Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei (fedpol)

Bern, November 2021

Verordnung über die Interoperabilität zwischen den Schengen/Dublin-Informationssystemen

N-IOP-Verordnung

Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens

Inhaltsübersicht

1. Ausgangslage 1

1.1. Allgemeines zur Interoperabilität 2
1.2. Notwendige Verordnungsanpassungen 2

2. Verordnung über die Interoperabilität zwischen den Schengen/Dublin-Informationssystemen 3

1. Abschnitt 3

Artikel 1 3
Artikel 2 3

2. Abschnitt 4

Artikel 3 4
Artikel 4 5
Artikel 5 5
Artikel 6 6
Artikel 7 7

3. Abschnitt 7

Artikel 8 7
Artikel 9 8
Artikel 10 8
Artikel 11 10
Artikel 12 11
Artikel 13 12
Artikel 14 13
Artikel 15 13
Artikel 16 14
Artikel 17 14

4. Abschnitt 15

Artikel 18 15
Artikel 19 16
Artikel 20 17

5. Abschnitt 17

Artikel 21 18
Artikel 22 18
Artikel 23 19
Artikel 24 20
Artikel 25 21
Artikel 26 22
Artikel 27 23
Artikel 28 23

6. Abschnitt 24

Artikel 29 24
Artikel 30 25

7. Abschnitt 26
Artikel 31 26
8. Abschnitt 26
3. Künftige Anpassungen weiterer Verordnungen 26
3.1. Verordnungen, die Schengen/Dublin-Informationssysteme regeln 26
3.2. Andere Verordnungen 27
4. Finanzielle und personelle Auswirkungen 27
4.1. Finanzielle und personelle Auswirkungen auf den Bund 27
4.2. Finanzielle und personelle Auswirkungen auf die Kantone 28
5. Rechtliche Aspekte 28
5.1. Verfassungsmässigkeit 28
5.2. Vereinbarkeit mit den internationalen Verpflichtungen der Schweiz 28
5.3. Erlassform 28
6. Datenschutz 29

1. Ausgangslage

Die Verordnungen (EU) 2019/817[1] und (EU) 2019/818[2] zur Herstellung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei wurden am 20. Mai 2019 vom Europäischen Parlament und vom Rat der EU verabschiedet und der Schweiz am 21. Mai 2019 als Weiterentwicklungen des Schengen-Besitzstands notifiziert. Die Schweiz verpflichtet sich mit dem Schengen-Assoziierungsabkommen (SAA; SR 0.362.31) grundsätzlich zur Übernahme aller Weiterentwicklungen des Schengen-Besitzstands. Der Bundesbeschluss über die Genehmigung und die Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Verordnungen (EU) 2019/817 und (EU) 2019/ 818 (nachfolgend: EU-IOP-Verordnungen) zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen wurde von der Bundesversammlung in der Frühlingssession 2021 verabschiedet. Die Referendumsfrist ist am 8. Juli 2021 unbenutzt abgelaufen. Die Umsetzung der beiden EU-IOP-Verordnungen bedingten auf Gesetzesstufe Anpassungen im Ausländer- und Integrationsgesetz (AIG), im Bundesgesetz über das Informationssystem für den Ausländer- und den Asylbereich (BGIAA), im Verantwortlichkeitsgesetz (VG) und im Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI).[3]

Mit dieser Vorlage werden die für die Umsetzung der Interoperabilität notwendigen Anpassungen auf Verordnungsstufe dem Bundesrat zur Genehmigung unterbreitet. Dies sind zum einen die zur Umsetzung der Gesetzesänderungen notwendigen Verordnungsanpassungen. Weiter bedürfen gewisse Bestimmungen der EU-IOP-Verordnungen einer Konkretisierung auf Verordnungsstufe. Zusätzlich sollen die der Schweiz bisher notifizierten tertiären Rechtsakte (Durchführungsbeschlüsse) zur Interoperabilität umgesetzt werden. Zu diesen Zwecken soll eine neue Verordnung über die Interoperabilität zwischen den Schengen-Dublin-Informationssystemen (N-IOP-Verordnung) geschaffen werden. Viele der auf Verordnungsebene festzulegenden Bestimmungen sind datenschutzrechtlicher Natur und betreffen die Konkretisierungen der Zugriffsrechte auf die

[1] Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates, ABl. L 135 vom 22.5.2019, S. 27; zuletzt geändert durch Verordnung (EU) 2021/1152, ABl. L 249 vom 14.7.2021, S. 15.

[2] Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816, ABl. L 135 vom 22.5.2019, S. 85; zuletzt geändert durch Verordnung (EU) 2021/1150, ABl L 249 vom 14.07.2021, S. 1

[3] Bundesbeschluss über die Genehmigung und die Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Verordnungen (EU) 2019/817 und (EU) 2019/ 818 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (Weiterentwicklungen des Schengen-Besitzstands), BBl 2021 674

Schengen-Dublin-Informationssysteme sowie die Aufbewahrung, Archivierung und Vernichtung der Daten.

1.1. Allgemeines zur Interoperabilität

Mit der Interoperabilität werden insbesondere vier Zentralkomponente eingeführt. So wird unter anderem ein Europäisches Suchportal (ESP) geschaffen, das die gleichzeitige Abfrage in allen beteiligten EU-Informationssystemen (Schengener Informationssystem [SIS], Fingerabdruck-Identifizierungssystem für den Abgleich der Fingerabdruckdaten aller Asylbewerber sowie von bestimmten Drittstaatsangehörigen und Staatenlosen [Eurodac], Visa-Informationssystem [VIS], Einreise- und Ausreisesystem [EES], Europäisches Reiseinformations- und -genehmigungssystem [ETIAS] und Europäisches Strafregisterinformationssystem für Drittstaatsangehörige [E-CRIS-TCN; keine Schengen/Dublin-Weiterentwicklung] sowie den Europol- und Interpol-Datenbanken ermöglicht. Ausserdem sieht die Interoperabilität die zentrale Speicherung der biometrischen und alphanumerischen Identitätsdaten im Gemeinsamen Speicher für Identitätsdaten (CIR) sowie einen gemeinsamen Dienst für den Abgleich biometrischer Daten (sBMS) vor. Zudem ermöglicht die Interoperabilität dank dem Detektor für Mehrfachidentitäten (MID) ein effizientes Aufdecken von Mehrfachidentitäten. Mit der Interoperabilität werden keine neuen Daten erhoben, sondern zusätzliche Funktionen für die bestehenden (SIS, VIS, Eurodac) und künftigen (EES, ETIAS, ECRIS-TCN) Informationssysteme geschaffen. In den EU-Verordnungen wird von der Interoperabilität der «EU-Informationssysteme» gesprochen. Was die rechtliche Umsetzung in der Schweiz angeht, wird hingegen der Begriff Interoperabilität der «Schengen/Dublin-Informationssysteme» verwendet, da nur diese im Schweizer Recht umgesetzt werden muss. Gemäss heutigem Zeitplan der EU-Kommission sollen der sBMS im Mai 2022, der CIR bis Mitte 2022 und das ESP sowie der MID voraussichtlich bis Mitte bzw. Ende 2023 in Betrieb genommen werden. Die Inbetriebnahme der Interoperabilität ist von der EU aktuell für Ende 2023/anfangs 2024 vorgesehen. Der genaue Zeitpunkt wird von der EU-Kommission zu einem späteren Zeitpunkt festgelegt. Um sicherzustellen, dass die Schweiz bei der Inbetriebnahme durch die EU technisch bereit ist, ist die Inkraftsetzung der N-IOP-Verordnung auf Ende 2022 geplant.

1.2. Notwendige Verordnungsanpassungen

Für die Herstellung der Interoperabilität zwischen den Schengen/Dublin-Informationssystemen müssen die neu einzuführenden vier Zentralkomponenten eine Verknüpfung herstellen zu den Informationssystemen, die insbesondere im AIG, sowie polizeilichen Datenbanken, die insbesondere im BPI geregelt sind. Aus Gründen der Transparenz wurden die Bestimmungen zu den Zentralkomponenten entsprechend in diesen beiden Gesetzen geregelt.

Die N-IOP-Verordnung soll unter anderem die neuen vier Zentralkomponenten umsetzen. Dar-

über hinaus werden in Zukunft auch punktuell Anpassungen in anderen Verordnungen vorzunehmen sein, die die Schengen/Dublin-Informationssysteme regeln, die von der Interoperabilität betroffen sind. Diese Änderungen sind jedoch nicht Teil dieser Vorlage und werden dem Bundesrat zu gegebener Zeit unterbreitet.

2. Verordnung über die Interoperabilität zwischen den Schengen/Dublin-Informationssystemen

Die N-IOP-Verordnung soll in acht Abschnitte unterteilt werden: Gegenstand und Begriffe (1. Abschnitt: Art. 1- 2), Gemeinsamer Dienst für den Abgleich biometrischer Daten (2. Abschnitt: Art. 3 - 7), Gemeinsamer Speicher für Identitätsdaten (3. Abschnitt: Art. 8 - 17), Europäisches Suchportal (4. Abschnitt: Art. 18 - 20), Detektor für Mehrfachidentitäten (5. Abschnitt: Art. 21 - 28), Rechte der betroffenen Personen (6. Abschnitt: Art. 29 - 30), Datensicherheit (7. Abschnitt: Art. 31) und Schlussbestimmungen (8. Abschnitt: Art. 32).

1. Abschnitt

Der 1. Abschnitt verschafft einen Überblick über den Regelungsgehalt zur Umsetzung der Interoperabilität zwischen den Schengen-Dublin-Informationssystemen nach den Artikeln 110 – 110*i* und Artikel 120*d* AIG, den Artikeln 16*a* – 16*f* BPI sowie den EU-IOP-Verordnungen.

Artikel 1

Artikel 1 führt den Gegenstand der N-IOP-Verordnung aus. Demnach regelt die N-IOP-Verordnung die Abfragerechte im ESP und MID (Bst. a), die Aktualisierung vom sBMS (Bst. b), die Abfragerechte des CIR (Bst. c), das Verfahren zur manuellen Verifizierung verschiedener Identitäten im MID (Bst. d), die Verantwortung für die Datenbearbeitung im MID, im CIR und sBMS (Bst. e), die Rechte der betroffenen Personen (Bst. f) sowie den Datenschutz und die Datensicherheit (Bst. g).

Artikel 2

Artikel 2 N-IOP-Verordnung legt die Begriffe fest, die in der Verordnung verwendet werden. Er unterteilt die im Rahmen einer Prüfung auf Mehrfachidentitäten sowie die nach einer Verifizierung durch die zuständige Behörde möglichen Verknüpfungen im MID in gelbe (Bst. a), grüne (Bst. b), rote (Bst. c) und weisse (Bst. d) Verknüpfungen und verweist für deren Definition auf die einschlägigen Bestimmungen der EU-IOP-Verordnungen (Art. 30-33), welche die verschiedenen Verknüpfungen ausführlich regeln. Hinsichtlich der Definition «terroristische Straftat» und «schwere Straftat» verweisen die EU-IOP-Verordnungen wie auch die EU-Rechtsgrundlagen zum SIS auf

die Richtlinie (EU) 2017/541[4] bzw. den Rahmenbeschluss 2002/584/JI[5]. Diese Begriffe, welche in Artikel 12 der N-IOP-Verordnung verwendet werden, werden in den Anhängen 1*a* und 1*b* der N-SIS-Verordnung (SR 362.0) näher ausgeführt. Entsprechend ist es angezeigt, in der vorliegenden Verordnung auf die Anhänge 1*a* und 1*b* der N-SIS-Verordnung zu verweisen (Bst. e und f). Die Straftatenkataloge wurden im Rahmen der Vorlage «Prüm Plus»[6] auf Gesetzesstufe geregelt. Anschliessend muss der Verweis in der vorliegenden Verordnung entsprechend angepasst werden.

2. Abschnitt

Der 2. Abschnitt enthält Bestimmungen zum sBMS. Der sBMS soll den systemübergreifenden Abgleich biometrischer Daten aus den Schengen/Dublin-Informationssystemen ermöglichen. Der sBMS speichert somit die biometrischen Templates, die er aus den biometrischen Daten des EES, C-VIS und SIS sowie in Zukunft von Eurodac generiert. Beim sBMS handelt es sich nicht um eine Datensammlung bzw. «Datenbank» im Sinne von Artikel 3 Buchstabe g des Bundesgesetzes über den Datenschutz (DSG, SR 235.1), da von den biometrischen Merkmalsdaten (sogenannte «Templates») keine Rückschlüsse auf die betroffenen Personen möglich sind. Anders als beim SIS und CIR erhalten Behörden keinen unmittelbaren Zugriff auf den sBMS. Da der sBMS – anders als der CIR – auch mit dem SIS verbunden ist, wurde sein Inhalt nicht nur im AIG (Art. 110 AIG), sondern auch im BPI geregelt (Art. 16*a* BPI). Der sBMS wurde trotz direkter Anwendbarkeit der Bestimmungen zum sBMS in den EU-IOP-Verordnungen der Vollständigkeit halber auch auf formell-gesetzlicher Stufe geregelt, damit einfacher auf ihn verwiesen werden kann.

Artikel 3

Artikel 3 N-IOP-Verordnung sieht vor, dass das SEM und fedpol die Verantwortung für die Datenverarbeitung im sBMS tragen. Rechtsgrundlage ist Artikel 40 Absatz 1 der EU-IOP-Verordnungen, der denjenigen mitgliedsstaatlichen Behörden die Verantwortung für die Verarbeitung von Daten im sBMS überträgt, die jeweils für die Verarbeitung im EES, im VIS und im SIS verantwortlich sind. Soweit es um Daten geht, deren Ursprung im EES und C-VIS zu finden sind, ist das SEM zuständig. Handelt es sich hingegen um Daten, die aus dem N-SIS stammen, ist fedpol verantwortlich.

---

[4] Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. L 88 vom 31.3.2017, S. 6

[5] Rahmenbeschluss des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten, ABl. L 190 vom 18.7.2002, S 1; zuletzt geändert durch Rahmenbeschluss 2009/299/JI, ABl. L 81 vom 27.3.2009, S. 24

[6] Prüm Plus besteht aus folgenden Abkommen: Prümer Abkommen, Genehmigung des Eurodac-Protokolls zwischen der Schweiz und der EU und Genehmigung des Abkommens mit den Vereinigten Staaten von Amerika sowie deren Umsetzung

Artikel 4

Artikel 4 Absatz 1 N-IOP-Verordnung führt die biometrischen Merkmalsdaten des sBMS aus. Demnach sind im sBMS die biometrischen Merkmalsdaten gespeichert, die aus den Fingerabdrücken und Gesichtsbildern generiert werden. Rechtsgrundlage hierfür ist Artikel 13 Absatz 1 der EU-IOP-Verordnungen, der die Speicherung biometrischer Merkmalsdaten im gemeinsamen Dienst für den Abgleich biometrischer Daten regelt. Dieser verweist wiederum auf die EU-Rechtsgrundlagen für das SIS (Daten nach Art. 20 Abs. 2 Bst. w und x, ausser Daten von Handflächenabdrücken der Verordnung (EU) 2018/1862[7] und Daten nach Art. 4 Abs. 1 Bst. u und v der Verordnung (EU) 2018/1860[8]), das EES (Daten nach Art. 16 Abs. 1 Bst. d, Art. 17 Abs. 1 Bst. b und c und Art. 18 Abs. 2 Bst. a, b und c der Verordnung 2017/2226[9]) und das VIS (Daten nach Art. 9 Nr. 6 der Verordnung (EG) 767/2008[10]). Auf die Nennung des Lichtbilds im Verordnungstext kann verzichtet werden. Zwar verweist Artikel 13 der EU-IOP-Verordnungen auf die Bestimmungen der einzelnen Systeme bezüglich derjenigen Daten, aus welchen die Templates für das sBMS generiert werden. Im Artikel 20 Absatz 2 Buchstabe w der Verordnung (EU) 2018/1862 (SIS Polizei) sowie Verordnung (EU) 2018/1861 (SIS Grenze) werden neben den Gesichtsbildern auch Lichtbilder genannt. Allerdings wird es seitens EU noch mehrere Jahre dauern, bis Lichtbilder im sBMS enthalten sein werden. Entsprechend kann derzeit auf deren Aufnahme in der N-IOP-Verordnung verzichtet werden.

Artikel 4 Absatz 2 N-IOP-Verordnung sieht vor, dass die biometrischen Merkmalsdaten im sBMS logisch voneinander getrennt nach den Informationssystemen, aus denen sie stammen, gespeichert werden. Dies ergibt sich aus Artikel 13 Absatz 1 der EU-IOP-Verordnungen.

Artikel 5

Artikel 5 Absatz 1 N-IOP-Verordnung führt aus, dass der sBMS immer dann einen automatisierten Datenabgleich über die im CIR und SIS erfassten biometrischen Daten vornimmt, wenn im EES,

---

[7] Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission, ABl L 312 vom 7.12.2018, S. 56; zuletzt geändert durch Verordnung (EU) 2021/1150, ABl. L 249 vom 14.7.2021, S. 1

[8] Verordnung (EU) 2018/1860 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger, ABl L 312 vom 7.12.2018, S. 1; zuletzt geändert durch Verordnung (EU) 2021/1152, ABl. L 249 vom 14.7.2021, S. 15

[9] 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) 2021/1152, ABl. L 249 vom 14.7.2021, S. 15

[10] 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) 2021/1152, ABl. L 249 vom 14.7.2021, S. 15

im C-VIS, im Eurodac oder im SIS neue Datensätze angelegt oder aktualisiert werden. Der sBMS generiert die Templates somit basierend auf den biometrischen Daten im SIS und CIR. Die entsprechenden Angaben im CIR stammen aus dem SIS, dem EES, dem C-VIS und Eurodac (ausgenommen ist ETIAS, da darin keine biometrischen Daten gespeichert sind). Detaillierte Regelungen zum sBMS sind in Kapitel III der beiden EU-IOP-Verordnungen enthalten. Die biometrischen Templates dürfen erst in den sBMS eingegeben werden, nachdem der sBMS die einem der Schengen/Dublin-Informationssysteme hinzugefügten biometrischen Daten einer automatischen Qualitätskontrolle unterzogen hat, um sicherzustellen, dass ein Mindestdatenqualitätsstandard eingehalten wird. Dieses Erfordernis ergibt sich aus Artikel 13 Absatz 3 der beiden EU-IOP-Verordnungen. Der Abgleich erfolgt gemäss dem Anhang des Durchführungsbeschlusses zu Artikel 13 Absatz 5 der beiden EU-IOP-Verordnungen entweder als «Eins-zu-eins-Abgleich» oder «Eins-zu-vielen-Abgleich».[11] Der «Eins-zu-eins-Abgleich» führt einen Verifikationsprozess durch, der zwei biometrische Datensätze miteinander vergleicht. Demgegenüber wird beim «Eins-zu-vielen-Abgleich» das aus den biometrischen Eingabedaten extrahierte Template mit den in der Datenbank des sBMS gespeicherten Templates verglichen.

Artikel 5 Absatz 2 N-IOP-Verordnung legt fest, dass die Abfragen anhand biometrischer Daten zu den Zwecken nach Artikel 14 der beiden EU-IOP-Verordnungen erfolgt. Diesbezüglich verweist Artikel 14 wiederum auf die Rechtsgrundlagen für das SIS, das EES und das VIS, also auf die Verordnungen (EG) Nr. 767/2008, (EU) 2017/2226, (EU) 2018/1860, (EU) 2018/1861, (EU) 2018/1862 und (EU) 2019/816, ohne diese genauer zu spezifizieren.

Artikel 6

In *Artikel 6* N-IOP-Verordnung wird festgehalten, dass sich die Speicherungsdauer der biometrischen Merkmalsdaten sowie der dazugehörigen Verweise im sBMS nach der Speicherung der biometrischen Daten im SIS und im CIR richtet. So werden im sBMS die biometrischen Templates gespeichert, die er aus den biometrischen Daten des SIS, EES, C-VIS und Eurodac generiert. Der CIR stellt einen Bestandteil der drei letztgenannten Systeme dar. Zudem enthält jedes Template einen Verweis auf das EU-Informationssystem, aus dem es stammt, sowie einen Verweis auf die darin enthaltenen Datensätze. Eine Löschung der biometrischen Daten im SIS oder im CIR hat auch die automatische Löschung der Daten im sBMS zur Folge. Die Bestimmung wird in Umsetzung von Artikel 15 EU-IOP-Verordnungen aufgenommen.

[11] Anhang des Durchführungsbeschlusses der Kommission vom 26.8.2021 zur Feststellung der Leistungsanforderungen und praktischen Vorkehrungen für die Überwachung der Leistung des gemeinsamen Dienstes für den Abgleich biometrischer Daten gemäss Artikel 13 Absatz 5 der Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates, C(2021) 6159 final

Artikel 7

Artikel 7 N-IOP-Verordnung regelt die Protokollierung. Er stellt klar, dass jede Abfrage der biometrischen Templates im sBMS in einem Protokoll festzuhalten ist. Die Protokollierung soll durch den Bund erfolgen, wobei dort diejenige Behörde zuständig ist, die das zugrundeliegende Schengen/Dublin-Informationssystem abfragt. Die Verpflichtung der Schengen/Dublin-Staaten, Protokolle zu erstellen, ergibt sich aus Artikel 16 Absatz 2 der EU-IOP-Verordnungen. Artikel 7 N-IOP-Verordnung legt demnach fest, dass folgende Informationen zu protokollieren sind: die abfragende Behörde (Bst. a), die abgefragten Schengen/Dublin-Informationssysteme (Bst. b), das Datum und die Uhrzeit der Abfrage (Bst. c), die für die Abfrage verwendeten biometrischen Daten (Bst. d) und die Abfrageergebnisse (Bst. e). Die Protokollierung dieser Informationen stellt sicher, dass die durch den 6. Abschnitt der vorliegenden Verordnung eingeräumten Rechte der betroffenen Personen effektiv wahrgenommen werden können. Biometrische Daten im Sinne von Buchstabe d sind diejenigen Daten, die zur Abfrage verwendet wurden, wie z.B. Fingerabdrücke. Die Abfrageergebnisse im Sinne von Buchstabe e enthalten die biometrischen Merkmalsdaten.

3. Abschnitt

Der 3. Abschnitt enthält Bestimmungen zum CIR. Im CIR wird für jede im EES, C-VIS, ETIAS oder in Eurodac erfasste Person eine individuelle Datei mit – sofern vorhanden – ihren Identitätsdaten, Daten zu den Reisedokumenten und biometrischen Daten aus diesen Schengen/Dublin-Informationssystemen angelegt. Der CIR ersetzt jeweils insofern einen Teil des Zentralsystems der verschiedenen Schengen/Dublin-Informationssysteme (C-VIS, Eurodac, EES und ETIAS), als im CIR gewisse alphanummerische (Identitätsdaten und Daten zu den Reisedokumenten) und biometrische Daten dieser Informationssysteme gespeichert werden. Der CIR stellt damit einen Bestandteil dieser Systeme dar. SIS-Daten werden nicht im CIR gespeichert werden, da sich dafür die Architektur des SIS als zu komplex erwiesen hat. Der CIR soll unter anderem die korrekte Identifizierung von Personen, die in einem der genannten EU-Informationssysteme erfasst sind, gemäss Artikel 20 der EU-IOP-Verordnungen erleichtern und unterstützen (Art. 17 Abs. 1 der EU-IOP-Verordnungen). Als nationale Rechtsgrundlage des CIR dient das AIG. Im AIG wurde geregelt, welche Daten im Zentralsystem des jeweiligen Informationssystems gespeichert bleiben und welche Daten neu im CIR-Teil gespeichert werden. Die entsprechenden Regelungen finden sich in den Artikeln 110*a*-110*d* AIG.

Artikel 8

Artikel 8 N-IOP-Verordnung hält fest, dass das SEM die Verantwortung für die Datenverarbeitung im CIR trägt. Nach Artikel 40 Absatz 2 der EU-IOP-Verordnungen ist derjenigen mitgliedsstaatlichen Behörde die Verantwortung für die Verarbeitung von Daten im CIR zu übertragen, die für die Verarbeitung im EES, im VIS und im ETIAS verantwortlich ist. Demnach ist in der Schweiz

das SEM zuständig.

Artikel 9

Artikel 9 Absatz 1 N-IOP-Verordnung regelt, dass die Identitätsdaten, die Daten zu den Reisedokumenten und die biometrischen Daten von Drittstaatsangehörigen im CIR logisch voneinander getrennt gespeichert werden nach den Informationssystemen, aus denen sie stammen im Sinne von Artikel 18 Absatz 1 der EU-IOP-Verordnungen.

Mit *Artikel 9 Absatz 2* N-IOP-Verordnung wird ausgeführt, dass eine Anpassung der Daten zu den Reisedokumenten und den biometrischen Daten von Drittstaatsangehörigen im EES, im ETIAS, im C-VIS oder im Eurodac automatisch eine Anpassung der Daten im CIR bewirkt. Diese Präzisierung ergibt aus Artikel 19 der EU-IOP-Verordnungen, der die Hinzufügung, Änderung und Löschung von Daten im CIR regelt. Eine Besonderheit besteht, wenn im MID eine weisse oder rote Verknüpfung zwischen Daten von dem CIR angehörigen Informationssystemen erstellt wird. In diesem Fall werden vom CIR keine neuen individuellen Dateien angelegt, sondern die neuen Daten der individuellen Datei der verknüpften Daten hinzugefügt (Art. 19 Abs. 2 der EU-IOP-Verordnungen).

Artikel 9 Absatz 3 verweist auf den Anhang 1 der N-IOP-Verordnung, der einen Datenkatalog aufstellt, der auf Artikel 18 der EU-IOP-Verordnungen beruht und die Daten nennt, die im CIR gespeichert werden. Da es sich beim CIR um ein Informationssystem handelt, ist ein Datenkatalog inklusive Abfragematrix zu erstellen. Die gestützt auf Artikel 18 der beiden EU-IOP-Verordnungen im CIR zu speichernden Daten sind in drei Kategorien zu unterteilen: Personalien, Daten zum Reisedokument und biometrische Daten. Inwieweit die Behörden diese Daten abfragen können, ergibt sich aus den Artikeln 10, 11 und 12 N-IOP-Verordnung. Die Abfragerechte werden ebenfalls im Anhang 1 illustriert.

Artikel 10

In *Artikel 10 Absatz 1* N-IOP-Verordnung werden die Organisationseinheiten des Bundes genannt, die zwecks Identifikation von Personen im Sinne von Artikel 110*b* AIG die im CIR gespeicherten Daten abfragen können. Der Zugriff auf das CIR zwecks Identifikation ist ein Zugriff für Organisationseinheiten mit polizeilichen Aufgaben. Abfragen des CIR zwecks Identifikation können fedpol, die Polizeibehörden der Kantone und Gemeinden sowie die EZV bzw. das Bundesamt für Zoll und Grenzsicherheit (BAZG; offizielle Bezeichnung ab dem 1.1.2022) im Rahmen ihrer zollrechtlichen und nicht zollrechtlichen Aufgaben zum Schutz der Bevölkerung und zur Wahrung der inneren Sicherheit durchführen (Art. 110*b* Abs. 3 AIG). Diese Behörden sind in der N-IOP-Verordnung näher zu konkretisieren (wenn immer möglich wird auf die konkrete Aufgabe und

nicht auf die derzeit geltende Bezeichnung der Einheit abgestellt, wie dies auch in anderen Verordnungsprojekten getan wird und was der Rechtssicherheit dient). Folgende Stellen bei fedpol sollen den CIR zwecks Identifizierung abfragen können (Bst. a): die Bundeskriminalpolizei (Ziff. 1), der Bundessicherheitsdienst (Ziff. 2), die Einsatz- und Alarmzentrale (Ziff. 3), die für die Bearbeitung von biometrischen erkennungsdienstlichen Daten zuständigen Dienststellen (Ziff. 4) und die Stelle, die für den internationalen polizeilichen Informationsaustausch bei Sportveranstaltungen zuständig ist für die Informationsgewinnung und den Informationsaustausch für die Abwehr von Gefahren für die öffentliche Sicherheit oder der Wahrung der inneren oder äusseren Sicherheit (Ziff. 5). Sie alle sind mit Personenkontrollen betraut, wobei die Identifikation von Personen einen wesentlichen Teil ihrer Aufgaben darstellt. Beim BAZG sollen diejenigen Mitarbeitenden, die für die Personenkontrolle eingesetzt werden, den CIR zwecks Identifikation abfragen können (Bst. b). Die Formulierung lehnt sich an Artikel 4 der Einreise- und Ausreisesystem-Verordnung (EESV; noch nicht in Kraft) an. Die Identifizierungen haben zur Verhinderung und Bekämpfung illegaler Einwanderung und der Gewährleistung eines hohen Masses an Sicherheit beizutragen (Art. 2 Abs. 1 Bst. b und c der EU-IOP-Verordnungen), wobei die Schengen/Dublin-Staaten die genauen Zwecke festzulegen haben (Art. 20 Abs. 5 der EU-IOP-Verordnungen). Demnach ist sicherzustellen, dass jede Diskriminierung von Drittstaatsangehörigen verhindert wird, die genauen Zwecke der erfolgenden Identifizierung festgelegt, die abfrageberechtigten Behörden benannt und die Verfahren, Bedingungen und Kriterien derartiger Kontrollen festgelegt werden. Diesen Voraussetzungen kommt Artikel 110*b* AIG nach; eine weitere Eingrenzung erscheint nicht notwendig. Zudem sind sämtliche der in Artikel 10 Buchstaben a und b genannten Organisationseinheiten mit Aufgaben betraut, die unter die Zwecke nach Artikel 2 Absatz 1 Buchstaben b und c der EU-IOP-Verordnungen fallen.

Da in Absatz 1 auf die Organisationseinheiten des Bundes eingegangen wird, soll der Zugriff der Polizeibehörden der Kantone und Gemeinden auf den CIR in Absatz 2 geregelt werden. Gemäss *Artikel 10 Absatz 2* der N-IOP-Verordnung dürfen auch die Polizeibehörden der Kantone und Gemeinden die im CIR gespeicherten Daten zwecks Identifikation abfragen. Die Bestimmung stützt sich auf Artikel 110*b* Absatz 3 Buchstabe b AIG, der den Polizeibehörden der Kantone und Gemeinden dieses Recht einräumt.

Artikel 10 Absatz 3 N-IOP-Verordnung regelt das Verfahren der Abfrage des CIR zwecks Identifikation. Die Abfrage erfolgt anhand der bei einer Identitätskontrolle direkt vor Ort erhobenen biometrischen Daten. Die Person muss bei der Einleitung des Verfahrens anwesend sein. Falls die biometrischen Daten der betreffenden Person nicht verwendet werden können oder die Abfrage anhand dieser Daten nicht erfolgreich ist, ist die Abfrage anhand von Identitätsdaten dieser Person in Verbindung mit Reisedokumentendaten oder anhand der von der betreffenden Person bereitgestellten Identitätsdaten vorzunehmen. Es ist sicherzustellen, dass jede Diskriminierung

von Drittstaatsangehörigen vermieden wird. Die Bestimmung beruht auf Artikel 20 Absätze 2 und 3 der EU-IOP-Verordnungen. Falls die Abfrage im CIR zwecks Identifikation ergibt, dass Daten zu der betreffenden Person gespeichert sind, erhält die berechtigte Behörde gemäss Absatz 1 und 2 als Treffer dieser Abfrage die im Anhang 1 der N-IOP-Verordnung genannten Daten, die im CIR gespeichert sind (vgl. Art. 9 Abs. 3 N-IOP-Verordnung). Die entsprechende Organisationseinheit erfährt jedoch nicht, aus welchem dem CIR zugrundliegenden Informationssystem diese Daten stammen.

Artikel 10 Absatz 4 N-IOP-Verordnung bestimmt, dass im Falle von Naturkatastrophen, bei Unfallereignissen oder Gewalttaten die abfrageberechtigten Behörden nach Artikel 10 Absatz 1 N-IOP-Verordnung den CIR ausschliesslich zur Identifikation unbekannter Personen, die sich nicht ausweisen können, oder nicht identifizierter menschlicher Überreste mit den biometrischen Daten dieser Person abfragen dürfen. Was als «Naturkatastrophe», «Unfallereignis» oder «Gewalttat» gilt, liegt im Ermessen der Mitgliedsstaaten, sofern es dafür sachliche Gründe gibt. Zu denken ist etwa an einen Erdrutsch oder eine Lawine (Naturkatastrophe), an einen Flugzeugabsturz oder Verkehrsunfall (Unfallereignis) oder an einen Mord (Gewalttat). Die Rechtsgrundlage hierfür findet sich in Artikel 20 Absatz 4 der EU-IOP-Verordnungen.

Artikel 11

Artikel 11 N-IOP-Verordnung nennt die Organisationseinheiten des Bundes und der Kantone, die zwecks Aufdeckung von Mehrfachidentitäten nach Artikel 110*c* AIG die im CIR gespeicherten Daten und Verweise abfragen dürfen. Bei gelben MID-Verknüpfungen erfolgt dies zu Verifizierungszwecken und bei roten MID-Verknüpfungen zur Bekämpfung von Identitätsbetrug. Als Ergebnis erhalten die Organisationseinheiten Zugriff sowohl auf die im CIR gespeicherten Daten als auch auf den Verweis, in welchen Informationssystem diese Daten gespeichert sind. Obwohl es sich im Wesentlichen um eine Wiederholung der Bestimmungen von Artikel 110*c* Absatz 1 AIG handelt, ist dies der Verständlichkeit und Vollständigkeit halber angebracht, da sämtliche Zugangsrechte auf den CIR in der N-IOP-Verordnung geregelt werden sollen. Soweit möglich, werden die im Gesetzestext genannten Organisationseinheiten präzisiert (Bst. a, Bst. b Ziff. 1, Bst. c Ziff. 1, 2 und 3). Zudem muss es dem SIRENE-Büro gemäss Buchstabe a möglich sein, bei der biometrischen Verifizierung der Identitätsdaten die für die Bearbeitung von biometrischen erkennungsdienstlichen Daten zuständigen Dienststellen bei fedpol beizuziehen. Ausserdem muss bei Aktualisierungen von SIS-Ausschreibungen aus dem Migrationsbereich die Sektion Identifikation und Visumkonsultation des SEM (SEM-SIV) unterstützen können, die hinsichtlich dieser Informationen Datenhoheit hat. Die abschliessende Verantwortung trägt in diesen Fällen aber weiterhin das SIRENE-Büro. Artikel 11 Buchstabe a wurde entsprechend präzisiert. Die gemäss Buchstabe c Ziffer 1 für die Visumerteilung zuständigen Einheiten im Direktionsbereich für

Zuwanderung und Integration des SEM umfassen auch die zentrale MID-Expertenstelle, die zur Unterstützung der manuellen Verifizierung von MID-Verknüpfungen geschaffen wird und die im CIR gespeicherten Daten und Verweise abfragen darf. Die MID-Expertenstelle wird sich aus Personal der Bundesämter zusammensetzen. Sie soll die für die manuelle Verifizierung zuständigen Behörden in besonders komplexen Fällen, oder wenn einer Behörde das nötige Expertenwissen für die Verifizierung einer MID-Verknüpfung fehlt, fachlich und personell unterstützen.

Artikel 12

Artikel 12 N-IOP-Verordnung führt die Organisationseinheiten des Bundes auf, die zwecks Verhütung, Aufdeckung oder Ermittlung terroristischer oder sonstiger schwerer Straftaten nach Artikel 110*d* AIG auf den CIR zugreifen können. Konkret können die benannten Behörden den CIR abfragen, um in Erfahrung zu bringen, ob im CIR Daten zu einer spezifischen Person gespeichert sind. Voraussetzung ist, dass in einem konkreten Einzelfall vernünftige Gründe bestehen, dass die Abfrage der Verhütung, Aufdeckung oder Ermittlung terroristischer oder sonstiger schwerer Straftaten dient. Falls die Abfrage im CIR ergibt, dass in einem Schengen/Dublin-Informationssystem Daten zu der betreffenden Person gespeichert sind, zeigt der CIR dies den Behörden durch einen Verweis auf das entsprechende System an. Für die Definition terroristischer Straftaten oder sonstiger schwerer Straftaten kann auf Artikel 2 Buchstabe e und f der N-IOP-Verordnung verwiesen werden. Abfragen des CIR zur Verhütung, Aufdeckung oder Ermittlung terroristischer oder sonstiger schwerer Straftaten dürfen fedpol, der NDB, die Bundesanwaltschaft sowie die kantonalen Polizei- und Strafverfolgungsbehörden und die Polizeibehörden der Städte Zürich, Winterthur, Lausanne, Chiasso und Lugano (Art. 110*d* Abs. 2 AIG) vornehmen. Es handelt sich hierbei um Behörden, die Aufgaben im Rahmen der Verhütung, Aufdeckung und Ermittlung terroristischer oder schwerer Straftaten vornehmen. Während in Absatz 1 auf die Zugriffsrechte der Organisationseinheiten des Bundes eingegangen wird, soll in Absatz 2 der Zugriff der kantonalen Polizei- und Strafverfolgungsbehörden sowie der Polizeibehörden der Städte Zürich, Winterthur, Lausanne, Chiasso und Lugano geregelt werden. Folgende Stellen bei fedpol sollen den CIR zwecks Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten abfragen können (Bst. a): die Bundeskriminalpolizei (Ziff. 1), die für die Bearbeitung biometrischer erkennungsdienstlicher Daten zuständigen Stellen (Ziff. 2) und die Einsatz- und Alarmzentrale (Ziff. 3). Beim NDB sollen folgende Stellen ein entsprechendes Abfragerecht erhalten (Bst. b): die Abteilung Beschaffung (Ziff. 1), die Abteilung Auswertung (Ziff. 2), die Steuerung Terrorismusabwehr (Ziff. 3), die Steuerung Nachrichtendienst (Ziff. 4), die Steuerung Extremismusabwehr (Ziff. 5), die Steuerung Nonproliferation (Ziff. 6), der Bereich Ausländerdienst (Ziff. 7), der Bereich Datenerfassung/Triage (Ziff. 8) und das Bundeslagezentrum (Ziff. 9). Die Aufzählung orientiert sich an Artikel 12 der Einreise- und Ausreisesystem-Verordnung (EESV;

noch nicht in Kraft), die sich derzeit im Entwurfsstadium befindet. Zusätzlich hat der NDB beantragt, den Bereich Datenerfassung/Triage und das Bundeslagezentrum aufzunehmen, die im Bereich der Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten tätig sind. Bei der Bundesanwaltschaft sollen schliesslich die verfahrensführenden Abteilungen den CIR zwecks Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten abfragen können (Bst. c). Diese werden in Artikel 1 Absatz 2 des Reglements vom 26. Februar 2021 über die Organisation und Verwaltung der Bundesanwaltschaft (SR 173.712.22) definiert.

Artikel 12 Absatz 2 N-IOP-Verordnung ermächtigt die kantonalen Polizei- und Strafverfolgungsbehörden und die Polizeibehörden der Städte Zürich, Winterthur, Lausanne, Chiasso und Lugano, zu den Zwecken nach Absatz 1 die im CIR gespeicherten Verweise abzufragen. Die diese Möglichkeit einräumende Rechtsgrundlage findet sich in Artikel 110*d* Absatz 2 Buchstabe d AIG.

Artikel 13

Artikel 13 Absatz 1 N-IOP-Verordnung regelt den ersten Schritt des nach Artikel 22 der EU-IOP-Verordnungen vorgesehenen zweistufigen Verfahrens. Ergibt sich bei diesem ersten Schritt ein Treffer (sprich, sind Daten zu einer Person in einem der Systeme EES, ETIAS, C-VIS oder Eurodac vorhanden), so meldet der CIR der abfragenden Behörde, in welchem Informationssystem Daten vorhanden sind. Diese Information darf ausschliesslich für die Zwecke der Übermittlung eines Antrags auf vollständigen Zugang gemäss Absatz 2 verwendet werden. Die Rechtsgrundlage hierfür findet sich in Artikel 110*d* Absatz 3 AIG.

Artikel 13 Absatz 2 N-IOP-Verordnung regelt den zweiten Schritt des Verfahrens (Art. 22 der EU-IOP-Verordnungen). Die abfragende Behörde hat im Falle eines Treffers nach Absatz 1 bei der Einsatz- und Alarmzentrale von fedpol (EAZ fedpol) ein Gesuch auf vollständigen Zugang zu mindestens einem der vom Treffer betroffenen Informationssysteme zu stellen. Der vollständige Zugang unterliegt weiterhin den Bedingungen und Verfahren, die in den einschlägigen Rechtsinstrumenten festgelegt sind. Die Rechtsgrundlage hierfür findet sich in Artikel 110*d* Absatz 4 AIG. Im Gesuch sind die jeweiligen Bedingungen des vollständigen Zugangs zum einschlägigen System gemäss deren Rechtsgrundlagen darzulegen. Damit soll sichergestellt werden, dass kein Phishing betrieben wird, also eine Abfrage ohne vernünftige Gründe, dass eine Person verzeichnet sein könnte. Damit soll ganz generell gegen Missbrauch vorgegangen werden. Die vernünftigen Gründe stellen eine Bedingung für den Zugang zu Daten des CIR zu Strafverfolgungszwecken dar.

In *Artikel 13 Absatz 3* der N-IOP-Verordnung wird das Vorgehen beschrieben, wenn ausnahmsweise kein Antrag auf vollständigen Zugang im Sinne von Absatz 2 gestellt wird. In diesem Fall ist die abfragende Behörde nach Absatz 2 bzw. Artikel 22 Absatz 2 der EU-IOP-Verordnungen verpflichtet, ihren Entscheid schriftlich zu begründen und zu protokollieren, wobei die Nichtbeantragung in der nationalen Datei rückverfolgbar sein muss. Damit soll ebenfalls Phishing/Missbrauch vorgebeugt werden. Die Aufsicht über die Datenbearbeitung in unabhängiger Weise wird in Artikel 30 der vorliegenden Verordnung geregelt, wodurch die durch den 6. Abschnitt eingeräumten Rechte der betroffenen Personen effektiv wahrgenommen werden können.

Artikel 14

Artikel 14 Absatz 1 N-IOP-Verordnung verpflichtet die EAZ fedpol, vor Genehmigung des Antrags auf vollständigen Zugang zu den Daten im Sinne von Artikel 12 Absatz 2 N-IOP-Verordnung sicherzustellen, dass die Daten zur Verhütung, Aufdeckung oder Ermittlung terroristischer oder sonstiger schwerer Straftaten beitragen können (Bst. a) und Beweise oder hinreichende Gründe zur Annahme bestehen, dass die Datenbekanntgabe dazu beitragen wird, den damit verfolgten Zweck zu erfüllen (Bst. b). Die Aufzählung setzt Artikel 22 Absatz 1 der EU-IOP-Verordnungen um, der die Abfrage des CIR vom Vorliegen «vernünftiger Gründe abhängig macht, die vermuten lassen, dass sie zur Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten beitragen». Ebenso folgt die Aufzählung der Logik von Artikel 14 der Einreise- und Ausreisesystem-Verordnung (EESV; noch nicht in Kraft), der eine ähnliche Formulierung enthält.

Artikel 14 Absatz 2 N-IOP-Verordnung nimmt Bezug auf Artikel 22 Absatz 3 der EU-IOP-Verordnungen, wonach der vollständige Zugang zu den im EES, ETIAS und C-VIS gespeicherten Daten, welche für die Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten erforderlich sind, den Bedingungen und Verfahren der jeweiligen Informationssysteme unterliegt. Konkret handelt es sich dabei um die Bedingungen und Verfahren, die in Artikel [...] der Verordnung über das Einreise- und Ausreisesystem (Bst. a), Artikel [...] der Verordnung über das Europäisches Reiseinformations- und -genehmigungssystem (Bst. b) und Artikel [...] der Verordnung über das zentrale Visa-Informationssystem und das nationale Visumsystem (Bst. c) festgelegt sind. Die konkreten Artikel werden zu einem späteren Zeitpunkt ergänzt; die entsprechenden Ausführungsverordnungen werden derzeit erarbeitet.

Artikel 15

In *Artikel 15* N-IOP-Verordnung soll die Datenspeicherung im CIR geregelt werden. So werden nach Artikel 23 der EU-IOP-Verordnungen die Daten im CIR nach Massgabe der Datenspeicherungsbestimmungen des jeweiligen EU-Informationssystems, aus dem sie stammen, automa-

tisch gelöscht. Die individuellen Dateien im CIR werden nur so lange gespeichert, wie die entsprechenden Daten in mindestens einem der EU-Informationssysteme gespeichert sind. Es ist vorzusehen, dass die einzelnen Dateien, die im CIR auf Daten im EES, im ETIAS, im C-VIS oder im Eurodac verweisen, aktualisiert werden, sobald Daten in den entsprechenden Systemen angepasst werden. Durch die Erstellung einer Verknüpfung wird die Speicherfrist der einzelnen durch die Verknüpfung bezeichneten Daten nicht berührt.

Artikel 16

Artikel 16 N-IOP-Verordnung regelt die Protokollierung von Abfragen im CIR durch die abfragende Behörde. Zu protokollieren sind folgende Informationen: die abfragende Behörde (Bst. a), die abgefragten Schengen/Dublin-Informationssysteme (Bst. b), das Datum und die Uhrzeit der Abfrage (Bst. c), die für die Abfrage verwendeten Daten (Bst. d) und die Abfrageergebnisse (Bst. e). Die rechtliche Verankerung dieser Verpflichtung findet sich in Artikel 24 Absatz 5 der EU-IOP-Verordnungen, wobei die Aufzählung sich zusätzlich an der Struktur von Artikel 7 N-IOP-Verordnung orientiert. Die Protokollierung dieser Informationen stellt sicher, dass die durch den 6. Abschnitt der vorliegenden Verordnung eingeräumten Rechte der betroffenen Personen effektiv wahrgenommen werden können. Insbesondere ist zu gewährleisten, dass die Aufsicht über die Datenbearbeitung nach Artikel 30 der vorliegenden Verordnung sichergestellt ist. Durchführungsrechtsakte speziell zur Protokollierung im CIR gibt es nicht. Als Abfrageergebnisse im Sinne von Buchstabe e gelten Informationen zu den Schengen/Dublin-Informationssystemen, aus denen die Daten für den CIR stammen; es werden keine Personendaten als Abfrageergebnisse protokolliert.

Artikel 17

Artikel 17 N-IOP-Verordnung soll das Recht auf Information der betroffenen Personen über Daten im CIR regeln. Die rechtliche Grundlage findet sich in Artikel 47 der EU-IOP-Verordnungen. Diese Bestimmung sieht vor, dass die Behörde, welche die personenbezogenen Daten erfasst, die im sBMS, im CIR oder im MID zu speichern sind, den betroffenen Personen in klarer und einfacher Sprache die Informationen zur Verfügung stellt, die nach den Artikeln 12 und 13 der Richtlinie (EU) 2016/680[12] und den Artikeln 15 und 16 der Verordnung (EU) 2018/1725[13] vorgeschrieben

[12] 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.

[13] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, ABl. L 295 vom 21.11.2018, S. 39

sind.[14] Im Gegensatz zum CIR oder zum MID handelt es sich beim sBMS nicht um eine Datensammlung bzw. «Datenbank» im Sinne von Artikel 3 Buchstabe g DSG. Die im sBMS enthaltenen biometrischen Merkmalsdaten sind keine biometrischen Personendaten, es werden auch keine weiteren Personendaten in diesem System gespeichert (siehe dazu Art. 2 der Verordnung über die Bearbeitung biometrischer erkennungsdienstlicher Daten[15]). Da im sBMS keine personenbezogenen Daten (sondern nur biometrische Templates) gespeichert werden und das Recht auf Information über Daten im MID in Artikel 24 Absatz 3 N-IOP-Verordnung geregelt wird, ist in Artikel 17 ein Verweis auf den CIR ausreichend. Um den Informationsfluss mit der betroffenen Person zu erleichtern, wird ein Web-Portal im Sinne von Artikel 49 EU-IOP-Verordnungen eingerichtet.

4. Abschnitt

Das ESP soll den zuständigen Behörden, nach Massgabe ihrer Zugangsrechte, einen raschen, unterbrechungsfreien, effizienten, systematischen und kontrollierten Zugriff auf die verschiedenen Schengen/Dublin-Informationssysteme sowie die Interpol-Datenbanken ermöglichen. Mittels einer einzigen Abfrage sollen die zuständigen Behörden in Zukunft gleichzeitig aus mehreren Informationssystemen alle relevanten Informationen, auf welche sie zugreifen dürfen, erhalten. Die Abfrage via ESP kann anhand von Identitätsdaten, Daten zu den Reisedokumenten und biometrischen Personendaten erfolgen.

Artikel 18

Die Abfragerechte des ESP sollen nicht in der N-IOP-Verordnung selber, sondern in den nationalen Verordnungen zu den einzelnen Informationssystemen geregelt werden. *Artikel 17 Absatz 1* N-IOP-Verordnung verweist somit hinsichtlich der Zugriffsrechte der Behörden, die das ESP abfragen können, auf die entsprechenden Artikel der EES-Verordnung, der ETIAS-Verordnung, der VIS-Verordnung (SR 142.512) und der N-SIS-Verordnung (SR 362.0). Hintergrund ist, dass nach Artikel 110*e* Absatz 2 AIG und Artikel 16*b* Absatz 2 BPI die Behörden, die auf mindestens eines der Informationssysteme zugriffsberechtigt sind, im Abrufverfahren auf das ESP zugreifen dürfen. Eine Datenabfrage über das ESP erfordert somit die Berechtigung, auf mindestens eines der Schengen/Dublin-Informationssysteme, die in den aufgeführten Artikeln festgelegt sind, resp. auf eine der Interpol-Datenbanken zugreifen zu dürfen. Aufgrund der noch nicht erfolgten Übernahme der revidierten Eurodac-Verordnung kann aktuell auf einen Verweis auf Eurodac verzichtet werden. Die EES- und ETIAS-Verordnung werden zurzeit ausgearbeitet; die massgeblichen

[14] Die ebenfalls in Art. 47 der EU-IOP-Verordnungen erwähnte Verordnung (EU) 2016/679 ist nicht Teil des Schengen-Besitzstandes und deshalb für die Schweiz nicht anwendbar.
[15] SR 361.3

Bestimmungen werden zu gegebener Zeit ergänzt.

Artikel 18 Absatz 2 N-IOP-Verordnung verweist für die weiteren Einzelheiten auf die Artikel 7 und 9 der EU-IOP-Verordnungen. Damit wird klargestellt, dass die beiden EU-IOP-Verordnungen die Grundlage für den Zugriff auf Daten über das ESP bilden. Die beiden Artikel umschreiben die Nutzung des ESP bzw. das Abrufverfahren auf das ESP. Entscheidend ist, dass die abfrageberechtigten Behörden nur für die Ziele und Zwecke, die in den für die Informationssysteme geltenden Rechtsinstrumenten sowie in den beiden EU-IOP-Verordnungen festgelegt sind, auf das ESP und die von ihm bereitgestellten Daten zugreifen dürfen. Das ESP liefert lediglich Daten aus den EU-Informationssystemen und zu den Interpol-Datenbanken, auf welche die abfragende Behörde zugriffsberechtigt ist.

Artikel 19

Artikel 19 Absatz 1 N-IOP-Verordnung legt dar, welche Informationen eine Behörde erhält, die das ESP abfragen darf. Demnach enthält die Antwort des ESP bei einem Treffer den Hinweis, dass Daten gefunden wurden (Bst. a), sofern keine Abfrage nach Artikel 10 erfolgt, einen Verweis auf das Schengen/Dublin-Informationssystem oder die Komponente, das oder die die entsprechenden Daten enthält (Bst. b) und die Daten, die im entsprechenden Informationssystem enthalten sind (Bst. c). Die Rechtsgrundlage hierfür findet sich in Artikel 9 Absatz 4 der EU-IOP-Verordnungen, wonach die Antwort die Daten der Informationssysteme umfasst, auf die die Behörde Zugriff hat, sowie den Hinweis, aus welchem EU-Informationssystem beziehungsweise aus welcher Datenbank die betreffenden Daten stammen. Nach derselben Bestimmung wird jedoch ein Verweis im Sinne von Artikel 19 Absatz 1 Buchstabe b nicht offengelegt, wenn eine Abfrage des CIR zwecks Identifikation gemäss Artikel 10 der vorliegenden Verordnung erfolgt. Artikel 4 Absatz 2 der Durchführungsbeschlüsse zu Artikel 9 Absatz 7 der EU-IOP-Verordnungen[16] legt den obgenannten Inhalt der Antwort des ESP fest.

Artikel 19 Absatz 2 N-IOP-Verordnung schildert das Verfahren, wenn im Rahmen einer Abfrage des ESP keine Daten gefunden werden. In diesem Fall informiert das ESP die abfragende Behörde, dass die Abfrage erfolgreich war, aber keine Daten gefunden wurden. Wenn bei der Abfrage ein Fehler auftritt, wird dieser ebenfalls mit einer Beschreibung zurückgemeldet. Die rechtliche Grundlage findet sich in Artikel 4 Absatz 3 der oben genannten Durchführungsbeschlüsse,

[16] Durchführungsbeschluss der Kommission vom 6.9.2021 zur Festlegung des technischen Verfahrens für Abfragen der EU-Informationssysteme, Europol-Daten und Interpol-Datenbanken durch das Europäische Suchportal und des Formats der vom Europäischen Suchportal erteilten Antworten gemäss Artikel 9 Absatz 7 der Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates, C(2021) 6484 final; Durchführungsbeschluss der Kommission vom 6.9.2021 zur Festlegung des technischen Verfahrens für Abfragen der EU-Informationssysteme, Europol-Daten und Interpol-Datenbanken durch das Europäische Suchportal und des Formats der vom Europäischen Suchportal erteilten Antworten gemäss Artikel 9 Absatz 7 der Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates, C(2021) 6486 final

der diese Verpflichtung statuiert.

Artikel 20

Artikel 20 Absatz 1 N-IOP-Verordnung legt fest, dass jede Abfrage von Daten über das ESP in einem Protokoll festzuhalten ist. Die Protokollierung soll durch den Bund erfolgen, wobei dort diejenige Behörde zuständig ist, die das zugrundeliegende Schengen/Dublin-Informationssystem abfragt. Zu protokollieren sind folgende Informationen: die Angaben zur Benutzerin oder zum Benutzer und das Benutzerprofil, das auf das ESP zugreift (Bst. a), die abgefragten Schengen/Dublin-Informationssysteme und Komponenten (Bst. b), das Datum und die Uhrzeit der Abfrage (Bst. c) und das Ergebnis der Abfrage (Bst. d). Die rechtliche Verankerung dieser Verpflichtung findet sich in Artikel 10 der EU-IOP-Verordnungen. Präzisiert wird die Verpflichtung in Artikel 5 Absatz 2 der Durchführungsbeschlüsse zu Artikel 9 Absatz 7 der EU-IOP-Verordnungen[17], der die entsprechende Auflistung macht. Die Protokolle stellen sicher, dass die durch den 6. Abschnitt der vorliegenden Verordnung eingeräumten Rechte der betroffenen Personen effektiv wahrgenommen werden können. Insbesondere ist zu gewährleisten, dass die Aufsicht über die Datenbearbeitung nach Artikel 30 der vorliegenden Verordnung sichergestellt ist.

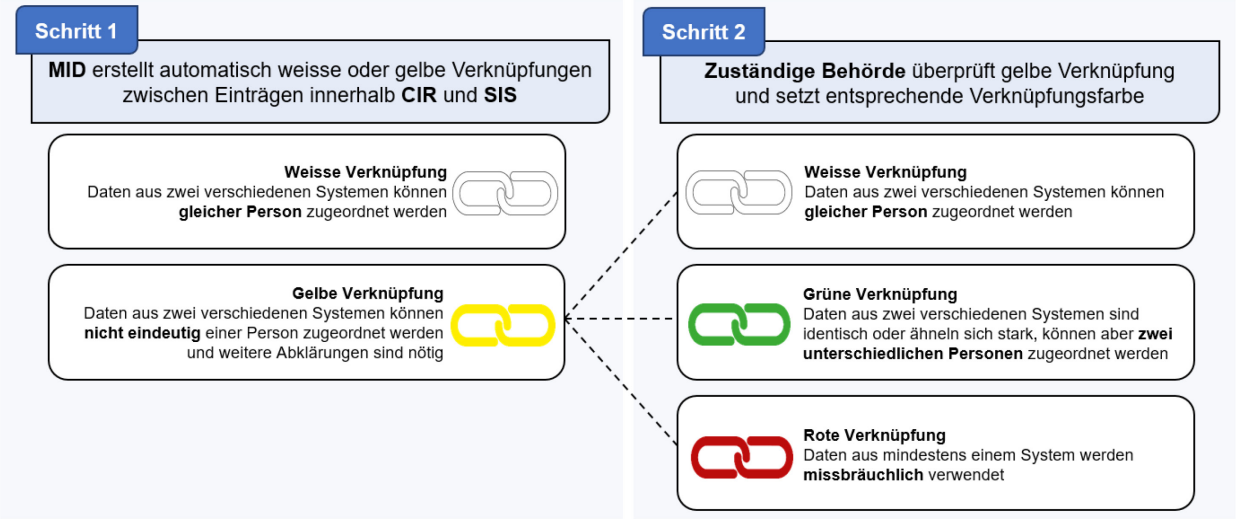
In *Artikel 20 Absatz 2* N-IOP-Verordnung wird festgehalten, dass sich die Einzelheiten der Protokollierung nach Artikel 10 Absatz 3 der EU-IOP-Verordnungen richten. Damit wird sichergestellt, dass die Protokolle nur zur datenschutzrechtlichen Kontrolle, einschliesslich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmässigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit und -integrität verwendet werden. Die Protokolle müssen zudem in geeigneter Weise vor unbefugtem Zugriff geschützt und ein Jahr nach ihrer Erstellung gelöscht werden. Eine Ausnahme von dieser Löschfrist besteht, wenn bereits ein Kontrollverfahren eingeleitet wurde. In diesem Fall werden die Protokolle gelöscht, sobald sie für das Kontrollverfahren nicht mehr benötigt werden.

5. Abschnitt

Der MID soll Identitätsprüfungen vereinfachen und die Bekämpfung von Identitätsbetrug unterstützen. Er soll zur Identifizierung von Personen beitragen, die mehrere oder falsche Identitäten benutzen. Dazu gleicht er die Daten im CIR mit denen im SIS ab. Für den Abgleich der biometri-

[17] Durchführungsbeschluss der Kommission vom 6.9.2021 zur Festlegung des technischen Verfahrens für Abfragen der EU-Informationssysteme, Europol-Daten und Interpol-Datenbanken durch das Europäische Suchportal und des Formats der vom Europäischen Suchportal erteilten Antworten gemäss Artikel 9 Absatz 7 der Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates, C(2021) 6484 final; Durchführungsbeschluss der Kommission vom 6.9.2021 zur Festlegung des technischen Verfahrens für Abfragen der EU-Informationssysteme, Europol-Daten und Interpol-Datenbanken durch das Europäische Suchportal und des Formats der vom Europäischen Suchportal erteilten Antworten gemäss Artikel 9 Absatz 7 der Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates, C(2021) 6486 final

schen Daten nimmt der MID den sBMS zu Hilfe, während über das ESP der Abgleich mit Identitätsdaten und Daten zu den Reisedokumenten realisiert wird. Der MID wird im nationalen Recht in den Artikeln 110*f* und 110*g* AIG sowie in den Artikeln 16*c* und 16*d* BPI geregelt.



Artikel 21

Artikel 21 N-IOP-Verordnung sieht vor, dass das SEM und fedpol die Verantwortung für die Datenverarbeitung im MID tragen. Rechtsgrundlage ist Artikel 40 Absatz 3 Buchstabe b der EU-IOP-Verordnungen, der denjenigen mitgliedsstaatlichen Behörden die Verantwortung für die Verarbeitung von Daten im MID überträgt, die Daten in der Identitätsbestätigungsdatei hinzufügen oder ändern. Soweit es um Daten geht, deren Ursprung im VIS, EES und ETIAS zu finden sind, ist das SEM zuständig. Handelt es sich hingegen um Daten, die aus dem N-SIS stammen, ist fedpol verantwortlich.

Artikel 22

Artikel 22 Absatz 1 N-IOP-Verordnung verweist für die Durchführung der Prüfung auf Mehrfachidentitäten auf Artikel 27 der EU-IOP-Verordnungen. Dieser beschreibt, wie die Prüfung auf Mehrfachidentitäten ablaufen wird. Eine solche Prüfung wird bei jeder Erfassung oder Aktualisierung von Daten in einem der Schengen/Dublin-Informationssystemen (VIS, SIS, ETIAS, EES, Eurodac) ausgelöst. Dazu werden jeweils die neuen Daten mit jenen, die bereits im CIR und im SIS vorhanden sind, verglichen. Dabei dient der sBMS zum Abgleich der biometrischen Daten und das ESP zum Abgleich der Identitätsdaten und der Daten zu den Reisedokumenten.

Artikel 22 Absatz 2 N-IOP-Verordnung verweist für die allenfalls zu erstellenden Verknüpfungen auf Artikel 28 Absätze 3 und 4 der EU-IOP-Verordnungen. Werden bei einer Überprüfung auf Mehrfachidentitäten eine oder mehrere Übereinstimmungen gefunden, werden Verknüpfungen zwischen den für die Abfrage verwendeten neuen oder aktualisierten Daten und den bereits in

einem anderen EU-Informationssystem vorhandenen Daten erstellt. Sind die Identitätsdaten, Reisedokumentendaten und biometrischen Daten der verknüpften Dateien gleich oder ähnlich, wird automatisch eine weisse Verknüpfung nach Artikel 2 Buchstabe d N-IOP-Verordnung erstellt (Bst. a). Können die Identitätsdaten, Reisedokumentendaten und biometrischen Daten hingegen nicht als ähnlich angesehen werden, wird automatisch eine gelbe Verknüpfung nach Artikel 2 Buchstabe a N-IOP-Verordnung erstellt (Bst. b), die sodann manuell zu verifizieren ist (siehe Art. 23 N-IOP-Verordnung).

Artikel 23

Artikel 23 N-IOP-Verordnung beschreibt das Verfahren der manuellen Verifizierung einer gelben Verknüpfung. Eine manuelle Verifizierung muss durchgeführt werden, wenn Verbindungen zwischen Daten aus verschiedenen Systemen bestehen und die Identitäten nicht übereinstimmen oder sich ähneln (gelbe Verknüpfung, Art. 28 Abs. 4 der EU-IOP-Verordnungen). Für das anwendbare Verfahren erlässt die Kommission gemäss Artikel 28 Absatz 5 der EU-IOP-Verordnungen delegierte Rechtsakte. Zuständig für die manuelle Verifizierung ist diejenige Behörde, die nach Artikel 110*g* Absatz 2 AIG die Daten in den Schengen/Dublin-Informationssystemen erfasst oder aktualisiert. Bei Verknüpfungen mit Ausschreibungen im SIS im Polizeibereich ist das SIRENE-Büro zuständig. Rechtsgrundlage hierfür ist Artikel 110*f* Absatz 2 AIG. Zur Unterstützung der manuellen Verifizierung von MID-Verknüpfungen soll in der Schweiz eine MID-Expertenstelle geschaffen werden. Die MID-Expertenstelle soll die Behörden in besonders komplexen Fällen unterstützen oder auch dann, wenn einer Behörde das nötige Expertenwissen für die Verifizierung einer MID-Verknüpfung fehlt. Sie wird sich aus Personal der Bundesämter zusammensetzen. Das Verfahren der manuellen Verifizierung bestimmt sich nach Artikel 29 Absätze 3 – 5 der EU-IOP-Verordnungen. Demnach erfolgt die manuelle Verifizierung verschiedener Identitäten unverzüglich, wobei die für die manuelle Verifizierung zuständige Behörde die Verknüpfung als grüne, rote oder weisse Verknüpfung nach den Artikeln 31–33 der EU-IOP-Verordnungen qualifiziert. Im Anwendungsbereich von Artikel 29 Absatz 4 der Verordnung (EU) 2019/817 wird die manuelle Verifizierung verschiedener Identitäten im Beisein der betroffenen Person eingeleitet. Diese erhält die Gelegenheit, sich gegenüber der zuständigen Behörde zu äussern. Erfolgt die manuelle Verifizierung verschiedener Identitäten an der Grenze, wird sie möglichst innerhalb von zwölf Stunden nach der Erstellung einer gelben Verknüpfung vorgenommen. Wird eine *grüne Verknüpfung* gesetzt, zeigt diese an, dass die Identitätsdaten der verknüpften Daten zwar nicht zu derselben Person gehören, jedoch nicht unrechtmässig verwendet werden. Dies kann beispielsweise dann der Fall sein, wenn die verknüpften Daten unterschiedliche biometrische Daten, aber dieselben Identitätsdaten enthalten, weil zwei Personen zufällig gleich heissen und dasselbe Geburtsdatum haben. Wird eine grüne Verknüpfung gesetzt, wird die Identitätskontrolle für die betroffenen rechtmässig reisenden Personen künftig erleichtert, indem sie nicht beim Zoll unnötig

lange angehalten werden zur genaueren Identitätsabklärung. Demgegenüber wird eine *rote Verknüpfung* erstellt, wenn unrechtmässige Mehrfachidentitäten oder ein Identitätsbetrug vorliegen, etwa wenn eine Person mehrere unterschiedliche Identitäten verwendet, das Reisedokument einer anderen Person benutzt oder sich als jemand anderes ausgibt. Eine *weisse Verknüpfung* wird schliesslich gesetzt, wenn es sich bei den verknüpften Daten um ein und dieselbe Person handelt, die schon in mindestens einem anderen Informationssystem verzeichnet ist. Damit wird die Mobilität für Personen, die beispielsweise rechtmässig mehrere gültige Reisedokumente besitzen, vereinfacht.

Artikel 24

Artikel 24 N-IOP-Verordnung bestimmt, wer Zugriff hat auf die Daten hat, bei denen eine rote, weisse oder grüne Verknüpfung vorliegt. Gemäss *Absatz 1* sind dies bei einer roten Verknüpfung die Behörden, die auf mindestens eines von der Verknüpfung betroffenen Informationssysteme nach Artikel 110*a* AIG oder Artikel 16*a* BPI Zugriff haben. Sie dürfen die Daten abfragen, die in der Identitätsbestätigungsdatei nach Artikel 34 Buchstaben a und b der EU-IOP-Verordnungen bzw. in Artikel 26 Buchstaben a und b der vorliegenden Verordnung gespeichert sind (siehe nachfolgend die Erläuterungen zu Art. 26, der die Identitätsbestätigungsdatei regelt). Die Rechtsgrundlage hierfür findet sich in Artikel 26 Absatz 2 der EU-IOP-Verordnungen.

Gemäss *Artikel 24 Absatz 2* der N-IOP-Verordnung dürfen die Behörden, die auf beide Informationssysteme nach Artikel 110*a* AIG oder Artikel 16*a* BPI Zugriff haben, bei einer weissen Verknüpfung die in der Identitätsbestätigungsdatei verzeichneten Daten abfragen (siehe auch hierzu die Erläuterungen zu Art. 26). Die rechtliche Grundlage dafür ist Artikel 26 Absatz 3 der EU-IOP-Verordnungen, der den Zugang zu weissen Verknüpfungen regelt. Voraussetzung ist, dass die abfragende Behörde Zugang zu beiden Informationssystemen hat, zwischen denen die weisse Verknüpfung besteht.

Artikel 24 Absatz 3 N-IOP-Verordnung regelt den Zugriff auf die Daten aus Verknüpfungen beim Vorliegen einer grünen Verknüpfung. Behörden, die auf beide Informationssysteme nach Artikel 110*a* AIG oder Artikel 16*a* BPI Zugriff haben, dürfen die Daten nach Artikel 26 abfragen, wenn verknüpfte Daten übereinstimmen. Voraussetzung ist, dass die abfragende Behörde Zugang zu beiden Informationssystemen hat, zwischen denen eine grüne Verknüpfung erstellt wurde. Dies sieht Artikel 26 Absatz 4 der EU-IOP-Verordnungen vor. Bezüglich der konkreten Daten, die beim Vorliegen einer grünen Verknüpfung abgerufen werden dürfen, kann wiederum Artikel 34 der beiden EU-IOP-Verordnungen bzw. Artikel 26 der vorliegenden Verordnung (und spezifisch dessen Abs. 2) herangezogen werden, die Ausführungen zur Identitätsbestätigungsdatei enthalten.

Artikel 25

Artikel 25 Absatz 1 N-IOP-Verordnung schliesst an den Prozess der manuellen Verifikation einer gelben Verknüpfung nach Artikel 22 N-IOP-Verordnung an und bestimmt, dass im Falle einer Erstellung einer roten oder weissen Verknüpfung die betroffene Person entsprechend Artikel 32 Absätze 4 und 5 beziehungsweise Artikel 33 Absatz 4 der EU-IOP-Verordnungen informiert wird. Demnach teilt die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde der betreffenden Person mit, dass ähnliche oder unterschiedliche Identitätsdaten vorliegen. Sie informiert die Person zudem über die in der Identitätsbestätigungsdatei nach Artikel 26 N-IOP-Verordnung enthaltene einmalige Kennnummer und die für die manuelle Verifizierung verschiedener Identitäten zuständigen Behörde. Ferner gibt sie der betroffenen Person die Adresse des nach Artikel 49 der beiden EU-IOP-Verordnungen eingerichteten Web-Portals bekannt. Zum Schutz der Sicherheit und der öffentlichen Ordnung, zur Verhinderung von Kriminalität und zur Gewährleistung, dass bei der Erstellung einer roten Verknüpfung keine nationalen Ermittlungen beeinträchtigt werden, oder im Zusammenhang mit Ausschreibungen im SIS gemäss den Verordnungen (EU) 2018/1860, (EU) 2018/1861 und (EU) 2018/1862 kann auf obige Information verzichtet werden. Die genannten Informationen sind der betroffenen Person schriftlich anhand eines Standardformulars zur Verfügung zu stellen. Die zu verwendenden Standartformulare finden sich in den Durchführungsbeschlüssen zur Festlegung eines Standardformulars zur Unterrichtung betroffener Personen über die Erstellung einer roten oder weissen Verknüpfung.[18]

Artikel 25 Absatz 2 N-IOP-Verordnung regelt das Verfahren, wenn Hinweise vorliegen, dass eine rote oder eine weisse Verknüpfung nicht korrekt erfasst worden ist, unrechtmässig verarbeitet wurde oder nicht mehr aktuell ist. In einem solchen Fall richtet sich das Verfahren nach Artikel 32 Absatz 7 beziehungsweise 33 Absatz 5 der EU-IOP-Verordnungen. Das Verfahren unterscheidet sich je nachdem, ob es sich um eine rote oder weisse Verknüpfung handelt. Hat eine Behörde mit Zugriff auf den CIR oder das SIS Belege dafür hat, dass eine rote Verknüpfung im MID unrichtig erfasst wurde, überprüft sie die betreffenden im CIR und im SIS gespeicherten Daten. Geht die rote Verknüpfung auf eine SIS-Ausschreibung gemäss Artikel 29 Absatz 2 der EU-IOP-Verordnungen zurück, informiert sie das Schweizer SIRENE-Büro, das seinerseits umgehend das zuständige SIRENE-Büro des Mitgliedstaats kontaktiert, das die SIS-Ausschreibung erstellt hat. Dieses prüft die Belege unverzüglich und berichtigt oder löscht die Verknüpfung gegebenenfalls.

[18] Anhang des Durchführungsbeschlusses der Kommission zur Festlegung eines Standardformulars zur Unterrichtung betroffener Personen über die Erstellung einer roten Verknüpfung gemäß der Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates, C(2021) 5989 final; Anhang des Durchführungsbeschlusses der Kommission zur Festlegung eines Standardformulars zur Unterrichtung betroffener Personen über die Erstellung einer roten Verknüpfung gemäß der Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates, C(2021) 5988 final; Anhang des Durchführungsbeschlusses der Kommission zur Festlegung eines Standardformulars zur Unterrichtung betroffener Personen über die Erstellung einer weißen Verknüpfung gemäß der Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates, C(2021) 5620 final; Anhang des Durchführungsbeschlusses der Kommission zur Festlegung eines Standardformulars zur Unterrichtung betroffener Personen über die Erstellung einer weißen Verknüpfung gemäß der Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates, C(2021) 5619 final

In allen anderen Fällen korrigiert die zuständige Behörde die fehlerhafte Verknüpfung oder löscht diese aus dem MID. Hat eine Behörde mit Zugriff auf den CIR hingegen Belege dafür, dass eine weisse Verknüpfung im MID unrichtig erfasst wurde, muss sie die betreffenden im CIR und im SIS gespeicherten Daten überprüfen und die Verknüpfung gegebenenfalls unverzüglich berichtigen oder aus dem MID löschen.

Artikel 25 Absatz 3 N-IOP-Verordnung soll das Recht auf Information über Daten im MID regeln. Die rechtliche Grundlage findet sich in Artikel 47 der EU-IOP-Verordnungen. Diese Bestimmung sieht vor, dass die Behörde, welche die personenbezogenen Daten erfasst, die im sBMS, im CIR oder im MID zu speichern sind, den betroffenen Personen in klarer und einfacher Sprache die Informationen zur Verfügung stellt, die nach den Artikeln 12 und 13 der Richtlinie (EU) 2016/680[19] und den Artikeln 15 und 16 der Verordnung (EU) 2018/1725[20] vorgeschrieben sind.[21] Da im sBMS keine personenbezogenen Daten (sondern nur biometrische Templates) gespeichert werden – beim sBMS handelt es sich nicht um eine Datensammlung bzw. «Datenbank» im Sinne von Artikel 3 Buchstabe g DSG – und das Recht auf Information über Daten im CIR in Artikel 17 N-IOP-Verordnung geregelt wird, ist in Artikel 25 Absatz 3 ein Verweis auf den MID ausreichend. Um den Informationsfluss mit der betroffenen Person zu erleichtern, wird ein Web-Portal im Sinne von Artikel 49 der EU-IOP-Verordnungen eingerichtet.

Artikel 26

Artikel 26 Absatz 1 N-IOP-Verordnung regelt den Inhalt der Identitätsbestätigungsdatei. Im Falle einer Verknüpfung von Daten zwischen den Informationssystemen SIS, EES, ETIAS, C-VIS oder Eurodac wird im Rahmen der Prüfung auf Mehrfachidentitäten eine Identitätsbestätigungsdatei erstellt. Rechtgrundlage hierfür sind Artikel 110*f* Absatz 4 AIG und Artikel 34 der EU-IOP-Verordnungen. Eine Identitätsbestätigungsdatei enthält folgende Daten: die Art der Verknüpfungen zwischen den Daten, also die gelbe, grüne, rote oder weisse Verknüpfung (Bst. a), die Angabe der Schengen/Dublin-Informationssysteme, in denen die verknüpften Daten gespeichert sind (Bst. b), die einmalige Kennnummer, die das Abrufen der verknüpften Daten aus den entsprechenden Schengen/Dublin-Informationssysteme ermöglicht (Bst. c), die Angabe der für die manuelle Verifizierung verschiedener Identitäten zuständigen Behörde (Bst. d) und das Datum der Erstellung

[19] 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, ABl. L 119 vom 4.5.2016, S. 89; zuletzt geändert durch Berichtigung der Richtlinie (EU) 2016/680, ABl. L 74 vom 4.3.2021, S. 36

[20] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (Text von Bedeutung für den EWR.), ABl. L 295 vom 21.11.2018, S. 39

[21] Die ebenfalls erwähnte Verordnung (EU) 2016/679 ist nicht Teil des Schengen-Besitzstandes, weshalb sie für die Schweiz nicht verbindlich ist.

oder jeder Aktualisierung der Verknüpfung (Bst. e).

Artikel 26 Absatz 2 N-IOP-Verordnung verweist auf den Anhang 2 der N-IOP-Verordnung, der einen Datenkatalog der Identitätsbestätigungsdatei des MID enthält. Die zugehörige Zugriffsmatrix orientiert sich an Artikel 23 N-IOP-Verordnung, der die manuelle Verifizierung einer gelben Verknüpfung regelt, sowie Artikel 24 N-IOP-Verordnung, der den Zugriff auf Daten aus Verknüpfungen bestimmt. Demnach können Behörden, die für die manuelle Verifizierung der verschiedenen Identitäten zuständig sind, die Identitätsbestätigungsdatei inkl. gelber Verknüpfung abfragen (vgl. Art. 110*g* Abs. 2 i.V.m. Art. 110*f* Abs. 2 und 4 AIG). Behörden, die auf mindestens eines der Informationssysteme nach Artikel 110*a* AIG oder Artikel 16*a* BPI Zugriff haben, zwischen denen eine rote Verknüpfung vorliegt, dürfen die Daten abfragen, die in der Identitätsbestätigungsdatei nach Artikel 34 Buchstaben a und b der EU-IOP-Verordnungen bzw. in Artikel 26 Buchstaben a und b der vorliegenden Verordnung gespeichert sind (Art. 24 Abs. 1 N-IOP-Verordnung). Ebenso dürfen Behörden, die auf die Informationssysteme nach Artikel 110*a* AIG oder Artikel 16*a* BPI Zugriff haben, zwischen denen eine weisse Verknüpfung erstellt wurde, die Identitätsbestätigungsdatei nach Artikel 26 dieser Verordnung abfragen (Art. 24 Abs. 2 N-IOP-Verordnung). Schliesslich dürfen die Behörden, die auf die Informationssysteme nach Artikel 110*a* AIG oder Artikel 16*a* BPI Zugriff haben, zwischen denen eine grüne Verknüpfung erstellt wurde, die Identitätsbestätigungsdatei nach Artikel 26 dieser Verordnung abfragen, wenn die Abfrage eine Übereinstimmung bei den verknüpften Daten ergeben hat (Art. 24 Abs. 3 N-IOP-Verordnung). Die oben genannten Rechte auf die Daten nach Absatz 1 werden im Anhang 2 illustriert.

Artikel 27

Artikel 27 N-IOP-Verordnung äussert sich zur Speicherung der Daten in der Identitätsbestätigungsdatei. Entsprechend den Ausführungen zum sBMS und zum CIR (vgl. Erläuterungen zu Art. 6 und 15), werden die Identitätsbestätigungsdateien und die in ihnen enthaltenen Daten nur so lange gespeichert, wie die verknüpften Daten in den zugrundeliegenden Informationssystemen gespeichert sind. Sie werden automatisch aus dem MID gelöscht. Die Bestimmung übernimmt den Regelungsgehalt von Artikel 35 der EU-IOP-Verordnungen.

Artikel 28

Artikel 28 N-IOP-Verordnung regelt die Protokollierung der Daten im MID. Jede Abfrage des MID ist in einem Protokoll festzuhalten. Die Protokollierung soll durch den Bund erfolgen, wobei dort diejenige Behörde zuständig ist, die das zugrundeliegende Schengen/Dublin-Informationssystem abfragt. Diese Verpflichtung folgt aus Artikel 36 Absatz 2 der EU-IOP-Verordnungen. Dementsprechend führt jeder Mitgliedsstaat Protokolle über die Abfragen, die die von ihm autorisierten Behörden durchführen. Die Protokolle stellen sicher, dass die durch den 6. Abschnitt der vorliegenden Verordnung eingeräumten Rechte der betroffenen Personen effektiv wahrgenommen

werden können. Folgende Informationen sind von der abfragenden Behörde zu protokollieren: die abfragende Nutzerin oder der abfragende Nutzer, wobei ersichtlich wird, welcher Behörde diese Person angehört (Bst. a), der Zweck des Zugriffs der Nutzerin oder des Nutzers (Bst. b), das Datum und Uhrzeit der Abfrage (Bst. c) und die Art der für die Abfrage verwendeten Daten (Bst. d).

6. Abschnitt

Der 6. Abschnitt regelt die Rechte der Personen, die in den Schengen/Dublin-Informationssystemen und deren Komponenten verzeichnet sind.

Artikel 29

Artikel 29 Absatz 1 N-IOP-Verordnung regelt die Rechte der in den Schengen/Dublin-Informationssystemen aufgeführten Personen auf Auskunft, Berichtigung und Löschung von Daten. Dazu verweist er auf die Verordnungen, die die entsprechenden Systeme regeln. Bei Einträgen aus dem N-SIS richtet sich das Verfahren nach den Artikeln 50 und 51 der N-SIS-Verordnung (Bst. a). Auch bei Einträgen im C-VIS, EES und ETIAS richtet sich das Verfahren nach den Verordnungen, die die entsprechenden Systeme regeln. Die Verordnungen zum C-VIS, EES und ETIAS befinden sich derzeit in Ausarbeitung. Die einschlägigen Bestimmungen werden deswegen zu einem späteren Zeitpunkt ergänzt. Aufgrund der noch nicht erfolgten Übernahme der revidierten Eurodac-Verordnung kann aktuell auf einen Verweis auf Eurodac verzichtet werden

Artikel 29 Absatz 2 N-IOP-Verordnung stellt klar, dass Gesuche um Auskunft, Berichtigung und Löschung von Verknüpfungen und Daten im MID sowie von Daten im CIR an das SEM zu richten sind. Hintergrund sind die Artikel 8 und 21 N-IOP-Verordnung, die die Verantwortung für die Datenverarbeitung im CIR bzw. MID regeln. Demnach ist das SEM für die Verarbeitung von Daten im CIR zuständig. Das SEM ist auch für die Datenverarbeitung im MID verantwortlich, soweit es Daten in der Identitätsbestätigungsdatei hinzufügt oder ändert, die die von ihm betriebenen Informationssysteme betreffen. Vorliegend rechtfertigt es sich deswegen, das SEM als Anlaufstelle für Gesuche um Auskunft, Berichtigung und Löschung von Verknüpfungen und Daten im MID sowie von Daten im CIR zu bezeichnen. So werden voraussichtlich die meisten Verknüpfungen im MID *ausschliesslich* Informationssysteme des SEM betreffen (VIS, EES, ETIAS). Konkret ist das schriftliche Gesuch an die MID-Expertenstelle beim SEM zu richten, die zur Unterstützung der manuellen Verifizierung von MID-Verknüpfungen geschaffen wird. Ergibt die Prüfung des Gesuchs durch die MID-Expertenstelle, dass eine andere Behörde als das SEM zuständig ist (also in Fällen, in denen das N-SIS betroffen ist), nimmt sie mit dieser Behörde Kontakt auf. Letztere prüft die Gründe und berichtigt oder löscht die entsprechenden Verknüpfungen und Daten im MID bzw. CIR gegebenenfalls. Das SEM gibt der antragstellenden Person (im Anschluss) Auskunft (vgl. dazu auch Abs. 3).

Artikel 29 Absatz 3 N-IOP-Verordnung stellt klar, dass das SEM die Gesuche gemäss Absatz 2 nach Rücksprache mit der Behörde bearbeitet, welche die Daten eingetragen hat oder hat eintragen lassen. Während das SEM für die Datenbearbeitung im CIR zuständig ist (Art. 8), sind das SEM und fedpol für die Datenbearbeitung im MID verantwortlich (Art. 21). Sofern eine MID-Verknüpfung mit dem SIS besteht, nimmt das SEM Rücksprache mit fedpol. Andernfalls wird mit den zuständigen SEM-internen Stellen Rücksprache genommen. Damit wird sichergestellt, dass die Gründe für eine Eintragung hinreichend bekannt sind.

Artikel 29 Absatz 4 N-IOP-Verordnung sieht vor, dass eine Person, deren personenbezogene Daten im MID gespeichert werden, um Berichtigung oder Löschung gemäss Artikel 48 der EU-IOP-Verordnungen ersuchen kann. Das Gesuch enthält die zur Identifizierung der betroffenen Person notwendigen Informationen (diese Informationen dürfen ausschliesslich für die Wahrnehmung der Rechte der betroffenen Person verwendet werden und sind anschliessend unverzüglich zu löschen). Zuständig für die Überprüfung und gegebenenfalls Berichtigung oder Löschung der Gesuche ist die nach Artikel 22 N-IOP-Verordnung für die manuelle Verifizierung einer gelben Verknüpfung zuständige Behörde. Werden Daten berichtigt oder gelöscht, wird die betroffene Person schriftlich darüber informiert. Ist die für die manuelle Verifizierung einer gelben Verknüpfung zuständige Behörde nicht der Auffassung, dass die im MID gespeicherten Daten unrichtig sind oder unrechtmässig gespeichert wurden, so erlässt sie eine anfechtbare Verfügung. Darin erläutert sie, warum sie nicht zu einer Berichtigung oder Löschung bereit ist. Die Verfügung hat eine Rechtsmittelbelehrung zu enthalten und kann bei einem Gericht angefochten werden; es gilt der ordentliche Rechtsmittelweg.

Artikel 30

Artikel 30 Absatz 1 N-IOP-Verordnung bestimmt, dass die kantonalen Datenschutzbehörden und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) im Rahmen ihrer jeweiligen Zuständigkeit zusammenarbeiten und die Aufsicht über die Bearbeitung von Personendaten koordinieren. Hintergrund ist Artikel 51 der EU-IOP-Verordnungen, der vorschreibt, dass unabhängige Aufsichtsbehörden die Rechtmässigkeit der im Rahmen der Interoperabilität vorgenommenen Verarbeitung personenbezogener Daten überwachen. In der Schweiz kommen den kantonalen Datenschutzbehörden und dem EDÖB diese Funktion zu.

Artikel 30 Absatz 2 N-IOP-Verordnung schreibt vor, dass der EDÖB bei der Wahrnehmung seiner Aufgaben mit dem Europäischen Datenschutzbeauftragten zusammenarbeitet. Für letzteren stellt der EDÖB die nationale Ansprechstelle dar. Die Norm lehnt sich an Artikel 22 der EES-Verordnung an, die derzeit ausgearbeitet wird.

Artikel 30 Absatz 3 N-IOP-Verordnung verweist für die weiteren Einzelheiten auf Artikel 51 der

EU-IOP-Verordnungen. Damit wird klargestellt, dass die beiden EU-IOP-Verordnungen die Grundlage für die Aufsicht über die Datenbearbeitung sind. So stellt der EDÖB unter anderem sicher, dass mindestens alle vier Jahre die durch die zuständigen nationalen Behörden erfolgenden Verarbeitungsvorgänge von personenbezogenen Daten überprüft werden. Er veröffentlicht jährlich die Zahl der Anträge auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung personenbezogener Daten, die getroffenen Folgemassnahmen und die Zahl der Berichtigungen, Löschungen und Einschränkungen der Verarbeitung, die auf Antrag der betroffenen Personen vorgenommen wurden.

7. Abschnitt

Der 7. Abschnitt gibt Auskunft über die Datensicherheit.

Artikel 31

Artikel 31 Absatz 1 N-IOP-Verordnung regelt die Datensicherheit. Demnach gelten für die Gewährleistung der Datensicherheit die Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (SR 172.010.58) sowie die Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (SR 120.73). Diesbezüglich ist auch auf Artikel 42 Absatz 1 und 4 der EU-IOP-Verordnungen hinzuweisen, der die Sicherheit der Verarbeitung personenbezogener Daten zum Inhalt hat.

Artikel 31 Absatz 2 N-IOP-Verordnung soll sicherstellen, dass die Behörden, welche Zugang zu den Interoperabilitätskomponenten haben, die nach den datenschutzrechtlichen Bestimmungen erforderlichen organisatorischen und technischen Massnahmen treffen, um den Zugriff unbefugter Personen auf die Daten zu verhindern. Diese Massnahmen haben den in Artikel 42 Absatz 3 der EU-IOP-Verordnungen aufgeführten Sicherheitsmassnahmen zu entsprechen (siehe dazu Art. 42 Abs. 2 der EU-IOP-Verordnungen).

8. Abschnitt

Der 8. Abschnitt regelt in *Artikel 32* N-IOP-Verordnung das Inkrafttreten der Verordnung. Das Datum der Inkraftsetzung wird zu einem späteren Zeitpunkt ergänzt.

3. Künftige Anpassungen weiterer Verordnungen

3.1. Verordnungen, die Schengen/Dublin-Informationssysteme regeln

Mehrere Verordnungen, die Schengen/Dublin-Informationssysteme regeln, müssen aufgrund der Interoperabilität überarbeitet werden. So wird in der nationalen EES-Verordnung unter anderem festzulegen sein, welche Daten auch im CIR gespeichert und wann die Daten gelöscht werden. Weiter erfordert die nationale ETIAS-Verordnung eine Anpassung in Bezug auf die Daten, die

ebenfalls im CIR gespeichert werden. Diese Verordnung wird demnächst ausgearbeitet und soll im Dezember 2022 in Kraft treten. Auch die nationale VIS-Verordnung wird in naher Zukunft anzupassen sein, ebenfalls in Bezug auf die Daten, die auch im CIR gespeichert werden. Schliesslich wird das Projekt zur Überarbeitung von Eurodac das System mit den anderen Informationssystemen interoperabel machen. Hierfür wird eine nationale Eurodac-Verordnung erarbeitet, die alle relevanten Elemente im Zusammenhang mit der Interoperabilität enthält. Die Entwicklung von Eurodac ist derzeit Teil des europäischen Migrationspakts und sollte gleichzeitig mit dem Pakt auf europäischer Ebene genehmigt werden. Letztlich wurde auch eine Trennung des Projektes vom Migrationspakt thematisiert, die eine frühere Inkraftsetzung der Interoperabilität mit Eurodac erlauben würde. In den genannten Verordnungen muss auch ein neues Verfahren für den Zugang der Strafverfolgungsbehörden zu den Systemen EES, VIS und ETIAS nach einer Abfrage des CIR vorgesehen werden. Die Verordnungen werden so angepasst, dass beide Möglichkeiten der Abfrage möglich sind. Den Vorrang wir jedoch der Abfrage des CIR gegeben. Da die vorstehend genannten Verordnungen teilweise noch nicht vorliegen, ist es zum jetzigen Zeitpunkt nicht möglich, eine abschliessende Liste aller Verordnungsänderungen zu erstellen. Diese werden jedoch minim sein.

3.2. Andere Verordnungen

Auch andere Verordnungen bedürfen aufgrund der Interoperabilität einer Anpassung. Es ist vorgesehen, dass Artikel 19 Absatz 1 der Verordnung über das Zentrale Migrationsinformationssystem (ZEMIS-Verordnung, SR 142.513) dahingehend geändert wird, dass er nicht mehr auf Artikel 111*f* AIG verweist, da dieser mit dem Inkrafttreten der neuen Struktur des AIG, die durch den Bundesbeschluss zu IOP eingeführt wird, aufgehoben wird (BBl 2021 674). Auch Artikel 87*a* der Verordnung über Zulassung, Aufenthalt und Erwerbstätigkeit (VZAE, SR 142.201) soll dahingehend geändert werden, dass er nicht mehr auf Artikel 111*i* AIG verweist, sondern auf den neuen Artikel 109*k* AIG, der mit dem Bundesbeschluss zu IOP geschaffen wird.

4. Finanzielle und personelle Auswirkungen

4.1. Finanzielle und personelle Auswirkungen auf den Bund

Mit der N-IOP-Verordnung sind keine zusätzlichen Kosten zu erwarten gegenüber den in der Botschaft dargelegten Schätzungen (BBl 2020 7983, hier 8048-8054). Für den Bund ergeben sich sowohl in der Projektphase als auch in der Anwendung der EU-IOP-Verordnungen ab Inbetriebnahme finanzielle und personelle Auswirkungen. Die Interoperabilität ist Teil des Programms Schengen-Weiterentwicklungen des EJPD. Die Projekte bei fedpol und beim SEM sind Bestandteil eines Verpflichtungskredites zur Weiterentwicklung des Schengen/Dublin-Besitzstands. Die Gesamtkosten der Interoperabilitätsprojekte für den Bund belaufen sich für die gesamte Zeitspanne von 2020 bis 2025 geschätzt auf 21 Millionen Franken. 2023 entstehen voraussichtlich

Betriebskosten von 0,2 Millionen Franken und ab 2024 von jährlich circa 2 Millionen Franken. Insgesamt entsteht ein personeller Mehrbedarf von 20 FTE sowie zwei FTE für die technische Anwendungsverantwortung.

4.2. Finanzielle und personelle Auswirkungen auf die Kantone

Der für die Kantone entstehende Mehraufwand ist in der Botschaft genauer dargelegt (BBl 2020 7983, hier 8053). Die kantonalen Migrations- und Polizeibehörden werden die Interoperabilität für ihre Tätigkeiten nutzen können. Dies wird technische und prozessuale Anpassungen bei den kantonalen Abfragesystemen nötig machen. Aktuell werden diese in enger Zusammenarbeit zwischen Bund und Kantonen identifiziert. Der Bund wird die Kantone mit einer MID-Expertenstelle bei der Verifizierung von Identitäten entlasten.

5. Rechtliche Aspekte

5.1. Verfassungsmässigkeit

Die Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der EU-IOP-Verordnungen stützen sich auf Artikel 54 Absatz 1 BV und wurden der Bundesversammlung zur Genehmigung vorgelegt.[22]

Die vorliegende Vorlage berücksichtigt die verfassungsrechtlichen Vorgaben und stellt namentlich sicher, dass verfahrensrechtliche Garantien sichergestellt sind (vgl. 6. Abschnitt). In Anbetracht der vorgesehenen Rechtsgrundlagen und der bereits gesetzlich garantierten Grundsätze des Datenschutzes und der Datensicherheit erscheinen die bereits auf Gesetzesstufe vorgesehenen Grundrechtseingriffe als verhältnismässig im Hinblick auf das verfolgte Ziel (Art. 36 Abs. 1-3 BV).

5.2. Vereinbarkeit mit den internationalen Verpflichtungen der Schweiz

Die Verordnungsanpassungen stehen im Einklang mit internationalem Recht. 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 Anpassungen mit den internationalen Verpflichtungen der Schweiz vereinbar.

5.3. Erlassform

Mit dieser Vorlage werden die für die Umsetzung der Interoperabilität notwendigen Anpassungen

[22] IOP-Botschaft, BBl 2020 8054 f.

auf Verordnungsstufe vorgenommen. Dies sind zum einen die zur Umsetzung der Gesetzesänderungen notwendigen Verordnungsanpassungen. Weiter bedürfen gewisse Bestimmungen der EU-IOP-Verordnungen einer Konkretisierung auf Verordnungsstufe. Zusätzlich sollen die bisher notifizierten tertiären Rechtsakte (Durchführungsbeschlüsse) zur Interoperabilität umgesetzt werden. Zu diesen Zwecken soll die obgenannte Verordnung über die Interoperabilität zwischen den Schengen-Dublin-Informationssystemen, sog. N-IOP-Verordnung, geschaffen werden.

6. Datenschutz

Aufgrund der Einführung der neuen Zentralkomponenten, welche Einfluss auf alle Schengen/Dublin-Informationssysteme haben, wurden auf Gesetzesstufe notwendige Anpassungen gemacht, unter anderem zum Datenschutz (vgl. 14. Kapitel, 14*a*. Kapitel, 14*b*. Kapitel und 14*c*. Kapitel AIG). Auch in der vorliegenden Vorlage finden sich Bestimmungen zum Datenschutz (vgl. 6. Abschnitt, 7. Abschnitt).