläuternden Bericht für die Kapitel 1 bis 3 sowie 6 und 7 verwendet. 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[12]. Gegenwärtig laufen Diskussionen dazu, ob die EU den Schengen-assoziierten Staaten zukünftig via ESP einen direkten Zugang zu seinen 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 AIG und BPI schon die ESP-Zugriffsmöglichkeit auf die Europol-Datenbestände zu verankern. Auf die oben aufgeführten Interpol Datenbanken verfügt die Schweiz als Mitgliedstaat über einen Zugriff.

Die Interoperabilität ist in der EU in zwei Verordnungen geregelt. Die erste Verordnung betrifft die Bereiche Grenzen und Visa (Verordnung «IOP Grenzen»), die zweite die polizeiliche und justizielle Zusammenarbeit, Asyl und Migration (Verordnung «IOP Polizei»). Der Grund für die Regelung in zwei Verordnungen ist, dass sich die Bestimmungen an Staaten richten, die in unterschiedlichem Grad an Schengen teilnehmen. So betreffen beispielsweise die Systeme VIS, EES und ETIAS Teile des Schengen-Besitzstandes an dem Irland und das Vereinigte Königreich nicht teilnehmen. Die Schweiz hat entsprechend ihrer Teilnahme am Schengen-Besitzstand beide EU-Verordnungen zu übernehmen. Die beiden EU-Verordnungen sind bis auf wenige Bestimmungen deckungsgleich.

2.2 Inkraftsetzung 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, da die EU-Kommission über die stufenweise Inbetriebnahme der einzelnen Zentralkomponenten entscheidet, womit die jeweils einschlägigen Bestimmungen erst dann anwendbar werden (vgl. Art. 79 Verordnung «IOP Grenzen», Art. 75 Verordnung «IOP Polizei»). Voraussetzung für die Inbetriebnahme der einzelnen Zentralkomponenten ist beispielsweise der erfolgreiche Abschluss eines umfassenden

[11] Die Schweiz prüft derzeit eine mögliche Teilnahme an ECRIS-TCN.

[12] Basierend auf Artikel 8 und 9 des Abkommens zwischen der Schweiz und Europol von 2004 (SR 0.362.2) kann die Schweiz ein Ersuchen an Europol richten, um Informationen aus dem Europol Informationssystem (EIS) zu erhalten. Die Schweiz setzt sich für einen direkten Zugriff auf Europol-Daten ein.

Tests in Zusammenarbeit mit den Schengen-Staaten und den europäischen Agenturen der jeweiligen Zentralkomponente. Zusätzlich müssen die technischen und rechtlichen Vorkehrungen für die Erhebung und Übermittlung von Daten getroffen worden sein (Art. 72 Verordnung «IOP Grenzen», Art. 68 Verordnung «IOP Polizei»). Die einzelnen Zentralkomponenten werden folglich zu einem unterschiedlichen Zeitpunkt operativ werden. Gemäss heutigem Zeitplan der EU-Kommission sollen der sBMS bis 2021, der CIR bis 2022 und das ESP sowie der MID bis 2023 in Betrieb genommen werden. Es sind ausserdem verschiedene Übergangsphasen geplant, bevor die einzelnen Zentralkomponenten zur Anwendung kommen werden.

Unabhängig hiervon gelten einige Bestimmungen der beiden EU-Interoperabilitätsverordnungen bereits seit dem 11. Juni 2019. Dabei handelt es sich um Regelungen, die für die Entwicklungsphase relevant sind. Sie richten sich in erster Linie an die europäische Agentur eu-LISA, welche für die Entwicklung der verschiedenen Zentralkomponenten zuständig ist. Auch die Rechtsgrundlagen für den Erlass von verschiedenen Durchführungsrechtsakten, mit welchen die EU-Kommission zu einzelnen Regelungsaspekten präzisierende Bestimmungen festlegen wird, traten bereits im Juni 2019 in Kraft. Vor diesem Hintergrund besteht aus Sicht der Schweiz keine «besondere Dringlichkeit», die gestützt auf Artikel 7b des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[13] (RVOG) eine vorläufige Anwendung der beiden Notenaustausche notwendig machen würde.

Schliesslich ist in Artikel 79 der Verordnung «IOP Grenzen», respektive 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 gelten werden. Die Einbindung von Eurodac im Rahmen der Interoperabilität ist aber vorgesehen, deshalb wird Eurodac auch im Kapitel 3 erwähnt. Konkrete Bestimmungen fehlen allerdings noch. Die rechtliche Umsetzung in der Schweiz wird deshalb erst mit der Übernahme der neuen Eurodac Verordnung erfolgen.

3 Inhalt der EU-Verordnungen

Das folgende Kapitel gibt einen Überblick über den Inhalt der beiden EU-Verordnungen. Der Fokus liegt auf den vier Zentralkomponenten. Weitere Neuerungen, die ebenfalls Auswirkungen auf die Schweiz haben, werden in Kapitel 3.2 aufgeführt. Dies sind beispielsweise Bestimmungen zur Auskunftsplicht oder Datenqualitätsanforderungen sowie zu Änderungen, die an anderen Rechtsakten vorgenommen werden.

Da die beiden EU-Verordnungen bis auf wenige Bestimmungen deckungsgleich sind, wird in Kapitel 3 auf eine getrennte Darstellung verzichtet und der Inhalt als Ganzes präsentiert. Die angegeben 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.

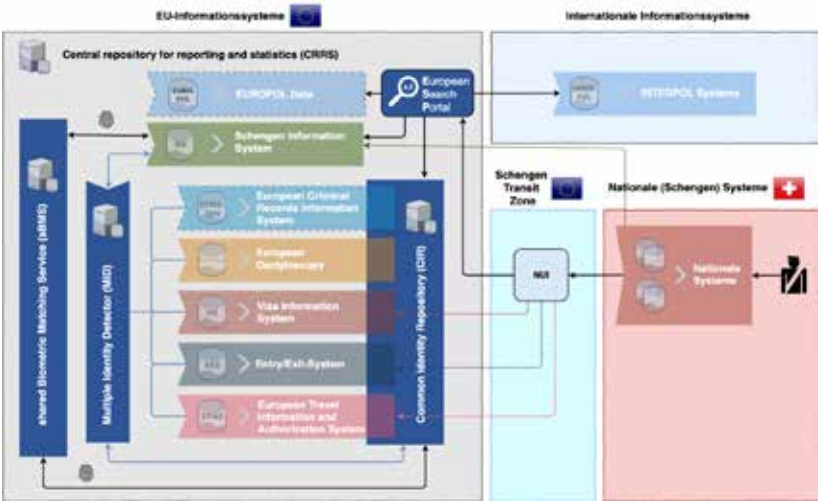
13 SR **172.010**

3.1 Die vier neuen Zentralkomponenten

Die vier neuen Zentralkomponenten bilden das Herzstück der Interoperabilität. Dank ihnen sollen die verschiedenen EU-Informationssysteme besser miteinander kommunizieren. Der Informationsaustausch wird dadurch effizienter, bestehende Sicherheitslücken werden geschlossen. Die verschiedenen Zentralkomponenten unterstützen 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 erfolgen als auch eine Abfrage der Daten im CIR, wo die Identitätsdaten, die Reisedokumentdaten und die biometrischen Daten aller Drittstaatsangehörigen, die in einem der nicht polizeilichen EU-Informationssysteme erfasst sind, gesammelt und gespeichert werden. Da die Daten von SIS nicht im CIR integriert sind, braucht es den MID, der dazu dient, innerhalb von CIR sowie zwischen CIR und SIS 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 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 Graphik 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 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.



3.1.1 Europäisches Suchportal (Kapitel II)

Die Schaffung des Europäischen Suchportals («ESP») ist ein zentraler Punkt der Interoperabilität. Es soll den zuständigen Behörden, nach Massgabe ihrer Zugangsrechte, einen raschen, unterbrechungsfreien, effizienten, systematischen und kontrollierten Zugang zu den verschiedenen EU-Informationssystemen, Europol-Daten und den 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 oder ECRIS-TCN), auf den CIR oder den MID, auf Europol-Daten oder Interpol-Datenbanken Zugriff haben, wenn das EU-Recht beziehungsweise das nationale Recht für sie entsprechende Zugriffsrechte auf die jeweiligen Systeme und/oder Zentralkomponenten vorsehen. Künftig nutzen die zuständigen Behörden der Schengen-Staaten sowie die Stellen der EU das ESP für Abfragen in EES, VIS, ETIAS, Eurodac oder ECRIS-TCN sowie für Abfragen im CIR für die in Artikel 20, 21 und 22 genannten Zwecke (für Abfragen im CIR siehe ausführlich Ziffer 3.1.3). Sie können das ESP auch für Abfragen im zentralen SIS (C-SIS)[14] sowie von Europol-Daten und Interpol-Datenbanken nutzen. Für die Behörden der Schengen-Staaten stellt dies keine Pflicht dar. Die Stellen der EU hingegen sind gehalten Abfragen im C-SIS künftig via ESP zu tätigen.

Erstellung von ESP-Nutzerprofilen (Art. 8)

In Zusammenarbeit mit den Schengen-Staaten erstellt die Agentur eu-LISA Nutzerprofile für alle Kategorien von ESP Nutzern. Jedes Profil enthält insbesondere die Informationen dazu, welche EU-Informationssysteme, Europol-Daten und Interpol-Datenbanken abgefragt werden dürfen. 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 Reisedokumenten oder biometrischer Daten erfolgen. Das ESP fragt entsprechend der Nutzerprofile gleichzeitig EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, CIR sowie Europol-Daten und Interpol-Datenbanken ab. Sobald aus einem der Systeme Daten verfügbar sind, werden diese den Nutzern im Rahmen ihrer Zugangsrechte über das ESP angezeigt.

14 Die Abfragen via ESP betreffen immer das zentrale SIS, das sich in Strassburg befindet. Es werde keine Abfragen in den nationalen Kopien durchgeführt.

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 betroffene Person erfasst ist (siehe Ziff. 3.1.3 zu Art. 20). Bei Abfragen des CIR nach Art. 22 wird den Strafverfolgungsbehörden lediglich angezeigt, ob Daten in einem Informationssystem vorhanden sind. Der Zugriff muss separat beantragt werden (siehe Ziff. 3.1.3 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 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 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 «IOP Grenzen» resp. Artikel 63 «IOP Polizei» ist geregelt, dass die Nutzung des ESP für zwei Jahre nach Inbetriebnahme der Zentralkomponente fakultativ ist. Diese Frist kann einmal um ein weiteres Jahr verlängert werden.

3.1.2 Gemeinsamer Dienst für den Abgleich biometrischer Daten (Kapitel III)

Der gemeinsame Dienst für den Abgleich biometrischer Daten („sBMS“[15]) soll die systemübergreifende Abfrage mehrerer EU-Informationssysteme mit biometrischen Daten ermöglichen (Art. 12).

[15] 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[16], die er aus den biometrischen Daten des EES, VIS, SIS und ECRIS-TCN sowie in Zukunft Eurodac, generiert. 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 einen Mindestdatenqualitätsstandard 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 in den Interoperabilitätsverordnungen sowie in den EU-Verordnungen zu den einzelnen Systemen genannten Zwecken erlaubt.

Datenspeicherung 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 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 3.1.1 zu Artikel 10 aufgeführt sind, gelten analog.

3.1.3 Gemeinsamer Speicher für Identitätsdaten (Kapitel IV)

Im gemeinsamen Speicher für Identitätsdaten („CIR“) wird für jede im EES, VIS, ETIAS, Eurodac oder ECRIS-TCN erfasste Person eine individuelle Datei angelegt. 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 seiner komplexen technischen Architektur, sind die Daten von SIS nicht Teil des CIR.

[16] Es handelt sich dabei um eine mathematische Repräsentation, die mittels Merkmalsauszug aus biometrischen Daten generiert wird, welche auf die für Identifizierungs- und Verifizierungszwecke erforderlichen Merkmale begrenzt sind (Art. 4 Abs. 12).

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

Der CIR speichert die Identitätsdaten, sowie, falls vorhanden, Daten zu Reisedokumenten und die biometrischen Daten aus EES, VIS, ETIAS, ECRIS-TCN und zu einem späteren Zeitpunkt auch aus Eurodac. Die Speicherung erfolgt dabei logisch voneinander getrennt und nach den Informationssystemen, aus welchen sie stammen. Für jeden im CIR gespeicherten Datensatz wird auch ein Verweis auf das EU-Informationssystem, aus dem er stammt, hinterlegt. Die Zugriffsrechte der Behörden auf den CIR richten sich dabei nach dem nationalen Recht, den Rechtsgrundlagen der jeweiligen EU-Informationssysteme sowie nach den in den EU-Interoperabilitätsverordnungen festgelegten Zugriffsrechten für die Zwecke nach Artikel 20, 21 und 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 siehe Ziffer 3.1.4) erstellt wird, die Daten aus dem CIR betrifft, werden keine neuen Dateien angelegt, sondern die neuen Daten der bestehenden individuellen Datei der verknüpften Daten hinzugefügt.

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

Der CIR soll die Identifizierung von Drittstaatenangehörigen erleichtern. Artikel 20 sieht deshalb vor, dass Polizeibeamte bei Kontrollen innerhalb eines Landes unter bestimmten Bedingungen die Identitätsdaten im CIR über eine Anfrage im ESP abfragen dürfen, um die betroffene Person zu identifizieren. 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 des Inhabers des Reisedokuments oder anderen Dokuments e) eine Person kann oder will 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 abgenommen 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, Unfällen oder Naturkatastrophen sowie nicht-identifizierter

menschlicher Überreste verwendet werden können. Schengen-Staaten, die diese beiden neuen Möglichkeiten nutzen wollen, müssen ihre nationalen Gesetze entsprechend anpassen und bestimmen, welche Behörden für die Abfrage berechtigt sind.

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

Zugang auf den CIR ist auch im Zusammenhang mit MID-Verknüpfungen vorgesehen (für Details dazu siehe Ziffer 3.1.4). 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 benannten Behörden, die von jedem Land entsprechend der Rechtsgrundlagen der einzelnen Systeme definiert werden, haben keinen direkten Zugriff auf die Daten im EES, VIS, ETIAS oder Eurodac, sondern müssen diese jeweils bei einer ebenfalls vom Land definierten zentralen Zugangsstelle beantragen.

Mit der Interoperabilität wird der Zugang der Strafverfolgungsbehörden 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, wenn Daten zu einer Person in einem der Systeme EES, ETIAS, VIS oder Eurodac vorhanden sind) so meldet der CIR den zuständigen Behörden in welchem EU-Informationssystem Daten vorhanden sind. Die benannten Behörden oder Europol haben anschliessend ein Gesuch auf uneingeschränkten Zugang auf mindestens eines der vom Treffer betroffenen EU-Informationssysteme zu stellen. D.h. bei benannten Behörden, dass diese ein Gesuch bei der zentralen Zugangsstelle einreichen müssen. Die Gewährung des vollständigen Zugangs auf die betroffenen Daten in 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 zu begründen und zu protokollieren.

Datenspeicherung im gemeinsamen Speicher für Identitätsdaten (Art. 23)

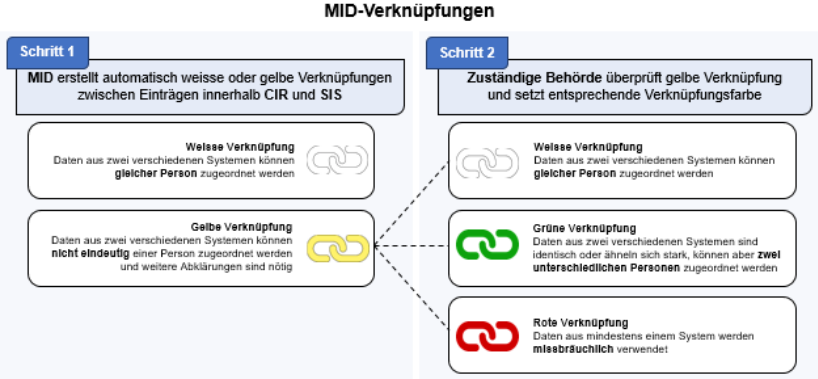
Die Daten im CIR werden automatisch, nach Massgabe der Datenspeicherungsbestimmungen des jeweiligen EU-Informationssystems aus dem sie stammen, gelöscht. Die individuellen Dateien im CIR werden nur solange gespeichert, wie die entsprechenden Daten in mindestens einem der EU-Informationssysteme gespeichert 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 gemäss Artikel 20, 21 und 22 zu führen, Europol über die Zugriffe gemäss Artikel 21 und 22. Die Bestimmungen zur Verwendung der Protokolle und der zu treffenden Sicherheitsmassnahmen, die in Ziffer 3.1.1 zu Artikel 10 aufgeführt sind, gelten analog.

3.1.4 Detektor für Mehrfachidentitäten (Kapitel V)

Der Detektor für Mehrfachidentitäten („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 erfassten Personendaten, Daten zu 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. Sprich, diese müssen die verschiedenen Identitäten prüfen und, je nachdem ob es sich um dieselbe oder eine andere Person handelt, die bereits in einem der EU-Informationssysteme verzeichnet ist, die Verknüpfung auf rot, grün oder weiss setzen. Die untenstehende Graphik 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 zu einem späteren Zeitpunkt Eurodac erfassen oder aktualisieren. Sie sind in den jeweiligen Rechtsgrundlagen der Informationssysteme definiert. Andererseits erhalten die Behörden der Schengen-Staaten und Stellen der EU Zugriff auf rote Verknüpfungen, wenn sie auf mindestens eines der betroffenen EU-Informationssysteme Zugriff haben, sowie auf weisse oder grüne Verknüpfungen, wenn sie 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 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, respektive das ESP zum Abgleich der Identitätsdaten und der Daten zu Reisedokumenten. Eine Prüfung auf Mehrfachidentitäten erfolgt nur, um Daten zwischen den verschiedenen EU-Informationssystemen abzugleichen. Eine derartige Prüfung innerhalb desselben Systems ist ausgeschlossen.

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 Daten, die zur Übereinstimmung geführt haben, 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. 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[17] der Verordnung (EU) 2018/1862[18] geprüft werden muss, ist das SIRENE-Büro des Schengen-Staates, der die Ausschreibung eingegeben hat, für die manuelle Verifizierung 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 Artikel 31, 32 und 32 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, was zum Beispiel bei einer Heirat mit Namenswechsel vorstellbar ist. 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 derselben

17 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.

18 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, ABI. L 312 vom 7.12.2018, S. 56.

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.

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 vorliegt. 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 anderen 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 Unionsrecht oder das nationale Recht möglich. Wird eine rote Verknüpfung zwischen Daten im EES, ETIAS, VIS, Eurodac oder 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 (siehe Ziff. 3.2) mitgeteilt). Die Behörde kann darauf verzichten, die Person zu informieren, 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 sicher zu stellen, 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.

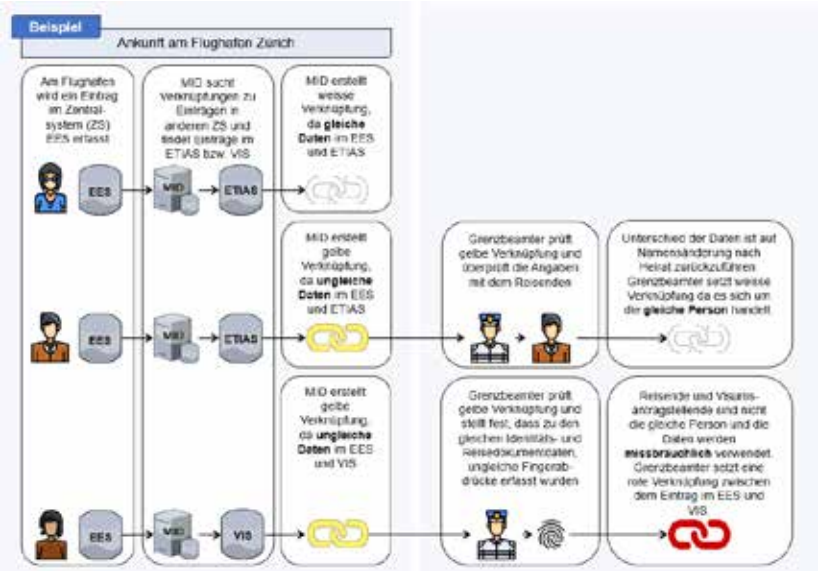
Weisse Verknüpfung (Art. 33)

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. Wird eine weisse Verknüpfung zwischen Daten im EES, ETIAS, VIS, Eurodac oder 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 und wo sie Informationen zu den Daten erhält (mittels Angabe der einmaligen Kennnummer und der Adresse des Webportals). 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 solange im MID gespeichert, wie die verknüpften Daten in zwei oder mehreren der zugrundeliegenden EU-Informationssystemen 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 3.1.1 zu Artikel 10 aufgeführt sind, gelten analog.

Übergangszeitraum für die Prüfung auf Mehrfachidentitäten

In Artikel 69 «IOP Grenzen», resp. Artikel 65 «IOP Polizei» ist der Übergangszeitraum für die Prüfung auf Mehrfachidentitäten geregelt. Nachdem der MID fertig entwickelt und erfolgreich getestet wurde, und bevor dieser für alle in Betrieb genommen wird, sollen alle bereits im EES, VIS, Eurodac und SIS vorhandenen Daten auf Mehrfachidentitäten geprüft werden. 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 sobald alle gelben Verknüpfungen geprüft und deren Status auf grün, weiss oder rot aktualisiert wurde, informiert die ETIAS-Zentralstelle die EU-Kommission, die danach über die effektive Inbetriebnahme des MID entscheidet. Die Prüfung sollte innerhalb eines Jahres abgeschlossen sein, eine Fristverlängerung ist möglich.

3.2 Weitere Bestimmungen

Die zwei EU-Verordnungen enthalten neben den Bestimmungen zu den vier neuen Zentralkomponenten, die den Hauptteil der EU-Interoperabilitätsverordnungen ausmachen, 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 ins Schweizer 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, Eurodac, ECRIS-TCN, ESP, CIR und MID verwendet werden und könnte auch von zukünftigen Informationssystemen genutzt werden. Für Analyse- und Statistikzwecke wird der 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 ganze 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 Austausch von Daten vorzusehen. Die Ahndung soll 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 hat die betroffen Person in einfacher und ihr verständlicher Sprache informiert zu 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 auf Berichtigung oder Löschung personenbezogener Daten bei einem Staat gestellt, der nicht für die manuelle Verifizierung verschiedener Identitäten zuständig ist, nimmt dieser mit dem zuständigen Schengen-Staat oder der ETIAS-Zentralstelle, falls diese für die Verifizierung zuständig ist, Kontakt auf, damit sie die Daten prüft. 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 Recht auf Auskunft und Berichtung, 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 des zuständigen Schengen-Staates ermittelt. Auf dem Webportal sind auch eine E-Mail-Vorlage für eine erleichterte Kommunikation sowie Informationen über Rechte und Verfahren enthalten.

Personendaten, die in den Zentralkomponenten gespeichert oder verarbeitet werden oder Daten, auf die über die Zentralkomponente zugegriffen 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 in den Rechtsgrundlagen der von der Interoperabilität betroffenen EU-Informationssysteme sowie die Abfrage von Interpol-Daten durch das ESP gemäss den EU-Interoperabilitätsverordnungen.

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 Artikel 54 und 55 sind die Verantwortlichkeiten 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, Eurodac, ECRIS-TCN nötig werden, sowie für die Kommunikationsinfrastruktur. Nach Inbetriebnahme garantiert sie 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 Verordnung «IOP Grenzen», Art. 58 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 Verordnungen, welche die Schweiz mittels Notenaustausch bereits übernommen hat bzw. für die derzeit das Übernahmeverfahren läuft. Es sind dies die Verordnung (EG) Nr. 767/2008 zu VIS, die Verordnung (EU) 2016/399 zum Schengener Grenzkodex, die Verordnung (EU) 2017/2226 zu EES, die Verordnung (EU) 2018/1240 zu ETIAS, die Verordnung (EU) 2018/1726 zu eu-LISA, die Verordnung (EU) 2018/1861 zu SIS, die Entscheidung 2004/512/EG betreffend die Einrichtung des VIS sowie der Beschluss 2008/633/JI betreffend den Zugang der Strafverfolgungsbehörden aufs VIS. Die Änderungen an diesen Rechtsakten werden in den Artikeln 58 bis 65 der Verordnung «IOP Grenzen» geregelt. Die Verordnung «IOP Polizei» führt in den Artikeln 59 bis 62 die Änderungen an der Verordnung (EU) 2018/1726 eu-LISA, der Verordnung (EU) 2018/1862 zu SIS und der Verordnung (EU) 2019/816 zu 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 der Aufgaben der verschiedenen Behörden, die dabei erfüllt werden müssen[19] (Art. 67 bis 69 «IOP Grenzen», resp. Art. 63 bis 65 «IOP Polizei»). Auch die Aufnahme des Betriebs (Art. 72 «IOP Grenzen», resp. Art. 68 «IOP Polizei»), die Schulung der zuständigen Behörden (Art. 76 «IOP Grenzen», resp. Art. 72 «IOP Polizei»), die Überwachung und Bewertung der Entwicklung und des Betriebs der Zentralkomponenten (Art. 78 «IOP Grenzen», resp. Art. 74 «IOP Polizei») sowie das Inkrafttreten (Art. 79 «IOP Grenzen», resp. Art. 75 «IOP Polizei») sind in diesem Kapitel geregelt.

4 Grundzüge des Umsetzungserlasses

4.1 Die beantragte Neuregelung

Bei der Vorlage handelt es sich um die Übernahme einer Weiterentwicklung des Schengen-Besitzstandes. Um deren Umsetzung in der Schweiz sicherzustellen, sind Anpassungen in Bundesgesetzen und später auch im zugehörigen Verordnungsrecht nötig (siehe Ziffer 4.3.1).

19 Deren Inhalt ist in den Kapiteln zu den einzelnen Zentralkomponenten unter Ziffer 3.1 wiedergegeben.

4.2 Abstimmung von Aufgaben und Finanzen

Die Umsetzung der EU-Interoperabilitätsverordnungen ist in der Schweiz mit finanziellem und personellem Aufwand bei der Bundesverwaltung und bei den Kantonen verbunden. Die in Kapitel 6 aufgeführten Aufwände sind jedoch im Zusammenhang mit dem zu erwartenden grossen Nutzen der neuen Möglichkeiten zu sehen, die durch die beiden EU-Interoperabilitätsverordnungen eingeführt werden. Vorhandene Informationen werden effizienter und gezielter genutzt werden können, was einen grossen Mehrwert für die Arbeit der Grenzkontroll-, Migrations- und Strafverfolgungsbehörden darstellt. Die Sicherheit im Schengen-Raum wird sich durch die Interoperabilität erhöhen.

4.3 Umsetzungsfragen

4.3.1 Rechtlicher Umsetzungsbedarf

Die Verordnungen «IOP Grenzen» und «IOP Polizei» enthalten sowohl direkt anwendbare Bestimmungen wie auch solche, die landesrechtlich konkretisiert werden müssen. 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 Zweckbindungsbestimmungen der EU-Informationssysteme geändert. 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 Ausländer- und Integrationsgesetz (AIG)[20] geregelt sind, sowie polizeiliche Datenbanken, die im Bundesgesetz über polizeiliche Informationssysteme des Bundes (BPI)[21] 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 von 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. 5 für die Erläuterungen zu den einzelnen Artikeln).

20 SR **142.20**
21 SR **361**

Ausländer- und Integrationsgesetz

Einige der im schweizerischen Recht umzusetzenden Bestimmungen bedingen Anpassungen im AIG.

Da es sich bei den im AIG geregelten Informationssystemen um Systeme handelt, die im Dublin-Assoziierungsabkommen geregelt sind und auch um Verwechslungen mit dem «Schengener Informationssystem 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 des 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 (zu ETIAS, EES, SIS, siehe dazu Ziff. 3.2), 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 von EES, ETIAS, VIS (und zu einem späteren Zeitpunkt 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 dass 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 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 des Bundesgesetzes vom 19. Juni 1992[22] über den Datenschutz (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 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.

22 SR **235.1**

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 zu 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 über das Informationssystem für den Ausländer- und den Asylbereich (BGIAA)[23] 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.

Verantwortlichkeitsgesetz

Das Verantwortlichkeitsgesetz (VG)[24] regelt in den Artikeln 19*a* und *b* aktuell das 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 eine Haftungsbestimmungen kennen, im Verantwortlichkeitsgesetz zu regeln. Der sBMS und das ESP stellen keine Zusammenstellung von Daten im Sinne von Art. 3 Bst. 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, wie einleitend ausgeführt wurde, auch das BPI anzupassen. Dieses regelt die Rechtsgrundlagen der bestehenden 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.

23 SR **142.51**
24 SR **170.32**

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

Da mehrere Artikel, welche die Datenbearbeitung in Schengen-Dublin-Informationssystemen betreffen, eingefügt werden sollen, drängt sich eine Anpassung der Systematik im BPI auf. Die Schengen-Dublin-Informationssysteme oder deren Komponenten sollen neu in einem separaten Abschnitt (neu 4. Abschnitt) geregelt werden. Sie werden der Reihenfolge ihrer voraussichtlichen Inbetriebnahme folgend, festgelegt (sBMS in Art. 18a, ESP in Art. 18b und MID in Art. 18c).

Mit der per 1. März 2019 in Kraft getretenen Umsetzung der Richtlinie (EU) 2016/680[25] regelt 349*c* StGB die Bekanntgabe von Personendaten an einen Drittstaat oder an ein internationales Organ.[26] Im Bundesgesetz vom 7. Oktober 1994[27] 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 Abs. 2 fest, dass sich die Bekanntgabe von Personendaten im Rahmen der Polizeizusammenarbeit mit ausländischen Strafverfolgungsbehörden nach den Artikeln 349a–349h des Strafgesetzbuchs StGB richtet.[28] Demgegenüber regelt das BPI generell die Nutzung polizeilicher Informationssystem des Bundes und wird mit der Umsetzung der vorliegend umzusetzenden EU-Verordnungen noch erweitert. Entsprechend ist in einer separaten Bestimmung die Datenbekanntgabe an Dritte und internationale Organisationen im Bereich der Interoperabilität festzulegen (Art. 18e). Weiter ist auch die Verantwortung für die Datenbearbeitung in den Schengen-Dublin-Informationssystemen oder deren Komponenten zu regeln (Art. 18f).

4.3.2 Geplante Evaluation des Vollzugs

Jeder Schengen-Staat wird mindestens alle fünf Jahre auf dessen Umsetzung und Anwendung des Schengen-Rechts evaluiert. Die Schweiz wurde bisher drei Mal evaluiert: 2008 im Hinblick auf die Aufnahme der operativen Zusammenarbeit, 2014 und 2018. Evaluiert werden jeweils die Bereiche Polizeikooperation, SIS/SIRENE, Aussengrenzen, Rückkehr, Datenschutz und Visa. Betroffen sind sowohl der Bund als auch die Kantone. Nach Abschluss der Ortsbesichtigungen erstellen die zuständigen Experten Evaluierungsberichte, worin sie allfällige Mängel aufzeigen können. Zur Behebung solcher Mängel kann der Rat der EU konkrete Empfehlungen an die Schweiz richten. Die Schweiz erstattet über allfällige Massnahmen, die sie aufgrund der Empfehlungen getroffen hat, gegenüber der EU Bericht. Bei künftigen Evaluationen wird auch die Umsetzung der EU-Interoperabilitätsverordnungen geprüft werden.

25 Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 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; Fassung gemäss ABl. L 119 vom 4.5.2016, S.89.

26 AS **2019** 625

27 SR **360**

28 AS **2019** 625

5 Erläuterungen zu einzelnen Artikeln des Umsetzungserlasses

5.1 Ausländer und Integrationsgesetz

Art. 5 Abs. 1 Bst. a^{bis} Fussnote

Da die Verordnung (EU) 2018/124029 zur ETIAS-Reisegenehmigung durch die Verordnung (EU) 2019/817 («IOP-Grenze») angepasst wird, ist die Fussnote in Artikel 5 Abs. 1 Bst. a^{bis} entsprechend anzupassen.

Diese Bestimmung ist zudem mit dem Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der EU betreffend die Übernahme der Verordnung (EU) 2018/1240 über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) (Weiterentwicklungen des Schengen-Besitzstands) [30] zu koordinieren.

Art. 7 Abs. 3 Fussnote

Da der Schengener Grenzkodex (SGK)[31] durch die Verordnung (EU) 2019/817 («IOP Grenzen») angepasst wird, ist die Fussnote in Artikel 7 Absatz 3 entsprechend anzupassen.

Diese Bestimmung ist zudem mit dem Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der EU betreffend die Übernahme der Verordnung (EU) 2018/1240 über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) (Weiterentwicklungen des Schengen-Besitzstands) zu koordinieren.

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.

29 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.

30 Zu dieser Vorlage wurde vom 13. Februar 2019 bis zum 20. Mai 2019 eine Vernehmlassung durchgeführt.

31 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; zuletzt geändert durch Verordnung (EU) 2019/817, ABl. L 135 vom 22.5.2019, S. 27.

Art. 68a Abs. 2 Fussnote

Da die Verordnung (EU) 2018/1861[32] durch die Verordnung (EU) 2019/818 («IOP Polizei») angepasst wird, ist die Fussnote in Artikel 68*a* Abs. 2 entsprechend anzupassen.

Diese Bestimmung ist zudem mit dem 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) (Verordnungen [EU] 2018/1862, 2018/1861 und 2018/1860) (Weiterentwicklungen des Schengen-Besitzstands) zu koordinieren[33].

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 1^{bis}, 2, 3, 3^{bis}, 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.

Datenschutz und Datenbearbeitung

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.
- Das 14*a*. Kapitel, soll neu alle Informationssysteme (SEM und Schengen) 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-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 in 14*a.* Kapitel integriert (eigener Abschnitt für Eurodac).

32 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, ABI. L 312 vom 7.12.2018, S. 14; zuletzt geändert durch Verordnung (EU) 2019/818, ABl. L 135 vom 22.5.2019, S. 85.

33 Zu dieser Vorlage wurde vom 13. Februar 2019 bis zum 20. Mai 2019 eine Vernehmlassung durchgeführt.

14. Kapitel: Datenbearbeitung und Datenschutz

Der Gliederungstitel von 14. Kapitel wird angepasst. Er regelt neu nur den Datenschutz und die Datenbearbeitung. 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* AIG (Bekanntgabe von Personendaten ans Ausland);
- 102*d* AIG (Bekanntgabe von Personendaten an den Heimat- oder Herkunftsstaat)
- 102*e* AIG (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 Artikel 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 Artikel 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 wird neu vor Artikel 103*a* AIG (INAD) eingefügt und befasst sich mit folgenden Informationssystemen:

- 1. Abschnitt (Informationssystem Einreiseverweigerungen, INAD): Art. 103*a* AIG;

- 2. Abschnitt (Einreise- und Ausreisesystem EES und automatisierte Grenzkontrolle): Art. 103*b* – 103*g* AIG;
- 3. Abschnitt (Passagier-Informationssystem, API-System): Art. 104*a* – 104*c* sowie 108 AIG (wobei Art. 108 AIG bereits aufgehoben ist);
- 4. Abschnitt (Europäisches Reiseinformations- und –genehmigungssystem ETIAS): Art. 108*a* – 108*g* und 109 AIG (wobei Art. 109 AIG bereits aufgehoben ist);
- 5. Abschnitt (Zentrales Visa-Informationssystem und nationales Visumsystem ORBIS): Art. 109*a* – 109*e* AIG*;*
- 6. Abschnitt Art. 109*f* – 109*j* AIG (Informationssystem für die Durchführung der Rückkehr[34]);
- 7. Abschnitt (Eurodac): Art. 109*k* AIG;
- 8. Abschnitt Personendossier- und Dokumentationssystem: Art. 109*m* AIG.

1. Abschnitt: Informationssystem Einreiseverweigerungen

Vor Artikel 103*a* wird neu ein Abschnitt eingefügt mit dem Titel «Informationssystem Einreiseverweigerungen».

Art. 103a

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 Einreise- und Ausreisesystem EES sowie zur automatisierten Grenzkontrolle.

Art. 103b Abs. 1 Fussnote, Abs. 2 Bst. a und b^{bis} und Abs. 4

Abs. 1 Fussnote

Da die Verordnung (EU) 2017/2226[35] zum Einreise- und Ausreisesystem (EES) durch die Verordnung (EU) 2019/817 («IOP Grenzen») angepasst wird, ist die Fussnote in Artikel 103*b* Absatz 1 entsprechend anzupassen.

34 AS **2019** 1413

35 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, S. 27.

Diese Bestimmung ist zudem mit dem Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der EU betreffend die Übernahme der Verordnung (EU) 2018/1240 über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) (Weiterentwicklungen des Schengen-Besitzstands) zu koordinieren.

Abs. 2 Bst. a und b^{bis}

In Buchstabe a von Artikel 103*b* Absatz 2 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 an den CIR (siehe hierzu Ausführungen zu Art. 110a) übermittelt und dort gespeichert werden. Die Identitätsdaten und die Daten zu 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 Übermittlung an den CIR ausgenommen; sie bleiben nach wie vor nur im EES gespeichert.

Art. 103d Sachüberschrift und Abs. 5

Da CIR neu ein Bestandteil von EES wird, gelten die Bestimmungen für die Bekanntgabe von EES-Daten auch für diejenigen EES-Daten, die im CIR gespeichert sind (Identitätsdaten, Daten zu Reisedokumenten und biometrische Daten). Aus diesem Grund ist die Sachüberschrift entsprechend mit «CIR» zu ergänzen. 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 Verordnungen (EU) 2019/817 und EU 2019/818 (vgl. Erläuterungen zu Art. 110*h* und Ziffer 3.2 Datenschutz).

Art. 104

Vgl. Kommentar zu Art. 92*a.*

3. Abschnitt: Passagier-Informationssystem (API-System)

Vor Artikel 104*a* wird ein neuer Abschnitt eingefügt. Der Abschnitt enthält Regelungen zum Passagier-Informationssystem API (Art. 104*a* bis 104*c*). Bei einzelnen Bestimmungen dieses Abschnittes müssen formelle Anpassungen vorgenommen werden. Materielle Änderungen gibt es keine.

Art. 104a Sachüberschrift und Abs. 1bis, 2, 3, 3bis, 4 und 5

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 Kapitel. 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: Europäisches Reiseinformations- und –genehmigungssystem ETIAS

Vor Artikel 108*a* wird ein neuer Abschnitt eingefügt. Der Abschnitt enthält Regelungen zum Europäischen Reiseinformations- und –genehmigungssystem ETIAS (Art. 108*a* bis 108*g*; Art. 109 ist bereits aufgehoben).

Art. 108a Abs.1 Bst. a und Abs. 3

Abs. 1 Bst. a

Buchstabe a von Absatz 1 wird dahingehend präzisiert, dass die Personendaten die Identitätsdaten und die Daten zu den Reisedokumenten darstellen. Diese werden neu im CIR gespeichert.

Abs. 3

Absatz 3 präzisiert, welche Daten an den CIR (siehe hierzu Ausführungen zu Art. 110*a*) übermittelt und dort gespeichert werden. Die Identitätsdaten und die Daten zu Reisedokumenten (Art. 108*a* Abs. 1 Bst. a) werden im CIR gespeichert. Die Informationen zu den bewilligten oder abgelehnten Gesuchen um eine ETIAS-Reisegenehmigung sowie die Daten der Überwachungsliste sind von einer Übermittlung an den CIR ausgenommen; sie bleiben nach wie vor nur im ETIAS gespeichert.

Art. 108f Sachüberschrift und Abs. 3

Da CIR neu ein Bestandteil von ETIAS wird, gelten die Bestimmungen für die Bekanntgabe von ETIAS-Daten auch für diejenigen ETIAS-Daten, die im CIR gespeichert sind (Identitätsdaten, Daten zu Reisedokumenten und biometrische Daten). Aus diesem Grund ist die Sachüberschrift «CIR» zu ergänzen. Hinsichtlich der Weitergabe von ETIAS-Daten, welche im CIR gespeichert sind, verweist Absatz 3 auf Artikel

110*h*. Dieser verweist wiederum auf Artikel 40 der beiden Verordnungen (EU) 2019/817 und EU 2019/818 (vgl. Erläuterungen zu Art. 110h und Ziffer 3.2 Datenschutz).

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

Vor Artikel 109*a* wird ein neuer Abschnitt eingefügt. Der Abschnitt enthält Regelungen zum zentralen Visa-Informationssystem und dem nationalen Visumsystem ORBIS (Art. 109*a* – 109*e* und Art. 109*f* – 109*j*; wobei die Art. 109*f* – 109*j* bereits aufgehoben sind).

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

Abs. 1 Fussnote

Da die Verordnung (EG) Nr. 767/2008[36] zum Visa-Informationssystem VIS durch die Verordnung (EU) 2019/817 («IOP Grenzen») angepasst wird, ist die Fussnote in Artikel 109*a* Absatz 1 entsprechend anzupassen.

Diese Bestimmung ist zudem mit dem Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der EU betreffend die Übernahme der Verordnung (EU) 2018/1240 über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) (Weiterentwicklungen des Schengen-Besitzstands) zu koordinieren.

Abs. 1bis

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

Art. 109b Sachüberschrift, Abs. 1, Abs. 2, Abs. 2bis, Abs. 3 und Fussnote

Mit der neuen Abschnittsüberschrift «Zentrales Visa-Informationssystem (C-VIS) und nationales Visumsystem ORBIS» wird der Begriff «ORBIS» für das nationale Visumsystem neu im AIG eingeführt. Entsprechend ersetzt der Begriff ORBIS in den nachfolgenden Bestimmungen den Begriff «nationales Visumsystem».

36 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, S. 27.

Art. 109c Sachüberschrift und Einleitungssatz

Vgl. Erläuterungen zu Artikel 109*b*

Art. 109d Fussnote

Die Fussnote muss aktualisiert werden.

6. 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 treten anfangs 2020 in Kraft. [37] Materielle Anpassungen der Bestimmungen gibt es keine.

7. 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 Reisedokumenten von in Eurodac erfassten Personen einschliessen. Jedoch gilt die Verordnung (EU) 2019/818 für Eurodac ab dem Tag der Anwendbarkeit der Neufassung der Verordnung (EU) Nr. 603/2013[38] (Art. 75 Verordnung [EU] 2019/818).

Art. 109l

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 Abschnitt 7.

8. Abschnitt: Personendossier- und Dokumentationssystem

Der bisherige Abschnitt 3 wird zu Abschnitt 8. Der Abschnitt enthält eine Bestimmung zum Personendossier und Dokumentationssystem des SEM.

Art. 109m

Dieser Artikel übernimmt den aktuellen Artikel 110 ohne materielle Änderungen.

37 AS **2019** 1413
38 ABl. L 180 vom 29.6.2013, S. 1.

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

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

Art. 110

Artikel 111 wurde mit der Änderung des AIG (Verfahrensregelungen und Informationssysteme) vom 14. Dezember 2018 aufgehoben.[39] Neu regelt Artikel 110 den gemeinsamen Dienst für den Abgleich biometrischer Daten(sBMS). Die Regelung vom geltenden Artikel 110 AIG ist nicht mehr notwendig und wird daher aufgehoben.

Abs. 1 und 3

Der sBMS ermöglicht mit Hilfe sogenannter «biometrischer Templates», bzw. biometrischer Merkmalsdaten aus den im CIR und SIS enthaltenen biometrischen Personendaten, die systemübergreifende Abfrage der von der Interoperabilität betroffenen Schengen-Dublin-Informationssysteme. Der Rückschluss vom Template auf die effektiven biometrischen Daten ist nicht möglich.

Der sBMS bildet eine der vier neuen Zentralkomponenten der Interoperabilität. Im Gegensatz zum CIR (Art. 110*a* ff. AIG) oder zum MID (Art. 110*g* AIG) handelt es sich jedoch 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 Ziffer 3.2.1).

Obwohl die Bestimmungen zum sBMS in den beiden EU–Verordnungen zur Interoperabilität 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.

Der sBMS enthält biometrische Merkmalsdaten auf der Grundlage der biometrischen Personendaten aus dem EES, dem VIS, Eurodac und dem SIS. ETIAS wird hier nicht aufgeführt, da in diesem Schengen-Dublin-Informationssystem keine biometrischen Personendaten gespeichert werden.

Abs. 2

Der entsprechende Verweis im sBMS 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 im Kapitel III der beiden EU-Verordnungen zur Interoperabilität (Verordnung [EU] 2019/817 und Verordnung [EU] 2019/818) enthalten. Ausführliche Informationen zum sBMS sind unter Ziffer 3.1.2 zu finden.

39 BBl **2018 7879**

2. Abschnitt: Gemeinsamer Speicher für Identitätsdaten (CIR)

Art. 110a Inhalt des Gemeinsamen Speichers für Identitätsdaten (CIR)

Abs. 1

Der CIR enthält für jede Person, welche im EES, im VIS im ETIAS oder zu einem späteren Zeitpunkt Eurodac erfasst ist, eine individuelle Datei mit ihren Identitätsdaten, Daten zu Reisedokumenten und biometrischen Daten aus diesen Schengen-Dublin-Informationssystemen. Die alphanumerischen Daten umfassen die Identitätsdaten der betroffenen Person und die Daten zu deren Reisedokumenten.

Der CIR soll die Identifizierung der Personen erleichtern, von denen Daten in den erwähnten Schengen-Informationssystemen enthalten sind und das Aufdecken von Mehrfachidentitäten unterstützen. Er soll auch den Zugang der benannten Behörden zu diesen Informationssystemen zur Verhütung, Aufdeckung oder Untersuchung terroristischer und anderer schwerer Straftaten erleichtern und vereinheitlichen. Die entsprechenden Zugriffsrechte werden in den Artikeln 110b – 110*d* AIG geregelt. Grundsätzlich wird zukünftig eine entsprechende Abfrage des CIR immer über das ESP (vgl. Art. 110*e* AIG) ausgelöst. Die Inbetriebnahme des CIR erfolgt gemäss aktueller Planung der Europäischen Kommission Mitte 2022, während das ESP erst Mitte 2023 betriebsbereit sein wird. Es muss entsprechend 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 3.1.3 zu finden.

Abs. 2

Der CIR enthält für jeden Satz der gespeicherten Identitätsdaten, Daten zu Reisedokumenten und biometrischen Daten einen Verweis auf das Schengen-Dublin-Informationssystem, aus welchem die entsprechenden Daten stammen sowie einen Verweis auf den tatsächlichen Datensatz in dem entsprechenden Schengen-Dublin-Informationssystem. Die Verweise dienen insbesondere einer Behörde, die keinen Zugriff auf das Schengen-Informationssystem hat, aus welchem die Daten ursprünglich stammen, dazu, bei der zuständigen zentralen Stelle die Herausgabe der notwendigen Daten zu beantragen.

Die detaillierten Regelungen zum CIR sind im Kapitel IV der beiden EU-Verordnungen zur Interoperabilität (Verordnung [EU] 2019/817 und Verordnung (EU) 2019/818) enthalten.

Art. 110b Abfrage des CIR zwecks Identifikation

Abs. 1 und 2

Gemäss Artikel 20 Absatz 1 der Verordnungen (EU) 2019/817 und (EU) 2019/818 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 des Inhabers eines Reisedokuments oder eines anderen glaubwürdigen Dokuments bestehen;
- 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 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

In Absatz 3 werden die Behörden genannt, welche im konkreten Einzelfall den CIR zur Identifikation von Ausländerinnen und Ausländern (Drittstaatsangehörigen) abfragen dürfen. Es sind dies fedpol, die Polizeibehörden der Kantone und Gemeinden sowie die Eidgenössische Zollverwaltung (EZV) zum Schutz der Bevölkerung und zur Wahrung der inneren Sicherheit. 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. Eine Abfrage darf ferner nur zu folgenden Zwecken erfolgen: zur Bekämpfung der illegalen Einwanderung, der Gewährleistung und Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie zum Schutz der inneren Sicherheit.

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 vorhandenerer 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. Ziffer 3.1.4) 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.

Abs. 2

Wenn bei der Abfrage des CIR eine rote Verknüpfung angezeigt wird (vgl. Ziffer 3.1.4), dürfen die Behörden, die auf der Grundlage des AIG oder des BPI Zugriff auf CIR, EES, ETIAS, C-VIS, Eurodac oder 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.

Art. 110d *Abfrage des CIR zwecks Verhütung Aufdeckung oder Ermittlung terroristischer Straftaten 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 der 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, in 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).

Abs. 3

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 1 den entsprechenden Verweis auf EES, VIS, ETIAS oder Eurodac an. Die entsprechende Antwort darf ausschliesslich zur Antragsstellung auf Zugang zu dem entsprechenden Schengen-Dublin-Informationssystem verwendet werden.

Abs. 4

Die Behörde nach Absatz 2 müssen sich mit der Antwort zwecks Antrag auf uneingeschränkten Zugang zu den Daten der betroffenen Person im entsprechenden Schengen-Dublin-Informationssystem an die Einsatzzentrale des fedpol wenden. 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 gleichzeitige, 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 Reisedokumenten und biometrischer Personendaten ist es möglich, mit dem ESP gleichzeitig das EES, das VIS, das ETIAS, Eurodac, SIS, die Interpol-Datenbanken SLTD und TDAWN sowie Europol-Daten abzufragen (Art. 6 ff. der Verordnungen [EU] 2019/817[40] und [EU] 2019/818[41]).

Eine Suche mittels ESP wird dann eingeleitet, wenn:

- Daten in eines der genannten Datenbanken eingegeben werden;
- 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 möglich für diejenigen Behörden, welche auf eine der genannten Datenbanken bereits zugriffsberechtigt sind (Art. 7 der Verordnungen [EU] 2019/817[42] und [EU] 2019/818[43]). Um die Nutzung des ESP zu ermöglichen, erstellt eu-LISA Kategorien von ESP-Nutzerprofilen, welche den Zugriffsberechtigungen Rechnung tragen (Art. 8 der Verordnungen [EU] 2019/817[44] und [EU] 2019/818[45]).

Es werden den Nutzern nur diejenigen Daten angezeigt, auf welche sie zugriffsberechtigt sind und die Verknüpfungen gemäss Artikel 30 – 33 der Verordnungen [EU]

40 Siehe Fussnote 2
41 Siehe Fussnote 3
42 Siehe Fussnote 2
43 Siehe Fussnote 3
44 Siehe Fussnote 2
45 Siehe Fussnote 3

2019/817[46] und [EU] 2019/818[47]. Es werden keine Angaben zu Daten geliefert, auf die der Nutzer nicht zugreifen darf (Art. 9. der Verordnungen (EU) 2019/817[48] und (EU) 2019/818[49])

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 (MID)

Der MID ist gleichzeitig ein Detektor und eine neue Datenbank, auf welche gewisse Behörden Zugriff haben. Der MID hat zum Ziel, die Identitätskontrollen zu erleichtern und den Identitätsbetrug zu bekämpfen.

Abs. 1

Absatz 1 übernimmt den Inhalt dieser Datenbank, wie in den EU-Verordnungen vorgesehen. Es handelt sich um Identitätsbestätigungsdateien nach Artikel 34 der Interoperabilitätsverordnungen. Deren Inhalte werden gleich lang gespeichert wie die damit verbundenen Daten in mindestens zwei der Schengen-Systeme (Art. 35 IOP Verordnung).

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 oder bei einer Aktualisierung im EES, VIS, ETIAS, oder wenn eine Ausschreibung im SIS erfasst oder aktualisiert wird, wird eine automatische Prüfung im CIR und im SIS ausgelöst.

Abs. 3

Dieser Absatz legt fest, wie die Überprüfung von Mehrfachidentitäten im Rahmen der Interoperabilität der verschiedenen Schengen-Informationssysteme abläuft. Der CIR, 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 Verordnungen). Das ESP ermöglicht eine Abfrage anhand der Identitätsdaten und Daten von Reisedokumenten (Art. 27, Ziffer 3 und 4 der Verordnungen). Die Überprüfung findet jeweils

46 Siehe Fussnote 2
47 Siehe Fussnote 3
48 Siehe Fussnote 2
49 Siehe Fussnote 3

statt nach der Erfassung oder Aktualisierung eines Dossiers in einem der verschiedenen Systeme (vgl. Art. 110*f*, Abs. 2).

Abs. 4

Dieser Absatz präzisiert den Inhalt des MID. Es handelt sich um die Verknüpfungen zwischen den Daten der verschiedenen Informationssysteme, welche mit derselben Person verbunden sind und möglicherweise zur selben Person gehören. Diese Verknüpfungen weisen insbesondere auf gerechtfertigt 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.

Die Identitätsbestätigungsdatei im MID nach Artikel 34 der Verordnungen (EU) 2019/817 und (EU) 2019/818 enthält folgende Angaben:

- die Art der Verknüpfung zwischen den Daten, sofern eine Übereinstimmung besteht (Art. 30 – 33 der Verordnungen (EU) 2019/817[50] und (EU) 2019/818[51]);
- den Verweis auf die Schengen-Dublin-Informationssysteme, aus denen die Daten gemäss Absatz 1 stammen;
- eine einmalige Kennnummer;
- die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde;
- sowie das Datum der Erstellung oder Aktualisierung der Verknüpfung.

110g Manuelle Verifizierung von Verknüpfungen 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 Ziffer 4 der Verordnungen). Zur Vornahme der manuellen Verifizierung, erhalten die dafür zuständigen Behörden (Art. 110*c*) Zugriff auf den MID haben. Die zuständigen Behörden stimmen mit denjenigen überein, welche zur Aufdeckung möglicher Mehrfachidentitäten auf den CIR zugreifen dürfen. Aus diesem Grund ist es angezeigt, auf den 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

50 Siehe Fussnoten zu Art. 110 Abs. 1
51 Siehe Fussnoten zu Art. 110 Abs. 1

die Wege leitet, indem sie ein Dossier erfasst oder Daten im C-VIS, im EES oder ETIAS aktualisiert. In Fällen in denen polizeiliche Ausschreibungen vorliegen, ist das SIRENE-Büro von fedpol die für die Verifizierung zuständige Behörde.

Abs. 3

Die Verifizierung von Mehrfachidentitäten wird in Anwesenheit der betroffenen Person durchgeführt (Art. 29 der Verordnung [EU] 2019/817). 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 unrechtsmässige Mehrfachidentität (rote Verknüpfung, Art. 32 der IOP-Verordnungen) entdeckt, oder sind die Daten einer Person rechtmässig in mehreren Schengen-Informationssystemen vorhanden (weisse Verknüpfung, Art. 33 der IOP-Verordnungen), 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 Ziffer 6 der IOP-Verordnungen).

5. Abschnitt: Datenbekanntgabe und Verantwortung für Datenbearbeitung

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

Grundsätzlich können 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 [EU] 2019/817 und 2019/818). Es handelt sich um den allgemeinen Artikel 111*d* AIG und die Artikel 103*d* 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 den verschiedenen Systemen, darin inbegriffen der Inhalt des CIR, in gewissen präzisen 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 Artikel 40 der beiden IOP-Verordnungen (EU) 2019/817 und (EU) 2019/818 (vgl. dazu Ziffer 3.2, Datenschutz).

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

Es bietet sich an, das aktuelle Kapitel 14*b* in 14*c* neu zu nummerieren. 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 die neue Artikel 109*l*, 111*a* und 111*d*. Er erfährt keine materielle Änderung.

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

Das Zugriffsrecht, welches im Artikel 111*f* vorgesehen ist, nimmt insbesondere Bezug auf das Bundesgesetz und die kantonalen Gesetze zum Datenschutz. Diese Bestimmung gilt ebenfalls für die Informationen, welche in den verschiedenen Schengen-Informationssystemen enthalten sind. Da dieser Artikel den Artikel 8 DSG übernimmt, wird dessen 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-Systeme und bezüglich der Interoperabilität betreffen, sind oder werden in den Anwendungsverordnungen konkretisiert. Daher werden die verschiedenen Datenschutzrechte in diesem Kapitel nicht aufgeführt.

Kapitel 14c Eurodac (aktuell)

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 120*d*, welcher im Rahmen der Projekte EES und ETIAS abgeändert wurde, muss im Hinblick auf die Interoperabilität erneut angepasst werden. 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-Systeme, welche nicht ausschliesslich in die Zuständigkeit des SEM fallen.

Absatz 1 wird neu in Artikel 101 Absatz 2 eingefügt. Er erfährt materiell keine Änderung.

Buchstabe a des Absatzes 2 sieht Bussen vor im Falle der zweckwidrigen Bearbeitung von Daten des C-VIS. Buchstabe b regelt dies für EES, Buchstabe c für ETIAS. Es bietet sich an, zwei Buchstaben d und e vorzusehen, welche die Bestimmungen für CIR und MID festlegen. Jede Datenbearbeitung, welche gegen die Artikel 110*a* bis 110*d*, 110*f oder* 110*g* E-AIG verstösst, ist mit einer Busse zu bestrafen, welche gemäss der Schweizerischen Strafordnung bis zu 10'000 Franken umfassen 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 92a.

Art. 122c Abs. 3 Bst. b

Vgl. Kommentar zu Artikel 92a.

Art. 126 Abs. 5

Vgl. Kommentar zu Artikel 102*e*.

5.2 Bundesgesetz über das Informationssystem für den Ausländer- und den Asylbereich (BGIAA) vom 20. Juni 2003

Art. 1 Abs. 2

Vgl. Kommentar zu Artikel 92*a*.

Art. 15 Bekanntgabe ins Ausland 111a-111d

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

5.3 Verantwortlichkeitsgesetz

Gliederungstitel Va. Abschnitt

Im Verantwortlichkeitsgesetz 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 das Abschnittes Va anzupassen und hat neu wie folgt zu lauten: *Va. Abschnitt: Haftung für Schäden im Zusammenhang mit dem Betrieb der Schengen-Dublin-Informationssysteme oder deren Komponenten*

Art. 19a

Artikel 19*a* des 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 Verordnung (EU) 2019/817, bzw. Verordnung (EU) 2019/818.

Entsprechend werden neu in die Bestimmung aufgenommen das EES (Bst. b), das VIS (Bst. c), das ETIAS (Bst. d), der CIR (Bst. e), das ESP (Bst. f), der MID (Bst. g) und Eurodac (Bst. h).

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 eines 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.

5.4 Bundesgesetz über die polizeilichen Informationssysteme des Bundes

Anpassung der Systematik

Im BPI sollen mehrere Artikel ergänzt werden, die Schengen-Dublin-Informationssysteme oder deren Komponenten regeln. Deswegen drängt sich eine Anpassung der Systematik auf. Die Schengen-Dublin-Informationssysteme und deren Komponenten sollen neu in einem separaten Abschnitt (4) nach den «nationalen» polizeilichen Informationssystemen geregelt werden.

Art. 2

Vorliegender Artikel zählt die Informationssysteme auf, die im BPI geregelt sind. Wie unter Ziffer 4.3.1 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 des Bundes (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, automatisiertes Polizeifahndungssystem (Art. 15): Neu Ziffer 2, Nationaler Polizeiindex (Art. 16): Neu Ziffer 3, Geschäfts- und Aktenverwaltungssystem des Bundesamtes für Polizei (fedpol; Art. 17): Neu Ziffer 4.

Als Schengen-Dublin-Informationssysteme und deren Komponenten werden in Buchstabe b erwähnt: Der nationale Teil des Schengener Informationssystems (N-SIS; Art. 18): neu Ziffer 1). Zu ergänzen sind ferner in den Ziffern 2 - 4 entsprechend ihrer voraussichtlichen Inbetriebnahme die Zentralkomponenten sBMS (geregelt in Art. 18a), das ESP (zu finden in Art. 18b) sowie der MID (in Art. 18c geregelt).

Art. 16, 17

Als Folge der Anpassung der Systematik sollen der Nationale Polizeiindex (aktuell geregelt in Art. 17) und das Geschäfts- und Aktenverwaltungssystem von fedpol (derzeit in Art. 18 geregelt) neu vor den «internationalen» Systemen in den Artikeln 16 und 17 ihre formell-gesetzliche Grundlage finden.

Neuer Gliederungstitel: 4. Abschnitt: Schengen-Dublin-Informationssysteme und deren Komponenten

Die Schengen-Dublin-Informationssysteme und deren Komponenten werden neu in einem separaten Abschnitt (4) geregelt. Deswegen ist ein entsprechender Gliederungstitel einzufügen.

Das SIS, das derzeit in Artikel 16 geregelt ist, findet seine formell-gesetzliche Grundalge neu in Artikel 18.

Art. 18a Gemeinsamer Dienst für den Abgleich biometrischer Daten (sBMS)

Da der sBMS auch ans SIS angeschlossen ist, soll er entsprechend Artikel 110 AIG auch im BPI geregelt werden. Dies geschieht in vorliegendem Artikel. Der sBMS wird, trotz direkter Anwendbarkeit der beiden Verordnungen (EU) 2019/817 und EU 2019/818, der Vollständigkeit halber ergänzt, sowie 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. 18b Europäisches Suchportal (ESP)

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

Abs. 1

Wie zu Artikel 110e AIG ausgeführt, wird es das ESP ermöglichen, mit nur einer einzigen Abfrage mittels Identitätsdaten, Daten zu Reisedokumenten oder biometrischer Personendaten alle einschlägigen Schengen-Dublin-Informationssysteme (SIS,

EES, VIS, ETIAS, Eurodac und CIR) und die Interpol-Datenbanken sowie Europol-Daten abzufragen.

Abs. 2

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

Abs. 3

Die Abfrage durch zugriffsberechtigte Behörden kann mittels Identitätsdaten, Daten zu 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 Online-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 noch festlegen. Diese Elemente werden auf Verordnungsstufe zu regeln sein.

Abs. 5

Es ist technisch geplant, für den Anschluss an das ESP eine «nationale Abfrageplattform» zu erstellen. An diese sollen auch polizeiliche Informationssysteme der Kantone angebunden werden, insoweit dies die beiden EU-Verordnungen zulassen. Derzeit ist aber technisch noch zu wenig bekannt, als dass dazu bereits eine detaillierte formell-gesetzliche Grundlage vorgesehen werden könnte. Diese wird zu einem späteren Zeitpunkt ergänzt.

Art. 18c Inhalt des Detektors für Mehrfachidentitäten (MID)

Auch der MID betrifft das SIS und soll neben dem AIG (Art. 110*f*) auch im BPI als Artikel 18c geregelt werden.

Abs. 1

Absatz 1 regelt die Zwecke des MID und seine Inhalte. 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, im EES, in ETIAS, im VIS, und später auch in Eurodac, Daten neu erfasst oder aktualisiert werden.

Abs. 3

Dieser Absatz erläutert, wie die automatisierte Prüfung auf Mehrfachidentität 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 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 (siehe Art. 34 der beiden Verordnungen (EU) 2019/817 und EU 2019/818) 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 18d 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 AIG).

Abs. 1

Die Zugriffsberechtigung dient der manuellen Verifizierung gelber Verknüpfungen (bei diesen ist noch keine manuelle Verifizierung erfolgt).

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 Eidgenössische Zollverwaltung (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 zu aktualisieren zu grün (Identitätsdaten der verknüpften Dateien gehören nicht zu derselben Person), rot (unrechtmässige Mehrfachidentität oder Identitätsbetrug liegt vor) oder 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 dies der erste Schengen-Staat ist.

Artikel 18e Bekanntgabe von Daten aus dem sBMS, dem CIR und dem MID

Vorliegender Artikel regelt die Bekanntgabe von Daten aus den Schengen-Dublin-Informationssystemen und deren Komponenten. Grundsätzlich dürfen die Daten nicht an Drittstaaten, internationale Organisationen oder private Stellen weitergegeben werden. Es gelten weiterhin die Vorschriften zur Datenbekanntgabe, welche für jedes System vorgesehen sind.

Artikel 18f *Verantwortung für die Datenbearbeitung im sBMS, dem CIR und dem MID*

Auch die Verantwortung für die Datenbearbeitung ist zu regeln. Sie richtet sich nach Artikel 40 der beiden Verordnungen (EU) 2019/817 und (EU) 2019/818.

6 Auswirkungen

6.1 Finanzielle und personelle Auswirkungen auf den Bund

Für fedpol und das SEM ergeben sich sowohl in der Projektphase als auch in der Anwendung der EU-Interoperabilitätsverordnungen finanzielle und personelle Auswirkungen. Diese werden nachfolgend separat dargelegt.

6.1.1 Projektkosten für fedpol und SEM

Bei fedpol wird die technische und organisatorische Umsetzung der EU-Interoperabilitätsverordnungen innerhalb des Projekts «Interoperabilität TO» koordiniert. Im Zentrum steht die Anbindung des nationalen Schengener-Informationssystem N-SIS an die neuen Zentralkomponenten CIR, MID und ESP. Aufgrund fehlender technischer Spezifikationen ist zurzeit noch nicht bekannt, wie die Komponenten der nationalen Infrastruktur aufgrund der Verifizierung von MID-Verknüpfungen angepasst werden müssen.

Beim SEM wird die Umsetzung der EU-Interoperabilitätsverordnungen im Projekt Interoperabilität SEM geführt. Es befasst sich mit übergeordneten technischen Themen, wie bspw. der gemeinsamen Nutzung neuer Systemkomponenten für die Schengen-Schnittstellen und mit organisatorischen Veränderungen. So ist mit neuen Prozessen unter Anwendung der vier neuen Zentralkomponenten zu rechnen, welche organisatorischen Einheiten zugeordnet werden müssen.

Fedpol und SEM koordinieren ihre Projekte zur technischen und organisatorischen Umsetzung der EU-Interoperabilitätsverordnungen sowohl auf strategischer als auch auf operativer Ebene. Um die Synergien zwischen den Projekten auf operativer Ebene zu nutzen, finden regelmässige Koordinationstreffen zwischen den beteiligten Programm- und Projektleitenden statt. Der Informationsaustausch wird, nebst dem direkten Kontakt, über gegenseitigen Zugriff auf die Projektplattformen gewährleistet. Die Interoperabilität gehört schliesslich zu den Vorhaben, die im Programm des GS EJPD «Weiterentwicklung des Schengen/Dublin-Besitzstandes» zusammengefasst sind. Im Rahmen dieses Programms werden die Vorhaben im Hinblick auf die Einhaltung der Termin-, Kosten- und Qualitätsvorgaben koordiniert. Übergeordnete strategische Fragen können im regelmässig tagenden strategischen Führungsausschuss behandelt werden.

Die Projekte befinden sich aktuell in der Initialisierungs- bzw. Konzeptphase. Die genaue Umsetzung der Anbindung an die Zentralkomponenten hängt unter anderem von deren Ausgestaltung durch die Agentur eu-LISA und von den technischen Besonderheiten ab. Die Entwicklung ist analog der gestaffelten Inbetriebnahme der Zentral-

komponenten durch die EU vorgesehen. Ende 2019 werden die ersten Durchführungsrechtsakte der EU zur Interoperabilität erwartet, womit für fedpol und das SEM mehr Details zur Umsetzung bekannt werden. Die aktuell veranschlagten Projektkosten basieren auf Schätzungen zum voraussichtlichen Aufwand.

In der Projektphase werden die nachfolgenden Auswirkungen erwartet:

Die Kosten für die Interoperabilitäts-Projekte von fedpol und SEM belaufen sich geschätzt auf 21.6 Millionen für den gesamten Zeitraum, respektive 14.1 Millionen für die Jahre 2020-2022. Die Finanzierung erfolgt über einen neuen Verpflichtungskredit zur Weiterentwicklung des Schengen/Dublin-Besitzstands, der über das Programm des GS-EJPD geführt wird. Die Botschaft zum Verpflichtungskredit wurde vom Bundesrat am 4. September 2019 ans Parlament überwiesen. Das Programm wird als IKT-Schlüsselprojekt geführt. Der Mittelbedarf für die Jahre 2020-2022 von 14.1 Millionen Franken fällt in die erste Tranche des Verpflichtungskredits und wird durch vom Bundesrat zugewiesene zentrale IKT-Mittel und über Eigenleistungen der betroffenen Ämter gedeckt.

Kosten 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	**8.3**	2.1	2.2	2.4	1.2	0.2	0.2
IOP Weiterentwicklung (SEM)	**2.0**					1.0	1.0
Total	**21.6**	**5.0**	**5.3**	**3.8**	**2.7**	**2.4**	**2.4**

Die Beträge entsprechen den Kosten aus der Botschaft zu einem Verpflichtungskredit zur Weiterentwicklung des Schengen/Dublin-Besitzstands, welche der Bundesrat am 4. September 2019 dem Parlament überwiesen hat.

Für fedpol verursacht die Umsetzung der Projektphase zwischen 2020 und 2023 voraussichtlich einen personellen Aufwand von 2800 Personentagen spezialisierte Ressourcen. Das SEM rechnet für dieselbe Zeitspanne mit 3960 Personentagen. Die entsprechenden personellen Mittel werden intern kompensiert. Die benötigten Ressourcen gemäss dieser Schätzung wurden dem ISC im August 2019 gemeldet. Nach vertiefter Analyse der Anforderungen durch das ISC können sich noch Anpassungen ergeben.

6.1.2 Anwendungs-, Betriebs- und Weiterentwicklungskosten für fedpol und SEM

Durch die Interoperabilität erhalten die zuständigen Behörden in Zukunft mehr Informationen. Es wird zu mehr Hits kommen, was wiederum zu mehr Fällen führen wird. Dadurch wird sich die Sicherheit im Schengen-Raum stark verbessern. Durch das erhöhte Fallaufkommen nimmt jedoch auch der Bearbeitungsaufwand zu. Auch kommt

mit der Verifizierung von MID-Verknüpfungen zur korrekten Identifizierung von Personen eine zusätzliche, neue Aufgabe auf die Behörden zu. Deshalb wird die Anwendung der Interoperabilitätsverordnungen sowohl bei fedpol als auch beim SEM zu einem personellen Mehrbedarf führen. Insbesondere die mit der Verifizierung von MID-Verknüpfungen verbundene Kontrolle biometrischer Daten wird zu einem personellen Mehrbedarf beim SIRENE-Büro, bei BiomID und Stellen des SEM führen. Der personelle Bedarf kann derzeit nicht verlässlich beziffert werden, wird aber in der Botschaft näher ausgeführt werden.

Die Mehrkosten für den technischen Betrieb ab Inbetriebnahme der Interoperabilität von rund 0,2 Millionen Franken werden durch Umpriorisierungen mit bestehenden Mitteln aufgefangen. Ein zusätzlicher finanzieller und personeller Bedarf wird bei der Erarbeitung der Botschaft zur Genehmigung und Umsetzung der EU-Interoperabilitätsverordnungen detailliert erhoben und entsprechend beantragt.

Die erwarteten technischen Weiterentwicklungen an den Zentralkomponenten ab der Inbetriebnahme der Interoperabilität bis 2025 verursachen voraussichtlich Investitionskosten von jährlich rund einer Million Franken und werden nach deren geplanter Betriebsaufnahme 2023 im Projekt IOP Weiterentwicklungen des SEM durchgeführt (z.B. am nationalen Zugriffsknoten). Zusätzliche Betriebskosten sind dadurch nicht zu erwarten.

6.1.3 Kosten für die EZV

Die vorliegende Weiterentwicklung hat finanzielle, prozessuale und personelle Auswirkungen auf die Eidgenössische Zollverwaltung (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 ergeben sollten, müssen ergänzend berücksichtigt werden.

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 Einsparungen durch eine höhere Automatisierung und die Aufwände durch die Aufdeckung von falschen Identitäten in etwa die Waage halten. Die personellen Auswirkungen beziehen sich auch auf Schulungs- und Ausbildungsmassnahmen.

Der finanzierungswirksame Mehraufwand für die Projektleitung und der Entwicklungsaufwand für die Anpassungen der mobilen und stationären Grenzkontrolllösungen dürfte sich 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.

6.2 Technische Auswirkungen

Aus der Übernahme und Umsetzung der EU-Interoperabilitätsverordnungen werden sich auch technische Auswirkungen ergeben.

Eine zusätzliche nationale Komponente soll die Anbindung der Schweizer Systeme an das ESP sicherstellen. Gleichzeitig soll dadurch die Interoperabilität der nationalen und kantonalen Polizeisysteme in der Schweiz verbessert werden. Diese soll Synergien zwischen den Informationssystemen nutzen und die Suchresultate für die Benutzenden übersichtlicher und schneller darstellen. In enger Zusammenarbeit prüfen fedpol und das SEM, ob dies mittels einer neuen nationalen Abfrageplattform realisiert werden kann, von der auch die Kantone profitieren könnten. Im Rahmen der Harmonisierung der Schweizer Polizeiinformatik (HPi) wurde dazu eine Vorstudie erstellt. Sie kommt zum Schluss, dass der Nutzen und die Machbarkeit einer nationalen Abfrageplattform klar gegeben sind. Die Studie empfiehlt einen zentralen Betrieb der Abfrageplattform, während die Datenhaltung und der Betrieb der Informationssysteme weiterhin bei den jeweiligen Behörden bleiben. Die Zugriffsrechte der Behörden bleiben unverändert. Diese nationale Komponente wird über den Verpflichtungskredit zur Weiterentwicklung des Schengen/Dublin-Besitzstands finanziert.

6.3 Auswirkungen auf Kantone und Gemeinden

Die vorliegenden EU-Verordnungen haben nicht nur Auswirkungen auf Bundesebene, sondern betreffen auch kantonale Polizei- und Migrationsbehörden.

Das ESP wird bei der Grenzkontrolle an den Schengen-Aussengrenzen zwingend zu nutzen sein, weshalb mit einem grösseren Aufwand bei den Grenzkontrollbehörden, insbesondere in der zweiten Kontrolllinie, zu rechnen ist. Da mehr Informationssysteme als früher gleichzeitig abgefragt werden, ist die Chance auf einen Treffer grösser. Die EZV und die für die Kontrolle der Schengen-Aussengrenzen verantwortlichen kantonalen Polizeibehörden müssen MID-Verknüpfungen prüfen. Dies stellt eine neue Aufgabe dar und kann, zusammen mit den Folgearbeiten, zu einem Mehraufwand führen. Das ESP kann aber auch von anderen Behörden wie Kantonspolizeien und kantonalen Migrationsbehörden genutzt werden. So 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. Dies wird die korrekte Identifizierung von Personen erleichtern. Bei ihrer Arbeit zur Verhütung, Ermittlung, Feststellung oder Verfolgung von schweren Straftaten oder Terrorismus werden die Kantonspolizeien auch durch das geplante neue Verfahren für den Zugriff der Strafverfolgungsbehörden profitieren können, da sie mittels einer Abfrage im CIR feststellen können, 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 den Zugang zu den benötigten Daten zu erteilen. Dieser Prozess wird bereits im Fall von VIS angewandt und ist im EES vorgesehen.

Aufgrund der Neuerungen der Interoperabilität ist mit Anpassungen verschiedener kantonaler Anwendungen zu rechnen. So wird bspw. die Anbindung der Schweizer Systeme ans ESP technische Anpassungen bei den kantonalen Abfragesystemen nötig machen. Weitere Anpassungen sind möglich, können aber zum jetzigen Zeitpunkt noch nicht abschliessend benannt werden.

Auch bei den operationellen Prozessen sind Anpassungen zu erwarten. Die Verifizierung von MID-Verknüpfungen stellt eine neue Aufgabe für die betroffenen Behörden dar. Diese Verknüpfungen sind das Resultat der Prüfung auf Mehrfachidentitäten, welche bei jeder Neuerfassung oder Änderung von Daten in einem der EU-Informationssysteme durchgeführt wird. Sobald die Abklärung biometrischer Daten nötig ist, wird dies auf Stufe fedpol (BiomID) zu erfolgen haben. Der Mehraufwand, der sich durch diese neue Aufgabe ergibt, lässt sich im Moment schwer abschätzen, da noch keine konkreten Zahlen zu den zu erwartenden Verknüpfungen vorliegen. Auch ist im Moment schwierig einzuschätzen, wie stark die Kantone von diesen Verifizierungen betroffen sein werden, da die konkreten Prozesse zur Verifizierung von MID-Verknüpfungen noch zu klären sind.

Dem zu erwartenden Mehraufwand ist der grosse Nutzen der Interoperabilität gegenüber zu stellen. Anstatt die Informationssysteme einzeln abzufragen, können Grenzkontroll-, Migrations-, und Strafverfolgungsbehörden mit der Interoperabilität künftig durch eine Abfrage eine Übersicht über die vorhandenen Daten zu einer Person erhalten. Die operativen Prozesse werden effizienter, da nicht jedes System einzeln abgefragt werden muss. Das Risiko, dass Daten unerkannt bleiben, wird reduziert und die Wahrscheinlichkeit eines Treffers erhöht. Vorhandene Informationen werden effizienter und gezielter genutzt werden können, was einen grossen Mehrwert für die Arbeit der Grenzkontroll-, Migrations- und Strafverfolgungsbehörden darstellt.

6.4 Auswirkungen in weiteren Bereichen

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

7 Rechtliche Aspekte

7.1 Verfassungsmässigkeit

Der Bundesbeschluss über die Genehmigung und Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Rechtsgrundlagen zur Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei (Verordnungen [EU] 2019/817 und 2019/818) stützt sich auf Artikel 54 Absatz 1 der Bundesverfassung[52] (BV). Demnach sind die auswärtigen Angelegenheiten Sache des Bundes. Gestützt auf Artikel 184 Absatz 2 BV unter-

52 SR **101**

zeichnet 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. 7a Abs. 1 und 2 [RVOG] sowie Art. 24 Abs. 2 des Bundesgesetzes vom 13. Dezember 2002[53] über die Bundesversammlung [ParlG]). Dementsprechend ist die Bundesversammlung für die Genehmigung der beiden Notenaustausche zuständig.

7.2 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 dem internationalen Recht vereinbar.

7.3 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. 3 vorstehend). Demzufolge muss der Bundesbeschluss über die Übernahme und Umsetzung der europäischen Rechtsgrundlagen für die Interoperabilität zwischen EU-Informationssystemen 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).

53 SR **171.10**

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.

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.

7.4 Besondere rechtliche Aspekte zum Umsetzungserlass

Delegationskompetenz an den Bundesrat nach Art. 110h AIG und Art. 22 BPI

Diese Kompetenzdelegation an den Bundesrat stützt sich auf Artikel 182 Absatz 1 BV, wonach der Bundesrat rechtsetzende Bestimmungen in der Form der Verordnung erlassen kann. Hierbei handelt es sich um rechtsetzende Bestimmungen, die zur Umsetzung der Rechtsvorschriften wie auch der EU-Interoperabilitätsverordnungen erforderlich sind.

Abkürzungsverzeichnis

CIR	Gemeinsamer Speicher für Identitätsdaten (*Common Identity Repository*)
COREPER	Ausschuss der Ständigen Vertreter der Mitgliedstaaten (*Comité des représentants permanents*)
ECRIS-TCN	Europäisches Strafregisterinformationssystem für Drittstaatsangehörige *(European Criminal Records Information System for third Country Nationals)*
EES	Einreise-/Ausreisesystem (*Entry-Exit System*)
ESP	Europäisches Suchportal (*European Search Portal*)
ETIAS	Europäisches Reiseinformations- und -genehmigungssystem *(European Travel Information and Authorisation System)*
eu-LISA	Europäische Agentur für das Betriebsmanagement von IT-Grosssystemen
Eurodac	Zentrale Datenbank für Fingerabdrücke von Asylsuchenden und Personen, die bei der illegalen Einreise aufgegriffen werden (*European Dactyloscopy*)
HPi	Harmonisierung der Schweizer Polizeiinformatik
IOP	Interoperabilität
IOP Grenzen	Verordnung (EU) 2019/817
IOP Polizei	Verordnung (EU) 2019/818
LIBE-Ausschuss	Ausschuss des Europäischen Parlaments, der sich mit Fragen zu den Themen bürgerliche Freiheiten, Justiz und Inneres beschäftigt (*Civil Liberties, Justice and Home Affairs*)
MID	Detektor für Mehrfachidentitäten (*Multiple Identity Detector*)
SAA	Schengen-Assoziierungsabkommen
sBMS	gemeinsamer Dienst für den Abgleich biometrischer Daten (*shared Biometric Matching Service*)
SIRENE-Büro	Zentrale Stelle, die für die Koordination und Bearbeitung aller SIS-Ausschreibungen zuständig ist (*Supplementary Information Request at the National Entry*)
SIS	Schengener Informationssystem *(Schengen Information System)*

SLTD	Interpol-Datenbank gestohlener und verlorener Reisedokumente (*Stolen and Lost Travel Documents Database*)
TDAWN	Interpol-Datenbank zur Erfassung von Ausschreibungen zugeordneten Reisedokumenten (*Travel Documents Associated with Notices*)
VIS	Visa-Informationssystem (*Visa Information System*)