EUROPÄISCHE
KOMMISSION

Straßburg, den 12.12.2017
COM(2017) 794 final

2017/0352 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration)

{SWD(2017) 473} - {SWD(2017) 474}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Hintergrund des Vorschlags

In den vergangenen drei Jahren war die EU mit einem Anstieg der Zahl der irregulären Grenzübertritte in die EU und – wie etliche Terroranschläge gezeigt haben – mit einer sich wandelnden, ständig präsenten Bedrohung der inneren Sicherheit konfrontiert. Die Bürgerinnen und Bürger der EU erwarten, dass die Personenkontrollen an den Außengrenzen und die Kontrollen innerhalb des Schengen-Raums so wirkungsvoll sind, dass sie eine effektive Steuerung der Migration ermöglichen und zur inneren Sicherheit beitragen. Diese Herausforderungen haben stärker verdeutlicht, dass die Informationsinstrumente der EU für Grenzmanagement, Migration und Sicherheit dringend zusammengeführt und umfassend gestärkt werden müssen.

Das Informationsmanagement in der EU kann und muss unter uneingeschränkter Achtung der Grundrechte, insbesondere des Rechts auf Schutz personenbezogener Daten, wirksamer und effizienter gestaltet werden, um einen besseren Schutz der EU-Außengrenzen zu gewährleisten, die Migrationssteuerung zu verbessern und die innere Sicherheit zum Wohl aller Bürger zu erhöhen. Auf EU-Ebene gibt es bereits eine Reihe von Informationssystemen, und es werden weitere Systeme entwickelt, um für Grenzschutz-, Einwanderungs- und Strafverfolgungsbeamte relevante personenbezogene Informationen bereitzustellen. Damit diese Unterstützung wirksam ist, müssen die von den EU-Informationssystemen gelieferten Informationen vollständig, präzise und zuverlässig sein. Allerdings weist die Informationsverwaltungsarchitektur der EU strukturelle Mängel auf. Die nationalen Behörden sehen sich einer komplexen Landschaft unterschiedlich geregelter Informationssysteme gegenüber. Da die Informationen jeweils getrennt in nicht miteinander verbundenen Systemen gespeichert werden, ergibt sich zudem eine Fragmentierung der Datenverwaltungsarchitektur für das Grenzmanagement und die Sicherheit. Dies führt zu Informationslücken. Folglich sind **die verschiedenen Informationssysteme auf EU-Ebene derzeit nicht interoperabel**, d. h. nicht in der Lage, Daten und Informationen auszutauschen, damit die Behörden und zuständigen Beamten die von ihnen benötigten Informationen erhalten, und zwar wann und wo sie diese benötigen. Die Interoperabilität der Informationssysteme auf EU-Ebene kann erheblich dazu beitragen, die derzeitigen Informationslücken zu schließen, aufgrund deren es möglich ist, dass Personen, einschließlich solcher, die unter Umständen an terroristischen Handlungen beteiligt sind, in verschiedenen, nicht miteinander verbundenen Datenbanken unter unterschiedlichen Aliasnamen erfasst werden.

Im April 2016 legte die Kommission die **Mitteilung *Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit***[1] vor, in der einige strukturelle Mängel der Informationssysteme aufgezeigt wurden.[2] Mit der Mitteilung vom April 2016 sollte eine Diskussion darüber angestoßen werden, wie die Informationssysteme in der Europäischen Union zu einem besseren Grenzmanagement, einer wirksameren Migrationssteuerung und einem höheren Maß an innerer Sicherheit beitragen können. Der

[1] COM(2016) 205 vom 6. April 2016.

[2] 1) suboptimale Funktionen in einigen der bestehenden Informationssysteme, 2) Informationslücken in der Datenverwaltungsarchitektur der EU, 3) die komplexe Landschaft unterschiedlich geregelter Informationssysteme und 4) die Fragmentierung der Datenverwaltungsarchitektur für das Grenzmanagement und die Sicherheit, in der Daten jeweils getrennt in nicht miteinander verbundenen Systemen gespeichert werden, wodurch Informationslücken entstehen.

Rat räumte seinerseits ebenfalls ein, dass in diesem Bereich dringender Handlungsbedarf besteht. Im Juni 2016 billigte er einen **Fahrplan zur Verbesserung des Informationsaustauschs und des Informationsmanagements** einschließlich von Interoperabilitätslösungen im Bereich Justiz und Inneres[3]. Ziel des Fahrplans war die Unterstützung von operativen Untersuchungen und die rasche Bereitstellung von umfassenden, aktuellen und hochwertigen Informationen für die Anwender an vorderster Front – wie Polizei- und Grenzschutzbeamte, Staatsanwälte, Einwanderungsbeamte und andere –, damit diese wirksam zusammenarbeiten und handeln können. Auch das **Europäische Parlament** drängte auf Maßnahmen in diesem Bereich. In seiner Entschließung vom Juli 2016[4] zum Arbeitsprogramm der Kommission für 2017 hat es diese aufgefordert, „*Vorschläge für die Verbesserung und Weiterentwicklung von bestehenden Informationssystemen, die Schließung von Informationslücken und Wege hin zur Interoperabilität sowie Vorschläge für einen zwingend vorgeschriebenen Informationsaustausch auf EU-Ebene mit den erforderlichen Datenschutzvorkehrungen vorzulegen*“. In Präsident Junckers Rede zur Lage der Union vom September 2016[5] und den Schlussfolgerungen des Europäischen Rates vom Dezember 2016[6] wurde betont, dass die derzeitigen Mängel bei der Datenverwaltung beseitigt und die Interoperabilität der bestehenden Informationssysteme verbessert werden müssen.

Als Folgemaßnahme zu der Mitteilung vom April 2016 setzte die Kommission im Juni 2016 eine **hochrangige Expertengruppe für Informationssysteme und Interoperabilität**[7] ein, die sich mit den rechtlichen, technischen und operativen Herausforderungen einer besseren Interoperabilität zwischen den zentralen EU-Systemen in den Bereichen Grenzmanagement und Sicherheit, einschließlich der Notwendigkeit, technischen Durchführbarkeit, Verhältnismäßigkeit und der datenschutzrelevanten Auswirkungen dieser Systeme, auseinandersetzen sollte. Der **Abschlussbericht** der hochrangigen Expertengruppe wurde im Mai 2017 veröffentlicht.[8] Er enthält eine Reihe von Empfehlungen zur Stärkung und Weiterentwicklung der EU-Informationssysteme und ihrer Interoperabilität. Die Agentur der EU für Grundrechte, der Europäische Datenschutzbeauftragte und der EU-Koordinator für die Terrorismusbekämpfung beteiligten sich aktiv an der Arbeit der Expertengruppe. Jede dieser Stellen gab unterstützende Erklärungen ab, wies allerdings gleichzeitig darauf hin, dass im Zuge des weiteren Vorgehens umfassendere Grundrechts- und Datenschutzaspekte erörtert werden müssten. Vertreter des Sekretariats des Ausschusses des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres und des Generalsekretariats des Rates nahmen als Beobachter teil. Die hochrangige Expertengruppe kam zu dem Schluss, dass **es notwendig und technisch möglich ist, auf praktische Lösungen für die Interoperabilität hinzuarbeiten,** und dass solche Lösungen grundsätzlich sowohl operative Verbesserungen bewirken als auch im Einklang mit den Datenschutzvorschriften umgesetzt werden können.

Auf der Grundlage des Berichts und der Empfehlungen der Expertengruppe erläuterte die Kommission in ihrer Mitteilung *Auf dem Weg zu einer wirksamen und echten*

---

3 Fahrplan vom 6. Juni 2016 zur Verbesserung des Informationsaustauschs und des Informationsmanagements einschließlich von Interoperabilitätslösungen im Bereich Justiz und Inneres (9368/1/16, REV 1).

4 Entschließung des Europäischen Parlaments vom 6. Juli 2016 zu den strategischen Prioritäten für das Arbeitsprogramm der Kommission für 2017 (2016/2773(RSP).

5 Lage der Union 2016 (14.9.2016), https://ec.europa.eu/commission/state-union-2016_de.

6 Schlussfolgerungen des Europäischen Rates vom 15.12.2016, http://www.consilium.europa.eu/media/21929/15-euco-conclusions-final.pdf.

7 Beschluss der Kommission vom 17. Juni 2016 zur Einsetzung der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität (2016/C 257/03).

8 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1

Sicherheitsunion – Siebter Fortschrittsbericht[9] ein **neues Konzept für die Verwaltung von Daten** in den Bereichen Grenzmanagement, Sicherheit und Migrationssteuerung, das unter uneingeschränkter Achtung der Grundrechte die Interoperabilität aller zentralen EU-Informationssysteme in den genannten Bereichen gewährleistet. Die Kommission kündigte an, sie werde ihre Arbeiten an einem Europäischen Suchportal fortsetzen, das die gleichzeitige Abfrage aller einschlägigen EU-Systeme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung ermöglicht – gegebenenfalls mit einheitlicheren Regeln für den Zugang der Strafverfolgungsbehörden –, und sie werde für diese Systeme einen gemeinsamen Dienst für den Abgleich biometrischer Daten (möglicherweise mit einer Trefferkennzeichnungsfunktion[10]) und einen gemeinsamen Speicher für Identitätsdaten entwickeln. Sie bekundete zudem ihre Absicht, so bald wie möglich einen Legislativvorschlag zur Interoperabilität vorzulegen.

Der Europäische Rat bekräftigte in seinen Schlussfolgerungen vom Juni 2017[11], dass gehandelt werden muss. Auf der Grundlage der Schlussfolgerungen des Rates „Justiz und Inneres“ vom Juni 2017[12] forderte der Europäische Rat die Kommission auf, so bald wie möglich Legislativvorschläge zur Umsetzung der Empfehlungen der hochrangigen Expertengruppe auszuarbeiten. Mit dieser Initiative wird auch der Forderung des Rates nach einem umfassenden Rahmen für den Zugang der Strafverfolgungsbehörden zu den verschiedenen Datenbanken im Bereich Justiz und Inneres im Hinblick auf eine stärkere Vereinfachung, eine größere Einheitlichkeit und Wirksamkeit sowie eine bessere Berücksichtigung operativer Erfordernisse entsprochen.[13] Um dem Engagement für eine sicherere Gesellschaft in der Europäischen Union unter uneingeschränkter Wahrung der Grundrechte Nachdruck zu verleihen, hat die Kommission im Rahmen ihres Arbeitsprogramms für 2018[14] angekündigt, bis Ende 2017 einen Vorschlag über die Interoperabilität der Informationssysteme vorzulegen.

- **Ziele des Vorschlags**

Die allgemeinen Ziele dieses Vorschlags resultieren aus den im Vertrag verankerten Zielen einer Verbesserung des Grenzmanagements an den Schengen-Außengrenzen und eines Beitrags zur inneren Sicherheit der Europäischen Union. Sie ergeben sich auch aus politischen Entscheidungen der Kommission und aus den einschlägigen Schlussfolgerungen des (Europäischen) Rates. Diese Ziele wurden in der Europäischen Migrationsagenda und den nachfolgenden Mitteilungen weiter ausgearbeitet, unter anderem in der Mitteilung „Schengen bewahren und stärken“[15], der Europäischen Sicherheitsagenda[16] sowie den Arbeiten und

---

9 COM(2017) 261 final.

10 Neues Konzept des „eingebauten Datenschutzes“ (privacy by design), wodurch der Zugang zu sämtlichen Daten insofern eingeschränkt wird, als lediglich mitgeteilt wird, ob die entsprechenden Daten vorhanden sind oder nicht („Treffer/kein Treffer“).

11 Schlussfolgerungen des Europäischen Rates vom 22./23 Juni 2017.

12 Ergebnisse der 3546. Tagung des Rates „Justiz und Inneres“ vom 8./9. Juni 2017 (10136/17).

13 Am 2. März 2017 erteilte der Ausschuss der Ständigen Vertreter (AStV) des Rates dem Ratsvorsitz ein Mandat für die Aufnahme von interinstitutionellen Verhandlungen über das Einreise-/Ausreisesystem der EU und stimmte anschließend dem Entwurf einer Erklärung des Rates zu, in der die Kommission aufgefordert wurde, einen umfassenden Rahmen für den Zugang der Strafverfolgungsbehörden zu den verschiedenen Datenbanken im Bereich Justiz und Inneres im Hinblick auf eine stärkere Vereinfachung, eine größere Einheitlichkeit und Wirksamkeit sowie eine bessere Berücksichtigung operativer Erfordernisse vorzuschlagen (Kurzniederschrift 7177/17 vom 21.3.2017).

14 COM(2017) 650 final.

15 COM(2017) 570 final.

16 COM(2015) 185 final.

Fortschrittsberichten der Kommission im Hinblick auf eine wirksame und echte Sicherheitsunion[17].

Die Ziele des vorliegenden Vorschlags basieren zwar vor allem auf der Mitteilung vom April 2016 und den Erkenntnissen der hochrangigen Expertengruppe, sind aber auch untrennbar mit den vorstehenden Vorgaben verbunden.

Die spezifischen Ziele dieses Vorschlags lauten:

1) Gewährleistung, dass die Endnutzer, insbesondere Grenzschutz- und Strafverfolgungsbeamte sowie Mitarbeiter von Einwanderungs- und Justizbehörden, einen **raschen, unterbrechungsfreien, systematischen und kontrollierten Zugang** zu den Informationen haben, die sie benötigen, um ihren Aufgaben nachzukommen,

2) Bereitstellung einer Lösung für die **Aufdeckung von Mehrfachidentitäten**, die mit ein und demselben Satz biometrischer Daten verknüpft sind, um zugleich eine korrekte Identifizierung von Bona-fide-Reisenden sicherzustellen und **Identitätsbetrug zu bekämpfen**,

3) Vereinfachung der **Identitätsprüfung von Drittstaatsangehörigen** im Hoheitsgebiet eines Mitgliedstaats durch Polizeibehörden und

4) Erleichterung und **einheitliche Regelung des Zugangs der Strafverfolgungsbehörden** zu den Informationssystemen anderer Behörden auf EU-Ebene, wenn dies für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung terroristischer und sonstiger schwerer Straftaten notwendig ist.

Der vorliegende Vorschlag wird nicht nur zur Verwirklichung dieser vorrangigen operativen Ziele, sondern auch zu Folgendem beitragen:

- Erleichterung der technischen und der operativen **Umsetzung** bestehender und künftiger Informationssysteme **durch die Mitgliedstaaten**,
- Verschärfung und Vereinheitlichung der für die einzelnen Systeme geltenden **Bedingungen für die Sicherheit und den Schutz der Daten** und
- Verbesserung und Harmonisierung der **Datenqualitätsanforderungen** der einzelnen Systeme.

Des Weiteren enthält der Vorschlag Bestimmungen für die Einführung und Regelung des universellen Nachrichtenformats (Universal Message Format – UMF) als EU-Standard für die Entwicklung von Informationssystemen im Bereich Justiz und Inneres sowie für die Einrichtung eines zentralen Speichers für Berichte und Statistiken.

- **Anwendungsbereich des Vorschlags**

Zusammen mit dem am selben Tag vorgelegten Parallelvorschlag betrifft dieser Interoperabilitätsvorschlag die auf zentraler Ebene betriebenen EU-Informationssysteme für die Bereiche Sicherheit, Grenzmanagement und Migrationssteuerung, von denen drei bereits

[17] COM(2016) 230 final.

vorhanden sind, eines nahezu entwickelt ist und zwei weitere derzeit als Vorschläge von den beiden gesetzgebenden Organen erörtert werden. Die Ziele, Zwecke, Rechtsgrundlagen, Regeln, Nutzergruppen und institutionellen Rahmenbedingungen sind systemspezifisch.

Bislang bestehen die folgenden drei zentralen Informationssysteme:

- das **Schengener Informationssystem (SIS)** mit einem breiten Spektrum von Personenfahndungsausschreibungen (Einreise- oder Aufenthaltsverweigerung, Europäischer Haftbefehl, Vermisste, Teilnahme an einem Gerichtsverfahren, verdeckte und gezielte Kontrolle) und Sachfahndungsausschreibungen (einschließlich verlorener, gestohlener und für ungültig erklärter Identitäts- oder Reisedokumente)[18];
- das System **Eurodac** mit Fingerabdruckdaten von Asylbewerbern und Drittstaatsangehörigen, die die Außengrenzen irregulär überschritten haben oder sich illegal in einem Mitgliedstaat aufhalten, und
- das **Visa-Informationssystem (VIS)** mit Daten über Kurzaufenthaltsvisa.

Zusätzlich zu diesen bestehenden Systemen schlug die Kommission 2016/2017 drei neue zentrale EU-Informationssysteme vor:

- das **Einreise-/Ausreisesystem (EES)**, über dessen Rechtsgrundlage unlängst Einigung erzielt wurde und das das derzeitige System des manuellen Abstempelns der Reisepässe ersetzen wird; im EES sollen der Name des Reisenden, die Art des Reisedokuments, biometrische Daten sowie Zeitpunkt und Ort der Ein- und der Ausreise von Drittstaatsangehörigen, die für einen Kurzaufenthalt in den Schengen-Raum reisen, elektronisch erfasst werden;
- das vorgeschlagene **Europäische Reiseinformations- und -genehmigungssystem (ETIAS)**, bei dem es sich – nach seiner Annahme – um ein weitgehend automatisiertes System zur Erfassung und Überprüfung der Angaben handeln würde, die von der Visumpflicht befreite Drittstaatsangehörige vor ihrer Reise in den Schengen-Raum übermitteln, und
- das vorgeschlagene **Europäische Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN)**, bei dem es sich um ein elektronisches System für den Austausch von Informationen über frühere Verurteilungen von Drittstaatsangehörigen durch Strafgerichte in der EU handeln würde.

Diese sechs Systeme ergänzen einander, und zielen – mit Ausnahme des Schengener Informationssystems (SIS) – ausschließlich auf Drittstaatangehörige ab. Mit den Systemen werden die nationalen Behörden beim Grenzmanagement, bei der Migrationssteuerung, der Visabearbeitung und der Asylgewährung sowie bei der Bekämpfung von Kriminalität und Terrorismus unterstützt. Letzteres gilt insbesondere für das SIS, das derzeit von den Strafverfolgungsbehörden am stärksten genutzte Instrument für den Informationsaustausch.

Neben diesen auf EU-Ebene zentral verwalteten Informationssystemen umfasst dieser Vorschlag auch die **Interpol**-Datenbank für gestohlene und verlorene Reisedokumente (SLTD), die gemäß den Bestimmungen des Schengener Grenzkodexes an den EU-

[18] In den SIS-Verordnungsentwürfen der Kommission vom Dezember 2016 wird vorgeschlagen, das System dahin gehend auszuweiten, dass Rückkehrentscheidungen und Ermittlungsanfragen einbezogen werden.

Außengrenzen systematisch abgefragt wird, und die Interpol-Datenbank zur Erfassung von Ausschreibungen zugeordneten Reisedokumenten (TDAWN). Außerdem erstreckt er sich auf die **Europol**-Daten, soweit diese für das Funktionieren des vorgeschlagenen Systems ETIAS und für die Unterstützung der Mitgliedstaaten bei der Abfrage von Daten über terroristische und sonstige schwere Straftaten von Bedeutung sind.

Nationale Informationssysteme und dezentrale EU-Informationssysteme sind nicht Teil dieses Vorschlags. Dezentrale Systeme, wie sie beispielsweise auf der Grundlage des Prüm-Rahmens,[19] der Richtlinie über Fluggastdatensätze (PNR-Daten)[20] und der API-Richtlinie[21] betrieben werden, können zu einem späteren Zeitpunkt mit einer oder mehreren der im Rahmen dieser Initiative vorgeschlagenen Komponenten verknüpft werden, sofern nachgewiesen wird, dass dies notwendig ist.[22]

Um der Differenzierung zwischen einerseits Angelegenheiten, die eine Entwicklung des Schengen-Besitzstands im Bereich Grenzen und Visa darstellen, und andererseits sonstigen Systemen, die den Schengen-Besitzstand im Bereich der polizeilichen Zusammenarbeit betreffen oder keinen Bezug zum Schengen-Besitzstand aufweisen, Rechnung zu tragen, geht es bei diesem Vorschlag um den Zugang zu dem derzeit durch den Beschluss 2007/533/JI geregelten Schengener Informationssystem sowie zu Eurodac und [ECRIS-TCN].

- **Zur Herstellung der Interoperabilität erforderliche technische Komponenten**

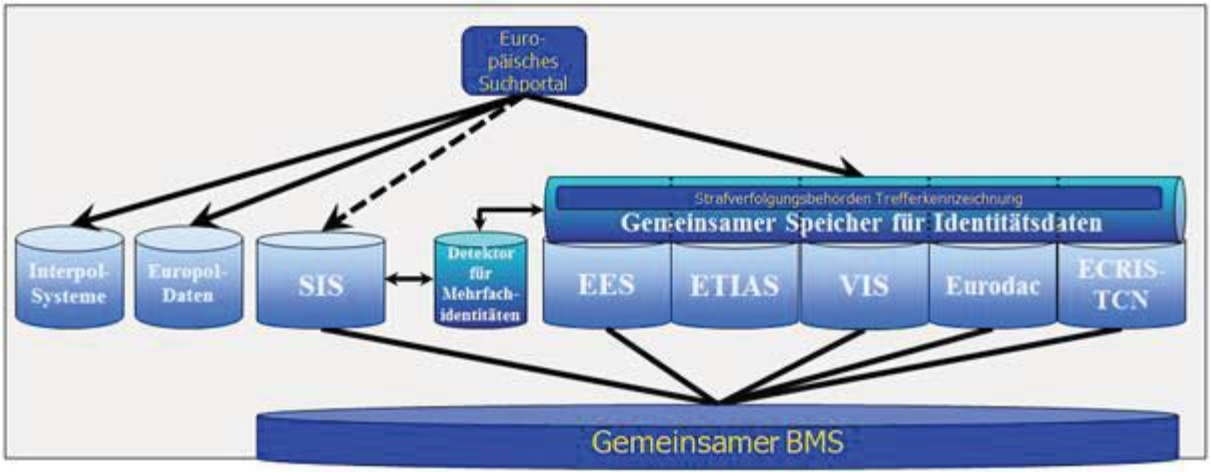
Damit die Ziele dieses Vorschlags erreicht werden können, müssen vier Interoperabilitätskomponenten eingeführt werden:

- Europäisches Suchportal – ESP (European search portal)
- gemeinsamer Dienst für den Abgleich biometrischer Daten – gemeinsamer BMS (biometric matching service)
- gemeinsamer Speicher für Identitätsdaten – CIR (common identity repository)
- Detektor für Mehrfachidentitäten – MID (multiple-identity detector)

Jede dieser Komponenten wird ausführlich in der Arbeitsunterlage der Kommissionsdienststellen über die Folgenabschätzung zu diesem Vorschlag beschrieben.

Zusammen führen die vier Komponenten zu der nachstehend erläuterten Interoperabilitätslösung.

[19] http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1508936184412&uri=CELEX%3A32008D0615
[20] http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1508936384641&uri=CELEX%3A32016L0681
[21] Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln.
[22] In Bezug auf die Zollsysteme forderte der Rat die Kommission in seinen Schlussfolgerungen vom Juni 2017 auf, eine Durchführbarkeitsstudie vorzunehmen, um die fachlichen, operationellen und rechtlichen Aspekte der Interoperabilität der Sicherheits- und Grenzmanagementsysteme mit Zollsystemen weiter auszuloten und dem Rat bis Ende 2018 ihre Erkenntnisse zur Erörterung vorzulegen.



Die Ziele und die Funktionsweise dieser vier Komponenten lassen sich wie folgt zusammenfassen:

1) Das **Europäische Suchportal (ESP)** ist die Komponente, die die gleichzeitige Abfrage mehrerer Systeme (zentrales SIS, Eurodac, VIS, künftiges EES und vorgeschlagene Systeme ETIAS und ECRIS-TCN sowie einschlägige Interpol-Systeme und Europol-Daten) unter Verwendung von Identitätsdaten (sowohl biografischer als auch biometrischer Art) ermöglichen würde. Es würde gewährleisten, dass die Nutzer der EU-Informationssysteme einen raschen, unterbrechungsfreien, effizienten, systematischen und kontrollierten Zugang zu allen Informationen haben, die sie benötigen, um ihren Aufgaben nachzukommen.

   Eine Abfrage über das Europäische Suchportal würde unverzüglich – innerhalb von Sekunden – Informationen aus den verschiedenen Systemen, zu denen der Nutzer rechtmäßig Zugang hat, liefern. Je nach Abfragezweck und den entsprechenden Zugangsrechten würde das ESP mit spezifischen Konfigurationen bereitgestellt.

   Das ESP würde keine neuen Daten verarbeiten und keine Daten speichern; es würde als einzige Schnittstelle („Fenster“) für eine unterbrechungsfreie, unter vollständiger Wahrung der Zugangskontroll- und Datenschutzanforderungen der zugrunde liegenden Systeme erfolgende Abfrage der erforderlichen Informationen in den verschiedenen Zentralsystemen dienen. Das ESP würde die genehmigte, ordnungsgemäße Nutzung der einzelnen bestehenden EU-Informationssysteme erleichtern und den Mitgliedstaaten eine einfachere und kostengünstigere Abfrage und Nutzung der Systeme im Einklang mit den für diese geltenden Rechtsinstrumenten ermöglichen.

2) Der **gemeinsame Dienst für den Abgleich biometrischer Daten (gemeinsamer BMS)** würde die Abfrage und den Abgleich biometrischer Daten (Fingerabdrücke und Gesichtsbilder) aus mehreren Zentralsystemen (insbesondere SIS, Eurodac, VIS, künftiges EES und vorgeschlagenes System ECRIS-TCN) ermöglichen. Das vorgeschlagene System ETIAS wird keine biometrischen Daten enthalten und wäre daher nicht mit dem gemeinsamen BMS verbunden.

Während die einzelnen bestehenden Zentralsysteme (SIS, Eurodac, VIS) derzeit über eine spezielle proprietäre Suchmaschine für biometrische Daten[23] verfügen, würde der gemeinsame Dienst für den Abgleich biometrischer Daten eine gemeinsame Plattform bieten, über die die Daten gleichzeitig abgefragt und abgeglichen werden. Durch den Rückgriff auf eine einzige technologische Komponente (anstatt auf fünf verschiedene) würde der gemeinsame BMS erheblich zur Sicherheit beitragen und beträchtliche finanzielle, wartungstechnische und operative Vorteile bieten. Die biometrischen Daten (Fingerabdrücke und Gesichtsbilder) werden ausschließlich von den zugrunde liegenden Systemen gespeichert. Der gemeinsame BMS würde eine mathematische Repräsentation der biometrischen Proben (Template) generieren und speichern, ohne jedoch die eigentlichen Daten zu erfassen, die somit auch künftig nur einmal an einem einzigen Ort gespeichert würden.

Der gemeinsame BMS würde maßgeblich dazu beitragen, Verbindungen zwischen Datensätzen und von derselben Person verwendeten unterschiedlichen Identitäten in verschiedenen Zentralsystemen aufzudecken. Ohne gemeinsamen BMS wird keine der drei anderen Komponenten funktionieren können.

3) Der **gemeinsame Speicher für Identitätsdaten (CIR)** wäre die gemeinsame Komponente für die Speicherung biografischer[24] und biometrischer Identitätsdaten von Drittstaatsangehörigen, die in Eurodac, im VIS, in dem künftigen EES, dem vorgeschlagenen ETIAS und dem vorgeschlagenen System ECRIS-TCN gespeichert sind. In jedem dieser fünf Zentralsysteme werden biografische Daten zu bestimmten Personen aus bestimmten Gründen erfasst bzw. sollen solche Daten erfasst werden. Dies würde sich nicht ändern. Die entsprechenden Identitätsdaten würden zwar im CIR gespeichert, würden aber weiterhin zu den jeweiligen zugrunde liegenden Systemen „gehören“, in denen diese Daten erfasst wurden.

Der CIR würde keine SIS-Daten enthalten. Die komplexe technische Architektur des SIS mit nationalen Kopien, nationalen Teilkopien und etwaigen nationalen Systemen für den Abgleich biometrischer Daten hätte eine so hohe Komplexität des CIR zur Folge, dass dieser in technischer und finanzieller Hinsicht möglicherweise nicht mehr zu realisieren wäre.

Der CIR soll vor allem die biografische Identifizierung von Drittstaatsangehörigen erleichtern. Er würde eine höhere Betriebsgeschwindigkeit, mehr Effizienz und Größenvorteile bewirken. Die Einführung des CIR ist notwendig, um eine wirksame Identitätsprüfung von Drittstaatsangehörigen, auch im Hoheitsgebiet eines Mitgliedstaats, zu ermöglichen. Durch Ergänzung des CIR durch eine „Trefferkennzeichnungsfunktion“ könnte zudem aufgrund einer einfachen Mitteilung „Treffer/ kein Treffer“ in Erfahrung gebracht werden, ob Daten in einem der vom CIR erfassten Systeme vorhanden sind (oder nicht). Auf diese Weise würde der CIR auch dazu beitragen, den Zugang der Strafverfolgungsbehörden zu Informationssystemen anderer Behörden einheitlich zu regeln und gleichzeitig ein hohes Datenschutzniveau zu wahren (siehe den Abschnitt über

[23] Diese biometrischen Suchmaschinen werden fachsprachlich als automatisiertes Fingerabdruck-Identifizierungssystem (AFIS) oder automatisiertes biometrisches Identifizierungssystem (ABIS) bezeichnet.

[24] Zu den in Reisedokumenten erfassten biografischen Daten gehören Nachname, Vorname, Geschlecht, Geburtsdatum, Nummer des Reisedokuments. Nicht dazu gehören Adressen, frühere Namen, biometrische Daten usw.

das zweistufige Datenabfrageverfahren für den Datenzugriff der Strafverfolgungsbehörden).

Drei der fünf vom CIR zu erfassenden Systeme, nämlich das künftige EES, das vorgeschlagene ETIAS und das vorgeschlagene System ECRIS-TCN, sind neue Systeme, die noch entwickelt werden müssen. Das derzeitige System Eurodac enthält keine biografischen Daten; die Entwicklungsarbeiten zur Ausweitung des Systems sollen erfolgen, sobald die neue Rechtsgrundlage für Eurodac angenommen worden ist. Das gegenwärtige VIS enthält biografische Daten, die notwendigen Interaktionen zwischen dem VIS und dem künftigen EES setzen allerdings voraus, dass das bestehende VIS modernisiert wird. Die Einführung des CIR käme daher zum richtigen Zeitpunkt und hätte in keinem Fall eine Duplizierung vorhandener Daten zur Folge. In technischer Hinsicht würde der CIR auf der Grundlage der EES/ETIAS-Plattform entwickelt.

4) Mit dem **Detektor für Mehrfachidentitäten (MID)** würde geprüft, ob die abgefragten Identitätsdaten in mehr als einem der mit dem Detektor verbundenen Systeme vorhanden sind. Der MID erstreckt sich auf die Systeme, mit denen Identitätsdaten im CIR gespeichert werden (Eurodac, VIS, künftiges EES, vorgeschlagenes ETIAS und vorgeschlagenes System ECRIS-TCN) sowie auf das SIS. Um sowohl eine korrekte Identifizierung von Bona-fide-Reisenden sicherzustellen als auch Identitätsbetrug zu bekämpfen, könnten mithilfe des MID Mehrfachidentitäten aufgedeckt werden, die mit ein und demselben Satz biometrischer Daten verknüpft sind.

Dank des MID könnte in Erfahrung gebracht werden, ob verschiedene Namen derselben Identität zuzuordnen sind. Dieser innovativen Komponente bedarf es, um wirksam gegen die betrügerische Verwendung von Identitäten, bei der es sich um eine schwerwiegende Verletzung der Sicherheit handelt, vorgehen zu können. Der MID würde nur solche biografischen Identitätsdatensätze anzeigen, die in verschiedenen Zentralsystemen miteinander verknüpft sind. Solche Verknüpfungen würden mithilfe des gemeinsamen Dienstes für den Abgleich biometrischer Daten auf der Grundlage biometrischer Daten ermittelt und müssten von der Behörde, die die Daten in dem Informationssystem erfasst hat, das zur Erstellung der Verknüpfung geführt hat, bestätigt oder zurückgewiesen werden. Zur Unterstützung der ermächtigten MID-Nutzer bei dieser Aufgabe müssten die ermittelten Verknüpfungen durch das System vier Kategorien zugeordnet werden:

- Gelbe Verknüpfung – möglicherweise unterschiedliche biografische Identitäten derselben Person
- Weiße Verknüpfung – Bestätigung, dass die verschiedenen biografischen Identitäten demselben Bona-fide-Reisenden zuzuordnen sind
- Grüne Verknüpfung – Bestätigung, dass verschiedene Bona-fide-Reisende zufällig dieselbe biografische Identität haben
- Rote Verknüpfung – Verdacht, dass sich dieselbe Person unrechtmäßig unterschiedlicher biografischer Identitäten bedient

In diesem Vorschlag werden die Verfahren beschrieben, die für den Umgang mit diesen verschiedenen Kategorien eingeführt würden. Damit unnötige Unannehmlichkeiten vermieden werden, sollte die Identität der betroffenen Bona-fide-Reisenden so rasch wie möglich geklärt und eine gelbe Verknüpfung in eine bestätigte grüne oder weiße Verknüpfung umgewandelt werden. Ergibt die Prüfung hingegen, dass eine rote

Verknüpfung bestätigt wird oder eine gelbe Verknüpfung in eine rote umzuwandeln ist, müssten geeignete Maßnahmen ergriffen werden.

- **Zweistufiges Datenabfrageverfahren für den über den CIR erfolgenden Datenzugriff der Strafverfolgungsbehörden**

Die Strafverfolgung wurde als sekundäres bzw. untergeordnetes Ziel von Eurodac, des VIS, des künftigen EES und des vorgeschlagenen ETIAS festgelegt. Folglich ist es nur in eingeschränktem Maße möglich, zu Strafverfolgungszwecken auf die in diesen Systemen gespeicherten Daten zuzugreifen. Die Strafverfolgungsbehörden können diese nicht vorrangig zu Strafverfolgungszwecken vorgesehenen Informationssysteme zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung terroristischer und sonstiger schwerer Straftaten nur direkt abfragen. Darüber hinaus gelten für die einzelnen Systeme unterschiedliche Zugangsbedingungen und Garantien, und einige dieser gegenwärtigen Vorschriften könnten die rechtmäßige Nutzung der Systeme durch diese Behörden verlangsamen. Generell werden die mitgliedstaatlichen Behörden durch die Vorgabe, dass grundsätzlich vorab eine Suchabfrage vorzunehmen ist, in ihren Möglichkeiten beschnitten, die betreffenden Systeme zu berechtigten Strafverfolgungszwecken zu Rate zu ziehen, was im Hinblick auf die Aufdeckung notwendiger Informationen zu verpassten Gelegenheiten führen kann.

In ihrer Mitteilung vom April 2016 stellte die Kommission fest, dass die bestehenden Instrumente unter Einhaltung der Datenschutzvorschriften für Strafverfolgungszwecke optimiert werden müssen. Dies wurde von den Mitgliedstaaten und den zuständigen Agenturen im Rahmen der hochrangigen Expertengruppe bestätigt und bekräftigt.

Durch Einrichtung des CIR mit einer „Trefferkennzeichnungsfunktion“ wird daher mit diesem Vorschlag die Möglichkeit eines Zugangs zum EES, zum VIS, zum ETIAS und zu Eurodac im Wege eines **zweistufigen Datenabfrageverfahrens** eingeführt. Dieses zweistufige Verfahren würde nichts daran ändern, dass die Strafverfolgung ein strikt untergeordnetes Ziel dieser Systeme ist und daher strengen Zugangsregeln unterliegen muss.

In einem ersten Schritt würde ein Strafverfolgungsbeamter eine Abfrage zu einer bestimmten Person anhand der Identitätsdaten, des Reisedokuments oder der biometrischen Daten des Betreffenden durchführen, um zu überprüfen, ob im CIR Angaben zu der gesuchten Person gespeichert sind. Liegen solche Daten vor, erhält der Beamte **eine Antwort, aus der hervorgeht, welches EU-Informationssystem bzw. welche EU-Informationssysteme Daten** zu dieser Person (**Trefferkennzeichnung**) **enthält bzw. enthalten**. Der Beamte hätte jedoch keinen Zugriff auf in den zugrunde liegenden Systemen erfasste Daten.

In einem zweiten Schritt kann der Beamte einen Einzelantrag auf Zugang zu jedem System stellen, das den Angaben zufolge relevante Daten enthält, um **im Einklang mit den für jedes dieser Systeme geltenden Vorschriften und Verfahren** die vollständige Datei über die betreffende Person zu erhalten. Dieser in dem zweiten Schritt beantragte Zugang müsste von einer benannten Behörde genehmigt werden und würde auch künftig eine bestimmte Nutzerkennung und Protokollierung erfordern.

Dieses neue Verfahren würde aufgrund des **Vorhandenseins etwaiger Verknüpfungen** im MID ebenfalls einen Mehrwert für die Strafverfolgungsbehörden bewirken. Der MID würde den CIR bei der Ermittlung bestehender Verknüpfungen unterstützen, wodurch noch präzisere

Abfragen möglich wären. Der MID könnte angeben, ob die Person in verschiedenen Informationssystemen **unter unterschiedlichen Identitäten** erfasst ist.

Das zweistufige Datenabfrageverfahren ist vor allem in Fällen sinnvoll, in denen der Verdächtige, der Täter oder das mutmaßliche Opfer einer terroristischen oder sonstigen schweren Straftat **unbekannt ist**. In derartigen Fällen würde der CIR mittels eines einzigen Suchvorgangs ermöglichen, das Informationssystem zu ermitteln, in dem die betreffende Person erfasst ist. Insofern würden sich die bestehenden Bedingungen für die vorherige Abfrage nationaler Datenbanken und die vorherige Abfrage des automatisierten Fingerabdruck-Identifizierungssystems anderer Mitgliedstaaten gemäß dem Beschluss 2008/615/JI (Überprüfung nach den Prüm-Kriterien) erübrigen.

Das neue zweistufige Abfrageverfahren würde **erst in Kraft treten, wenn** die für die Interoperabilität erforderlichen **Komponenten voll funktionsfähig sind**.

- **Weitere in diesem Vorschlag vorgesehene Elemente zur Unterstützung der Interoperabilitätskomponenten**

1) Neben den oben genannten Komponenten sieht dieser Verordnungsentwurf auch die Einrichtung eines **zentralen Speichers für Berichte und Statistiken (central repository for reporting and statistics – CRRS)** vor. Dieser Speicher ist notwendig, damit Berichte mit (anonymen) statistischen Daten zu politischen und operativen Zwecken sowie für die Zwecke der Datenqualität erstellt und ausgetauscht werden können. Die derzeitige Praxis, statistische Daten nur zu den einzelnen Informationssystemen zu erheben, wirkt sich nachteilig auf die Datensicherheit und die Leistung aus und ermöglicht keine systemübergreifende Korrelation von Daten.

   Der CRRS wäre ein spezieller, separater Speicher für anonyme Statistiken, die aus dem SIS, dem VIS, Eurodac, dem künftigen EES, dem vorgeschlagenen ETIAS, dem vorgeschlagenen System ECRIS-TCN, dem gemeinsamen Speicher für Identitätsdaten, dem Detektor für Mehrfachidentitäten und dem gemeinsamen Dienst für den Abgleich biometrischer Daten extrahiert würden. Der Speicher würde den Mitgliedstaaten, der Kommission (einschließlich Eurostat) und den EU-Agenturen den sicheren Austausch von Berichten (nach Maßgabe der jeweiligen Rechtsinstrumente) ermöglichen.

   Im Hinblick auf die Einrichtung, den Betrieb und die Wartung wäre es kostengünstiger und weniger aufwendig, einen einzigen zentralen Speicher anstatt separate Speicher für die einzelnen Systeme zu entwickeln. Außerdem würde die Datensicherheit erhöht, da die Datenspeicherung und die Verwaltung der Zugangskontrolle in einem einzigen Speicher erfolgen würden.

2) In diesem Verordnungsentwurf wird außerdem vorgeschlagen, das **universelle Nachrichtenformat (Universal Message Format – UMF)** auf EU-Ebene als Standard festzulegen, um Interaktionen zwischen mehreren Systemen, einschließlich der von eu-LISA entwickelten und verwalteten Systeme, auf interoperable Weise zu ermöglichen. Europol und Interpol würden ebenfalls ermutigt, diesen Standard zu verwenden.

   Mit dem UMF-Standard wird eine gemeinsame, einheitliche Fachsprache zur Beschreibung und Verknüpfung von Datenelementen, insbesondere der Elemente in Bezug auf Personen und (Reise-)Dokumente, eingeführt. Die Verwendung des UMF bei

der Entwicklung neuer Informationssysteme gewährleistet eine einfachere Integration und Interoperabilität mit anderen Systemen, vor allem für die Mitgliedstaaten, die Schnittstellen für die Kommunikation mit diesen neuen Systemen einrichten müssen. Daher ist die obligatorische Verwendung des UMF bei der Entwicklung neuer Systeme als notwendige Voraussetzung für die Einführung der in dieser Verordnung vorgeschlagenen Interoperabilitätskomponenten zu erachten.

Um die vollständige EU-weite Einführung des UMF-Standards zu gewährleisten, wird eine angemessene Regelungsstruktur vorgeschlagen. Die Kommission wäre im Rahmen eines Prüfverfahrens mit den Mitgliedstaaten für die Festlegung und Entwicklung des UMF-Standards verantwortlich. Die assoziierten Schengen-Länder sowie die an den UMF-Projekten beteiligten EU-Agenturen und internationalen Einrichtungen (darunter eu-LISA, Europol und Interpol) werden ebenfalls einbezogen. Die vorgeschlagene Regelungsstruktur ist für das UMF von entscheidender Bedeutung, um den Standard zu erweitern und zugleich eine größtmögliche Einsatzbarkeit und Anwendbarkeit zu gewährleisten.

3) Darüber hinaus werden mit diesem Verordnungsentwurf **Mechanismen für die automatische Datenqualitätskontrolle** und gemeinsame Qualitätsindikatoren eingeführt. Zudem sieht die vorgeschlagene Verordnung vor, dass die Mitgliedstaaten bei der Speisung und Nutzung der Systeme eine möglichst hohe Datenqualität gewährleisten müssen. Wenn die Daten nicht von höchster Qualität sind, können möglicherweise nicht nur gesuchte Personen nicht identifiziert, sondern auch die Grundrechte Unschuldiger beeinträchtigt werden. Probleme, die auf die Eingabe von Daten durch Menschen zurückzuführen sind, lassen sich durch automatische Validierungsregeln vermeiden, die das Bedienpersonal daran hindern, Fehler zu begehen. Anzustreben wäre die automatische Ermittlung anscheinend falscher oder unstimmiger Dateneinträge, damit der Mitgliedstaat, der die Daten eingegeben hat, die betreffenden Daten überprüfen und etwaige erforderliche Abhilfemaßnahmen ergreifen kann. Ergänzend dazu würde eu-LISA regelmäßig Datenqualitätsberichte erstellen.

- **Folgen für andere Rechtsinstrumente**

Zusammen mit dem Parallelvorschlag werden mit dieser vorgeschlagenen Verordnung Innovationen eingeführt, die Änderungen anderer Rechtsinstrumente erfordern:

- Verordnung (EU) 2016/399 (Schengener Grenzkodex)
- Verordnung (EU) 2017/2226 (EES-Verordnung)
- Verordnung (EG) Nr. 767/2008 (VIS-Verordnung)
- Entscheidung 2004/512/EG des Rates (VIS-Entscheidung)
- Beschluss 2008/633/JI des Rates (Beschluss VIS/Zugang der Strafverfolgungsbehörden)
- [ETIAS-Verordnung]
- [Eurodac-Verordnung]
- [SIS-Verordnungen]
- [ECRIS-TCN-Verordnung, einschließlich der entsprechenden Bestimmungen der Verordnung (EU) 2016/1624 (Verordnung über die Europäische Grenz- und Küstenwache)]

- [eu-LISA-Verordnung]

Der vorliegende Vorschlag und der Parallelvorschlag enthalten eingehende Bestimmungen für die notwendigen Änderungen an den Rechtsinstrumenten, die in der von den beiden gesetzgebenden Organen angenommenen Fassung als stabile Texte vorliegen: Schengener Grenzkodex, EES-Verordnung, VIS-Verordnung, Beschluss 2008/633/JI des Rates und Entscheidung 2004/512/EG des Rates.

Über die anderen aufgeführten Instrumente (Verordnungen über ETIAS, Eurodac, SIS, ECRIS-TCN, eu-LISA) wird derzeit im Europäischen Parlament und im Rat verhandelt. Für diese Instrumente können daher die erforderlichen Änderungen zum gegenwärtigen Zeitpunkt nicht angegeben werden. Die Kommission wird die entsprechenden Änderungen für jedes dieser Instrumente innerhalb von zwei Wochen nach Erzielung einer politischen Einigung über die jeweiligen Verordnungsentwürfe vorlegen.

- **Kohärenz mit den bestehenden Vorschriften in diesem Bereich**

Dieser Vorschlag erfolgt im Rahmen des umfassenderen Prozesses, der durch die Mitteilung *Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit* vom April 2016 sowie die anschließenden Arbeiten der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität eingeleitet wurde. Damit sollen drei Ziele verfolgt werden:

a) Erhöhung und Maximierung des Nutzens der **bestehenden Informationssysteme**,

b) Schließung von Informationslücken durch Einführung neuer Informationssysteme,

c) Verbesserung der Interoperabilität zwischen diesen Systemen.

Im Hinblick auf das erste Ziel nahm die Kommission im Dezember 2016 Vorschläge zur weiteren Stärkung des bestehenden Schengener Informationssystems (SIS)[25] an. In Bezug auf Eurodac wurden nach der Vorlage des Kommissionsvorschlags vom Mai 2016[26] die Verhandlungen über die überarbeitete Rechtsgrundlage beschleunigt. Ein Vorschlag für eine neue Rechtsgrundlage für das Visa-Informationssystem (VIS) wird ebenfalls ausgearbeitet und soll im zweiten Quartal 2018 vorgelegt werden.

Was das zweite Ziel anbelangt, so wurden die Verhandlungen über den Kommissionsvorschlag vom April 2016 über ein Einreise-/Ausreisesystem (EES)[27] bereits im Juli 2017 abgeschlossen, als die beiden gesetzgebenden Organe eine politische Einigung erzielten, die im Oktober 2017 vom Europäischen Parlament bestätigt und im November 2017 vom Rat förmlich angenommen wurde. Die Rechtsgrundlage wird im Dezember 2017 in Kraft treten. Die Verhandlungen über den im November 2016 unterbreiteten Vorschlag über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS)[28] haben begonnen und werden voraussichtlich in den kommenden Monaten abgeschlossen. Im Juni 2017 schlug die Kommission eine Rechtsgrundlage vor, um eine weitere Informationslücke zu schließen. Gegenstand des Vorschlags ist das Europäische Strafregisterinformationssystem für

[25] COM(2016) 883 final.
[26] COM(2016) 272 final.
[27] COM(2016) 194 final.
[28] COM(2016) 731 final.

Drittstaatsangehörige (System ECRIS-TCN)[29]. Auch hier streben die beiden gesetzgebenden Organe laut eigenen Angaben eine baldige Annahme der Rechtsgrundlage an.

Mit dem vorliegenden Vorschlag wird das in der Mitteilung vom April 2016 genannte dritte Ziel angegangen.

- **Kohärenz mit der Politik der Union im Bereich Justiz und Inneres**

Dieser Vorschlag dient – zusammen mit dem Parallelvorschlag – der Umsetzung der Europäischen Migrationsagenda und der nachfolgenden Mitteilungen, unter anderem der Mitteilung „Schengen bewahren und stärken"[30], der Europäischen Sicherheitsagenda[31] sowie der Arbeiten und Fortschrittsberichte der Kommission im Hinblick auf eine wirksame und echte Sicherheitsunion[32] und steht damit in Einklang. Er ist auch mit der Politik der Union in anderen Bereichen vereinbar, insbesondere in folgenden Bereichen:

- Innere Sicherheit: Wie in der Europäischen Sicherheitsagenda festgestellt wird, sind einheitliche hohe Standards beim Grenzmanagement für die Verhütung von grenzüberschreitender Kriminalität und Terrorismus unverzichtbar. Der Vorschlag trägt außerdem zu einem hohen Maß an innerer Sicherheit bei, indem er vorsieht, den Behörden einen raschen, unterbrechungsfreien, systematischen und kontrollierten Zugang zu den von ihnen benötigten Informationen zu ermöglichen.
- Asyl: Der Vorschlag sieht vor, dass Eurodac als eines der zentralen EU-Systeme in die Interoperabilität einbezogen wird.
- Außengrenzenmanagement und Sicherheit: Der Vorschlag dient der Stärkung der Systeme SIS und VIS, die zur wirksamen Kontrolle der Außengrenzen der Union beitragen, sowie der Stärkung des künftigen EES und der vorgeschlagenen Systeme ETIAS und ECRIS-TCN.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄSSIGKEIT

- **Rechtsgrundlage**

Die Hauptrechtsgrundlage werden folgende Artikel des Vertrags über die Arbeitsweise der Europäischen Union bilden: Artikel 16 Absatz 2, Artikel 74, Artikel 78 Absatz 2 Buchstabe e, Artikel 79 Absatz 2 Buchstabe c, Artikel 82 Absatz 1 Buchstabe d, Artikel 85 Absatz 1, Artikel 87 Absatz 2 Buchstabe a und Artikel 88 Absatz 2,

Nach Artikel 16 Absatz 2 kann die Union Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr erlassen. Nach Artikel 74 kann der Rat Maßnahmen erlassen, um die Verwaltungszusammenarbeit zwischen den zuständigen Dienststellen der Mitgliedstaaten im Raum der Freiheit, der Sicherheit und des Rechts zu gewährleisten. Nach Artikel 78 kann die Union Maßnahmen in Bezug auf ein gemeinsames europäisches Asylsystem erlassen. Nach

[29] COM(2017) 344 final.
[30] COM(2017) 570 final.
[31] COM(2015) 185 final.
[32] COM(2016) 230 final.

Artikel 79 Absatz 2 Buchstabe c kann die Union Maßnahmen im Bereich der illegalen Einwanderung und des illegalen Aufenthalts erlassen. Nach Artikel 82 Absatz 1 Buchstabe d und Artikel 87 Absatz 2 Buchstabe a kann die Union Maßnahmen zur Verstärkung der polizeilichen und justiziellen Zusammenarbeit in Bezug auf das Einholen, Speichern, Verarbeiten, Analysieren und Austauschen sachdienlicher Informationen erlassen. Nach Artikel 85 Absatz 1 und Artikel 88 Absatz 2 kann die Union die Aufgaben von Eurojust bzw. Europol festlegen.

- **Subsidiarität**

Die Freizügigkeit innerhalb der EU setzt ein wirksames Management der EU-Außengrenzen voraus, damit die Sicherheit gewährleistet ist. Daher haben sich die Mitgliedstaaten darauf verständigt, die diesbezüglichen Herausforderungen gemeinsam anzugehen, indem sie vor allem über zentrale EU-Systeme im Bereich Justiz und Inneres Informationen austauschen. Dies wird in verschiedenen Schlussfolgerungen bestätigt, die sowohl der Europäische Rat als auch der Rat insbesondere seit 2015 angenommen haben.

Die Kontrollfreiheit an den Binnengrenzen setzt ein solides Management der Schengen-Außengrenzen voraus, bei dem die einzelnen Mitgliedstaaten und assoziierten Schengen-Länder die Außengrenzen im Namen der anderen Schengen-Staaten kontrollieren müssen. Ein einzelner Mitgliedstaat ist also nicht in der Lage, die irreguläre Migration und die grenzüberschreitende Kriminalität allein zu bewältigen. Drittstaatsangehörige, die in den Raum ohne Binnengrenzkontrollen einreisen, können ungehindert in andere Länder dieses Raums reisen. In einem Raum ohne Binnengrenzen sollte gemeinsam gegen irreguläre Einwanderung, internationale Kriminalität und Terrorismus vorgegangen werden, unter anderem durch Maßnahmen zur Aufdeckung von Identitätsbetrug. Nur auf EU-Ebene lassen sich diese Probleme erfolgreich in den Griff bekommen.

Auf EU-Ebene sind zentrale gemeinsame Informationssysteme vorhanden oder werden derzeit eingerichtet. Zur Erhöhung der Interoperabilität zwischen diesen Informationssystemen bedarf es zwingend eines Tätigwerdens auf EU-Ebene. Im Wesentlichen zielt der Vorschlag auf eine bessere Effizienz und Nutzung der von eu-LISA verwalteten zentralen Systeme ab. Aufgrund des Umfangs, der Auswirkungen und der Folgen der geplanten Maßnahmen lassen sich die grundlegenden Ziele nur auf EU-Ebene effizient und systematisch verwirklichen.

- **Verhältnismäßigkeit**

Wie in der Folgenabschätzung zu der vorgeschlagenen Verordnung ausführlich erläutert, werden die im Rahmen dieses Vorschlags getroffenen politischen Entscheidungen als verhältnismäßig erachtet. Sie gehen nicht über das für die Erreichung der vereinbarten Ziele erforderliche Maß hinaus.

Das **Europäische Suchportal (ESP)** ist erforderlich, um eine verstärkte zulässige Nutzung der bestehenden und künftigen EU-Informationssysteme zu ermöglichen. Das ESP hat nur sehr begrenzte Auswirkungen auf die Datenverarbeitung. Es wird keine Daten speichern – ausgenommen Informationen über die verschiedenen ESP-Nutzerprofile sowie die Daten und Informationssysteme, zu denen die Nutzer Zugang haben, und die Erfassung der Systemnutzung durch Protokolle. Das ESP als Schnittstelle, die einen effizienten Informationsaustausch ermöglicht und erleichtert, ist angemessen und notwendig; in Bezug auf Abfragen und Zugangsrechte nach Maßgabe der Rechtsgrundlagen für

Informationssysteme und die vorgeschlagene Verordnung über die Interoperabilität sind Einschränkungen vorgesehen.

Der **gemeinsame Dienst für den Abgleich biometrischer Daten (gemeinsamer BMS)** ist notwendig für das Funktionieren des ESP, des gemeinsamen Speichers für Identitätsdaten und des Detektors für Mehrfachidentitäten und erleichtert die Nutzung und Wartung der bestehenden und künftigen einschlägigen EU-Informationssysteme. Seine Funktionen ermöglichen die effiziente, unterbrechungsfreie und systematische Abfrage biometrischer Daten aus verschiedenen Quellen. Die biometrischen Daten werden ausschließlich von den zugrunde liegenden Systemen gespeichert. Der gemeinsame BMS generiert Templates, ohne jedoch die eigentlichen Bilder zu erfassen. Die Daten werden somit nur einmal an einem einzigen Ort gespeichert.

Der **gemeinsame Speicher für Identitätsdaten (CIR)** ist notwendig, um die bezweckte korrekte Identifizierung von Drittstaatsangehörigen, zum Beispiel bei einer Identitätsprüfung im Schengen-Raum, zu ermöglichen. Der CIR unterstützt außerdem das Funktionieren des Detektors für Mehrfachidentitäten und ist daher sowohl erforderlich, um die Identitätsprüfung von Bona-fide-Reisenden zu vereinfachen als auch um Identitätsbetrug zu bekämpfen. Der zu diesem Zweck erfolgende Zugang zum CIR wird auf diejenigen Nutzer beschränkt, die die entsprechenden Informationen zur Erfüllung ihrer Aufgaben benötigen (was voraussetzt, dass die betreffenden Prüfungen einem neuen sekundären Zweck von Eurodac, des VIS, des künftigen EES, des vorgeschlagenen ETIAS und des vorgeschlagenen Systems ECRIS-TCN dienen). Die Datenverarbeitung ist strikt auf das zur Erreichung dieses Ziels erforderliche Maß beschränkt, und es werden angemessene Garantien festgelegt, damit sichergestellt ist, dass die Zugangsrechte eingehalten und nur die unbedingt notwendigen Daten im CIR gespeichert werden. Um Datenminimierung zu gewährleisten und eine ungerechtfertigte Duplizierung von Daten zu vermeiden, enthält der CIR die benötigten biografischen Daten der einzelnen zugrunde liegenden Systeme, die im Einklang mit deren jeweiliger Rechtsgrundlage gespeichert, ergänzt, geändert und gelöscht, jedoch nicht kopiert werden. Die Bedingungen für die Dauer der Datenspeicherung entsprechen vollständig den Datenspeicherungsbestimmungen der zugrunde liegenden Informationssysteme, die die Identitätsdaten liefern.

Der **Detektor für Mehrfachidentitäten (MID)** ist erforderlich, damit Mehrfachidentitäten aufgedeckt werden können, um zugleich die Identitätsprüfung von Bona-fide-Reisenden zu vereinfachen und Identitätsbetrug zu bekämpfen. Der MID wird Verknüpfungen zwischen Personen enthalten, die in mehr als einem zentralen Informationssystem erfasst sind, wobei der diesbezügliche Datenzugriff strikt auf die Daten begrenzt wird, die erforderlich sind, um zu verifizieren, ob eine Person korrekt erfasst oder illegal mit mehreren biografischen Identitäten in unterschiedlichen Systemen erfasst ist, oder aber um zu überprüfen, ob es sich bei zwei Personen mit ähnlichen biografischen Daten um ein und dieselbe Person handelt. Die durch den MID und den gemeinsamen BMS erfolgende Datenverarbeitung im Hinblick auf die systemübergreifende Verknüpfung individueller Dateien wird auf das unbedingt erforderliche Mindestmaß beschränkt. Der MID wird Absicherungen gegen eine mögliche Diskriminierung von Personen mit legalen Mehrfachidentitäten oder gegen derartige Personen beschwerende Entscheidungen einschließen.

- **Wahl des Instruments**

Es wird eine Verordnung des Europäischen Parlaments und des Rates vorgeschlagen. Die vorgeschlagenen Rechtsvorschriften betreffen unmittelbar den Betrieb der zentralen EU-Informationssysteme in den Bereichen Grenzmanagement und Sicherheit, die alle auf der

Grundlage von Verordnungen eingerichtet wurden oder werden sollen. Auch die Agentur eu-LISA, die für die Konzipierung und Entwicklung sowie zu gegebener Zeit für die technische Verwaltung der Komponenten verantwortlich sein wird, wird auf einer Verordnung basieren. Eine Verordnung ist daher das geeignete Rechtsinstrument.

3. ERGEBNISSE DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

• Öffentliche Konsultation

In Vorbereitung dieses Vorschlags leitete die Kommission im Juli 2017 eine öffentliche Konsultation ein, um die Ansichten der Interessenträger zur Thematik der Interoperabilität einzuholen. Im Zuge der Konsultation gingen 18 Antworten verschiedener Interessenträger ein, darunter Regierungen der Mitgliedstaaten, privatwirtschaftliche Organisationen, sonstige Organisationen wie NRO und Denkfabriken sowie Privatpersonen.[33] Insgesamt wurden die grundlegenden Prinzipien dieses Interoperabilitätsvorschlags weitgehend befürwortet. Die überwiegende Mehrheit der Befragten stimmte darin überein, dass die Probleme im Zuge der Konsultation richtig erkannt wurden und dass mit dem Interoperabilitätspaket die richtigen Ziele angestrebt werden. Die Befragten waren insbesondere der Ansicht, dass die im Konsultationspapier dargelegten Optionen

- den Bediensteten vor Ort den Zugang zu den von ihnen benötigten Informationen erleichtern würden,
- dazu beitragen würden, die Duplizierung von Daten zu vermeiden, Überschneidungen zu reduzieren und Abweichungen zwischen Daten aufzuzeigen,
- eine zuverlässigere Identifizierung von Personen – auch von solchen mit mehreren Identitäten – ermöglichen und zur Bekämpfung von Identitätsbetrug beitragen würden.

Eine klare Mehrheit der Befragten sprach sich für die vorgeschlagenen Optionen aus und hält sie für erforderlich, um die Ziele dieser Initiative zu erreichen, wobei in den Antworten betont wurde, dass es strenger und klarer Datenschutzmaßnahmen bedarf – insbesondere in Bezug auf den Zugang zu den in den Systemen erfassten Informationen und die Dauer der Datenspeicherung – und dass die Systeme aktuelle, hochwertige Daten enthalten müssen und dies durch entsprechende Maßnahmen gewährleistet werden muss.

Alle angesprochenen Aspekte wurden bei der Ausarbeitung des vorliegenden Vorschlags berücksichtigt.

• Eurobarometer-Umfrage

Eine im Juni 2017 durchgeführte Eurobarometer-Sonderumfrage[34] hat ergeben, dass die EU-Strategie des Austauschs von Informationen auf EU-Ebene zur Bekämpfung von Kriminalität und Terrorismus die breite Unterstützung der Öffentlichkeit findet: Nahezu alle Befragten

[33] Weitere Einzelheiten sind dem der Folgenabschätzung beigefügten zusammenfassenden Bericht zu entnehmen.

[34] Im *Report on Europeans' attitudes towards security* (Bericht über die Einstellung der Europäer/-innen in Sachen Sicherheit) werden die Ergebnisse der Eurobarometer-Sonderumfrage (464b) zu dem Sicherheitsbewusstsein der Bürger/-innen, ihren Erfahrungen in Sachen Sicherheit und ihrem Sicherheitsempfinden analysiert. Diese Umfrage wurde vom TNS Political & Social network zwischen dem 13. und 26. Juni 2017 in den 28 Mitgliedstaaten durchgeführt. Befragt wurden 28 093 EU-Bürger/-innen aus verschiedenen sozialen und demografischen Bevölkerungsgruppen.

(92 %) sind der Meinung, dass die nationalen Behörden Informationen mit den Behörden anderer Mitgliedstaaten austauschen sollten, um Kriminalität und Terrorismus besser bekämpfen zu können.

Eine klare Mehrheit (69 %) der Befragten vertrat die Auffassung, dass die Polizei und andere nationale Strafverfolgungsbehörden systematisch Informationen mit anderen EU-Ländern austauschen sollten. In allen Mitgliedstaaten sind die meisten Befragten der Ansicht, dass in jedem Fall ein Informationsaustausch stattfinden sollte.

- **Hochrangige Expertengruppe für Informationssysteme und Interoperabilität**

Wie einleitend bereits erwähnt wurde, stützt sich der vorliegende Vorschlag auf die Empfehlungen der **hochrangigen Expertengruppe für Informationssysteme und Interoperabilität**[35]. Diese Gruppe wurde im Juni 2016 eingesetzt und sollte sich mit den rechtlichen, technischen und operativen Herausforderungen im Zusammenhang mit den verfügbaren Optionen zur Herstellung der Interoperabilität zwischen den zentralen EU-Informationssystemen in den Bereichen Grenzmanagement und Sicherheit auseinandersetzen. Die Gruppe befasste sich umfassend mit vielen unterschiedlichen Aspekten der Datenverwaltungsarchitektur für das Grenzmanagement und die Strafverfolgung und berücksichtigte dabei auch die entsprechenden Aufgaben, Zuständigkeiten und Systeme der Zollbehörden.

Der Gruppe gehörten Sachverständige aus den Mitgliedstaaten und den assoziierten Schengen-Ländern an sowie aus den EU-Agenturen eu-LISA, Europol, Europäisches Unterstützungsbüro für Asylfragen, Europäische Agentur für die Grenz- und Küstenwache und Agentur der EU für Grundrechte. Der EU-Koordinator für die Terrorismusbekämpfung und der Europäische Datenschutzbeauftragte beteiligten sich ebenfalls als Vollmitglieder an den Arbeiten der Expertengruppe. Des Weiteren nahmen Vertreter des Sekretariats des Ausschusses des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres sowie des Generalsekretariats des Rates als Beobachter teil.

Der **Abschlussbericht der hochrangigen Expertengruppe** wurde im Mai 2017 veröffentlicht.[36] Wie in dem Bericht herausgestellt wurde, besteht Handlungsbedarf, um die in der Mitteilung vom April 2016 aufgezeigten strukturellen Mängel zu beheben. Der Bericht enthält eine Reihe von Empfehlungen zur Stärkung und Weiterentwicklung der EU-Informationssysteme und ihrer Interoperabilität. Die Expertengruppe kam zu dem Schluss, dass es **notwendig und technisch möglich ist, auf ein Europäisches Suchportal, einen gemeinsamen Dienst für den Abgleich biometrischer Daten und einen gemeinsamen Speicher für Identitätsdaten als Lösungen für die Interoperabilität hinzuarbeiten**, und dass diese Lösungen grundsätzlich sowohl operative Verbesserungen bewirken als auch im Einklang mit den Datenschutzvorschriften umgesetzt werden können. Die Gruppe empfahl zudem, die zusätzliche Option eines zweistufigen Verfahrens für den Datenzugriff der Strafverfolgungsbehörden auf der Grundlage einer Trefferkennzeichnungsfunktion zu erwägen.

Dieser Verordnungsentwurf trägt auch den Empfehlungen der hochrangigen Expertengruppe zur Datenqualität, zum universellen Nachrichtenformat (UMF) und zur Schaffung eines „Data Warehouse“ (hier der zentrale Speicher für Berichte und Statistiken (CRRS)) Rechnung.

---

[35] Beschluss der Kommission vom 17. Juni 2016 zur Einsetzung der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität (2016/C 257/03).

[36] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1

Die in diesem Verordnungsentwurf vorgeschlagene vierte Interoperabilitätskomponente (der Detektor für Mehrfachidentitäten) wurde zwar von der hochrangigen Expertengruppe nicht genannt, seine Notwendigkeit ergab sich aber im Zuge der zusätzlichen technischen Analyse und der Verhältnismäßigkeitsbewertung, die die Kommission durchführte.

- **Technische Studien**

Zur Unterstützung der Ausarbeitung des Vorschlags wurden drei Studien vergeben. Im Auftrag der Kommission erstellte Unisys einen Bericht über eine Durchführbarkeitsstudie für das Europäische Suchportal. eu-LISA gab bei Gartner (mit Unisys) einen technischen Bericht zur Unterstützung der Entwicklung des gemeinsamen Dienstes für den Abgleich biometrischer Daten in Auftrag. PWC erstellte für die Kommission einen technischen Bericht über einen gemeinsamen Speicher für Identitätsdaten.

- **Folgenabschätzung**

Dieser Vorschlag wird von einer Folgenabschätzung gestützt (siehe beigefügte Arbeitsunterlage der Kommissionsdienststellen SWD(2017) XXX).

Der Ausschuss für Regulierungskontrolle prüfte den Entwurf der Folgenabschätzung in seiner Sitzung vom 6. Dezember 2017 und gab am 8. Dezember 2017 eine befürwortende Stellungnahme mit Vorbehalten ab, in der er sich dahin gehend äußerte, dass die Folgenabschätzung angepasst werden sollte, um den Empfehlungen des Ausschusses zu bestimmten Aspekten Rechnung zu tragen. Diese betrafen erstens zusätzliche Maßnahmen im Rahmen der bevorzugten Option, um die Datenzugriffsrechte der Endnutzer für die EU-Informationssysteme einheitlich zu regeln und die damit verbundenen Datenschutz- und Grundrechtsgarantien aufzuzeigen. Zweitens sollte vor allem geklärt werden, wie das Schengener Informationssystem im Rahmen von Option 2 integriert werden soll und wie es um die Wirksamkeit und die Kosten von Option 2 bestellt ist, damit diese leichter mit der bevorzugten Option 3 verglichen werden kann. Die Kommission aktualisierte ihre Folgenabschätzung, um diesen wichtigen Erwägungen Rechnung zu tragen und eine Reihe weiterer Anmerkungen des Ausschusses zu berücksichtigen.

In der Folgenabschätzung wurde bewertet, ob und wie jedes der festgelegten Ziele erreicht werden könnte, indem eine oder mehrere der von der hochrangigen Expertengruppe und durch eine anschließende Analyse bestimmten technischen Komponenten verwendet wird bzw. werden. Unter Beachtung des Datenschutzrahmens wurden bei Bedarf auch die für die Verwirklichung dieser Ziele erforderlichen Unteroptionen geprüft. Die Folgenabschätzung ergab Folgendes:

- Zur Verwirklichung des Ziels, ermächtigten Nutzern einen raschen, unterbrechungsfreien, systematischen und kontrollierten Zugang zu den entsprechenden Informationssystemen zu ermöglichen, sollte ein Europäisches Suchportal (ESP) geschaffen werden, das sich auf einen gemeinsamen Dienst für den Abgleich biometrischer Daten (gemeinsamer BMS) stützt, damit alle Datenbanken abgedeckt werden.
- Zur Verwirklichung des Ziels, die Identitätsprüfung von Drittstaatsangehörigen im Hoheitsgebiet eines Mitgliedstaats durch dazu ermächtigte Bedienstete zu erleichtern, sollte ein gemeinsamer Speicher für Identitätsdaten (CIR) geschaffen werden, der den Mindestsatz an Identifizierungsdaten enthält und sich auf denselben gemeinsamen BMS stützt.

- Zur Verwirklichung des Ziels, Mehrfachidentitäten aufzudecken, die mit ein und demselben Satz biometrischer Daten verknüpft sind, um zugleich die Identitätsprüfung von Bona-fide-Reisenden zu vereinfachen und Identitätsbetrug zu bekämpfen, bedarf es eines Detektors für Mehrfachidentitäten (MID), der systemübergreifend Verknüpfungen zwischen Mehrfachidentitäten enthält.
- Zur Verwirklichung des Ziels, den Zugang der Strafverfolgungsbehörden zu den Informationssystemen anderer Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung terroristischer und sonstiger schwerer Straftaten zu erleichtern und einheitlich zu regeln, sollte in den CIR eine Trefferkennzeichnungsfunktion integriert werden.

Da alle Ziele erreicht werden müssen, **ist die beste Lösung eine Kombination der allesamt auf den gemeinsamen BMS gestützten Komponenten ESP, CIR (mit Trefferkennzeichnung) und MID**.

Die wichtigsten positiven Auswirkungen dieser Lösung werden ein besseres Grenzmanagement und eine höhere innere Sicherheit in der Europäischen Union sein. Die neuen Komponenten werden einen einheitlich geregelten und rascheren Zugang der nationalen Behörden zu den erforderlichen Informationen sowie eine einfachere und schnellere Identifizierung von Drittstaatsangehörigen ermöglichen. Sie werden die Behörden in die Lage versetzen, bei Grenzübertrittskontrollen im Zusammenhang mit Visum- und Asylanträgen oder im Rahmen der Polizeiarbeit Querverbindungen zu bereits vorhandenen erforderlichen Informationen über bestimmte Personen herzustellen. Somit kann auf Informationen zugegriffen werden, die dazu beitragen können, dass sowohl bei Ermittlungen im Zusammenhang mit terroristischen oder sonstigen schweren Straftaten als auch im Migrations- und Asylbereich verlässliche Entscheidungen getroffen werden. Die vorgeschlagenen Maßnahmen betreffen die EU-Bürger zwar nicht direkt (sie zielen in erster Linie auf Drittstaatsangehörige ab, deren Daten in einem zentralen Informationssystem der EU erfasst sind), dürften aber das Vertrauen der Öffentlichkeit stärken, da sie gewährleisten, dass die Sicherheit der EU-Bürger aufgrund der Konzipierung und Nutzung der Systeme erhöht wird.

Die unmittelbaren finanziellen und wirtschaftlichen Auswirkungen des Vorschlags werden auf die Konzipierung, die Entwicklung und den Betrieb der neuen Komponenten beschränkt sein. Die Kosten gehen zulasten des EU-Haushalts und der Behörden der Mitgliedstaaten, die die Systeme betreiben. Auf den Tourismus werden sich die vorgeschlagenen Maßnahmen positiv auswirken, da sie nicht nur zu einer höheren Sicherheit in der Europäischen Union beitragen werden, sondern auch zügigere Grenzkontrollen ermöglichen dürften. Auch für Flughäfen, Seehäfen und Verkehrsunternehmen sind – insbesondere aufgrund der beschleunigten Grenzübertrittskontrollen – positive Auswirkungen zu erwarten.

- **Grundrechte**

In der Folgenabschätzung wurden insbesondere die Auswirkungen der vorgeschlagenen Maßnahmen auf die Grundrechte und vor allem auf das Recht auf Datenschutz untersucht.

Im Einklang mit der Charta der Grundrechte der Europäischen Union, an die die Organe, Einrichtungen und sonstigen Stellen der EU und die Mitgliedstaaten bei der Durchführung des EU-Rechts gebunden sind (Artikel 51 Absatz 1 der Charta), müssen die Möglichkeiten, die die Interoperabilität als Maßnahme zur Erhöhung der Sicherheit und zur Verbesserung des Schutzes an den Außengrenzen bietet, in einem ausgewogenen Verhältnis zu der

Verpflichtung stehen, der zufolge zu gewährleisten ist, dass Eingriffe in die Grundrechte, zu denen es aufgrund der neuen Interoperabilitätsumgebung kommen könnte, unter Wahrung des Grundsatzes der Verhältnismäßigkeit auf das beschränkt werden, was unbedingt notwendig ist, um den dem Gemeinwohl dienenden Zielsetzungen tatsächlich zu entsprechen (Artikel 52 Absatz 1 der Charta).

Die vorgeschlagenen Interoperabilitätslösungen ergänzen die bestehenden Systeme. Daher würde sich nichts an der Ausgewogenheit, die die einzelnen vorhandenen Zentralsysteme in Bezug auf ihre positiven Auswirkungen auf die Grundrechte gewährleisten, ändern.

Dennoch könnte die Interoperabilität zusätzliche indirekte Auswirkungen auf eine Reihe von Grundrechten haben. Die korrekte Identifizierung von Personen wirkt sich positiv auf das Recht auf Achtung des Privatlebens und insbesondere das Recht auf persönliche Identität (Artikel 7 der Charta) aus, da sie dazu beitragen kann, Identitätsverwechslungen zu vermeiden. Andererseits können Kontrollen auf der Grundlage biometrischer Daten als Eingriff in das Recht auf Menschenwürde (Artikel 1 der Charta) wahrgenommen werden, insbesondere wenn solche Kontrollen als demütigend empfunden werden. Als jedoch in einer Erhebung[37] der Agentur der EU für Grundrechte (FRA) speziell die Frage gestellt wurde, ob die Bereitstellung der biometrischen Daten im Rahmen von Grenzkontrollen als erniedrigend empfunden werden könnte, wurde dies von den meisten Befragten verneint.

Die vorgeschlagenen Interoperabilitätskomponenten bieten die Möglichkeit, gezielte Präventivmaßnahmen zur Erhöhung der Sicherheit zu beschließen. Damit können sie zum Schutz des Rechts auf Leben (Artikel 2 der Charta) beitragen, wodurch sich auch eine positive Verpflichtung für die Behörden ergibt, operative Präventivmaßnahmen zu ergreifen, um – wenn sie Kenntnis von einer unmittelbaren Bedrohung haben oder haben sollten – eine Person, deren Leben gefährdet ist, zu schützen,[38] sowie das Verbot der Sklaverei und der Zwangsarbeit (Artikel 5 der Charta) einzuhalten. Durch eine zuverlässigere, besser zugängliche und einfachere Identifizierung kann die Interoperabilität das Auffinden von vermissten Kindern oder Kindern, die Opfer von Menschenhandel sind, sowie rasche und gezielte Reaktionen erleichtern.

Eine zuverlässige, besser zugängliche und einfachere Identifizierung könnte auch dazu beitragen, das Recht auf Asyl (Artikel 18 der Charta) und das Verbot der Zurückweisung (Artikel 19 der Charta) wirksam zu garantieren. Die Interoperabilität könnte in der Tat verhindern, dass Asylbewerber unrechtmäßig festgenommen, inhaftiert und abgeschoben werden. Außerdem wird Identitätsbetrug aufgrund der Interoperabilität leichter erkannt werden. Ferner wäre es nur noch in geringerem Maße erforderlich, im Hinblick auf die Identitätsfeststellung und die Ausstellung von Reisedokumenten Daten und Informationen über Asylbewerber mit Drittländern (insbesondere mit dem Herkunftsland) auszutauschen, die die betreffenden Personen in Gefahr bringen könnten.

- **Schutz personenbezogener Daten**

[37] *FRA survey in the framework of the eu-LISA pilot on smart borders — travellers' views on and experiences of smart borders* (Erhebung der FRA im Zusammenhang mit dem Pilotprojekt von eu-LISA zu intelligenten Grenzen – diesbezügliche Ansichten und Erfahrungen von Reisenden), Bericht der Agentur der EU für Grundrechte: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf.

[38] Europäischer Gerichtshof für Menschenrechte, Osman gegen Vereinigtes Königreich, Nr. 87/1997/871/1083, 28. Oktober 1998, Rn. 116.

Da es um personenbezogene Daten geht, wird sich die Interoperabilität vor allem auf das Recht auf Schutz personenbezogener Daten auswirken. Dieses Recht ist in Artikel 8 der Charta, Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union und Artikel 8 der Europäischen Menschenrechtskonvention festgeschrieben. Wie der Gerichtshof der EU betont hat[39], kann das Recht auf Schutz der personenbezogenen Daten jedoch keine uneingeschränkte Geltung beanspruchen, sondern muss im Hinblick auf seine gesellschaftliche Funktion gesehen werden.[40] Der Datenschutz und die Achtung des Privat- und Familienlebens, die durch Artikel 7 der Charta geschützt ist, hängen eng zusammen.

Nach der Datenschutz-Grundverordnung[41] darf der freie Datenverkehr in der EU nicht aus Gründen des Datenschutzes eingeschränkt werden. Jede Einschränkung der Ausübung der durch die Charta geschützten Grundrechte unterliegt einer Reihe von Grundsätzen und ist nur rechtmäßig, wenn die folgenden in Artikel 52 Absatz 1 der Charta festgelegten Kriterien erfüllt sind:

- Sie muss gesetzlich vorgesehen sein;
- sie muss den Wesensgehalt der Rechte achten;
- sie muss den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen;
- sie muss erforderlich sein; und
- sie muss verhältnismäßig sein.

Wie in der Folgenabschätzung zu der vorgeschlagenen Verordnung ausführlich erläutert wurde, trägt der vorliegende Vorschlag all diesen Datenschutzvorschriften Rechnung. Der Vorschlag beruht auf den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen. Er enthält geeignete Bestimmungen, denen zufolge die Datenverarbeitung auf das für den jeweiligen Zweck erforderliche Maß begrenzt und nur denjenigen Stellen Zugriff auf die Daten gewährt wird, die diese benötigen. Die Datenspeicherfristen (soweit relevant) sind angemessen und begrenzt. Der Datenzugriff ist ausschließlich den dazu ermächtigten Bediensteten der Behörden der Mitgliedstaaten oder der EU-Stellen vorbehalten, die für die festgelegten Zwecke der einzelnen Informationssysteme zuständig sind, soweit die Daten zur Erfüllung ihrer Aufgaben im Einklang mit diesen Zwecken erforderlich sind.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Die Auswirkungen auf den Haushalt sind dem beigefügten Finanzbogen zu entnehmen. Dieser erstreckt sich auf den verbleibenden Zeitraum des derzeitigen mehrjährigen Finanzrahmens (bis 2020) und die sieben Jahre des folgenden Zeitraums (2021-2027). Die für

---

[39] Gerichtshof der EU, Urteil vom 9.11.2010 in den verbundenen Rechtssachen C-92/09 und C-93/09, Volker und Markus Schecke und Eifert, Slg. 2010, I-0000.

[40] Im Einklang mit Artikel 52 Absatz 1 der Charta kann die Ausübung des Rechts auf Datenschutz eingeschränkt werden, sofern diese Einschränkungen gesetzlich vorgesehen sind, den Wesensgehalt des Rechts und der Freiheiten achten, unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sind und den von der Europäischen Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

[41] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

die Jahre ab 2021 vorgeschlagenen Haushaltsmittel dienen lediglich der Veranschaulichung und sollen nicht dem nächsten mehrjährigen Finanzrahmen vorgreifen.

Zur Umsetzung dieses Vorschlags bedarf es Mittelzuweisungen für:

1) Die **Entwicklung** und Integration der vier Interoperabilitätskomponenten und des zentralen Speichers für Berichte und Statistiken durch eu-LISA sowie anschließend ihren **Betrieb und ihre Wartung**.

2) Die **Migration der Daten** in den gemeinsamen Dienst für den Abgleich biometrischer Daten (gemeinsamer BMS) und den gemeinsamen Speicher für Identitätsdaten (CIR). Was den gemeinsamen BMS anbelangt, so müssen die biometrischen Templates der entsprechenden Daten aus den drei Systemen, in denen derzeit biometrische Daten erfasst werden (SIS, VIS und Eurodac), im gemeinsamen BMS neu erstellt werden. Was den CIR betrifft, so müssen die personenbezogenen Datenelemente aus dem VIS in den CIR übertragen werden, und die etwaigen Verknüpfungen zwischen Identitäten im SIS, im VIS und in Eurodac müssen validiert werden. Insbesondere dieser letzte Prozess ist ressourcenintensiv.

3) Die Aktualisierung der bereits in die EES-Verordnung aufgenommenen **einheitlichen nationalen Schnittstelle** (national uniform interface – NUI) durch eu-LISA und damit einhergehend ihre Umwandlung in eine generische Komponente, die den Austausch von Mitteilungen zwischen den Mitgliedstaaten und dem Zentralsystem bzw. den Zentralsystemen ermöglicht.

4) Die **Integration der nationalen Systeme der Mitgliedstaaten** und der NUI, die die mit dem CIR bzw. dem Detektor für Mehrfachidentitäten ausgetauschten Mitteilungen über das Europäische Suchportal übermittelt.

5) Die **Schulung** der Endnutzer in Bezug auf die Nutzung der Interoperabilitätskomponenten, unter anderem durch die Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL).

Die Interoperabilitätskomponenten werden im Rahmen eines Programms eingerichtet und gewartet. Während das Europäische Suchportal (ESP) und der Detektor für Mehrfachidentitäten völlig neue Komponenten sind, handelt es sich bei dem gemeinsamen BMS und dem CIR zusammen mit dem zentralen Speicher für Berichte und Statistiken (CRRS) um gemeinsame Komponenten zur Zusammenführung vorhandener Daten, die in bestehenden oder neuen Systemen erfasst wurden bzw. zu erfassen sind, mit den für sie jeweils bereits veranschlagten Haushaltsmitteln.

Das **ESP** wird bekannte bestehende Schnittstellen zum SIS, zum VIS und zu Eurodac implementieren und zu gegebener Zeit auf neue Systeme ausgedehnt.

Das ESP soll von den Mitgliedstaaten und den Agenturen über eine auf das universelle Nachrichtenformat (UMF) gestützte Schnittstelle abgefragt werden. Diese neue Schnittstelle wird Entwicklungen, Anpassungen, Integrationen und Erprobungen durch die Mitgliedstaaten, eu-LISA, Europol und die Europäische Agentur für die Grenz- und Küstenwache erfordern. Das ESP würde nach den Konzepten gestaltet, die der für das EES eingeführten einheitlichen nationalen Schnittstelle (NUI) zugrunde liegen, was den Integrationsaufwand verringern würde.

Mit dem ESP werden insofern zusätzliche Kosten für Europol entstehen, als die QUEST-Schnittstelle für die Verwendung von BPL-Daten (BPL – basic protection level – Basisschutzniveau) angepasst werden muss.

Die Grundlage für den **gemeinsamen BMS** wird de facto mit der Einrichtung des neuen EES geschaffen, da die in diesem System erfassten Daten die weitaus größte Menge an neuen biometrischen Daten darstellen. Die erforderlichen Haushaltsmittel wurden im Rahmen des EES-Rechtsinstruments vorgesehen. Aufgrund der Aufnahme weiterer biometrischer Daten aus dem VIS, dem SIS und Eurodac in den gemeinsamen BMS ergeben sich zusätzliche Kosten, die in erster Linie mit der Migration der vorhandenen Daten zusammenhängen. Diese Kosten werden für alle drei Systeme mit 10 Mio. EUR veranschlagt. Aufgrund der Aufnahme neuer biometrischer Daten aus dem vorgeschlagenen System ECRIS-TCN ergeben sich begrenzte zusätzliche Kosten, die aus den im Rahmen des vorgeschlagenen ECRIS-TCN-Rechtsakts zur Einrichtung eines automatisierten Fingerabdruck-Identifizierungssystems (ECRIS-TCN) vorgesehenen Mitteln gedeckt werden können.

Der **gemeinsame Speicher für Identitätsdaten** wird mit der Einrichtung des künftigen EES erstellt und bei der Entwicklung des vorgeschlagenen ETIAS erweitert. Die Speicher- und Suchmaschinen für die betreffenden Daten wurden bei den Haushaltsmitteln berücksichtigt, die im Rahmen der Rechtsakte für das künftige EES und das vorgeschlagene ETIAS vorgesehen wurden. Aufgrund der Aufnahme neuer biografischer Daten sowohl aus Eurodac als auch aus dem vorgeschlagenen System ECRIS-TCN ergeben sich geringfügige zusätzliche Kosten, die bereits im Rahmen der Rechtsakte für Eurodac und das vorgeschlagene System ECRIS-TCN vorgesehen wurden.

Insgesamt belaufen sich die während eines Zeitraums von neun Jahren (2019-2027) erforderlichen Haushaltsmittel auf 424,7 Mio. EUR für folgende Posten:

1) Mittel in Höhe von 225 Mio. EUR für eu-LISA, die Folgendes abdecken: die Gesamtkosten für die Entwicklung des Programms zur Bereitstellung der fünf Interoperabilitätskomponenten (68,3 Mio. EUR), die Wartungskosten ab dem Zeitpunkt der Bereitstellung der Komponenten bis zum Jahr 2027 (56,1 Mio. EUR), ein spezielles Budget von 25 Mio. EUR für die Migration der Daten aus den bestehenden Systemen in den gemeinsamen BMS und die zusätzlichen Kosten für die Aktualisierung der NUI, für das Netz sowie für Schulungen und Sitzungen. Ein spezielles Budget von 18,7 Mio. EUR deckt die Kosten für die Modernisierung des ECRIS-TCN und dessen ab 2022 vorgesehenen Betrieb im Hochverfügbarkeitsmodus.

2) Mittel in Höhe von 136,3 Mio. EUR für die Änderungen, die die Mitgliedstaaten im Hinblick auf die Nutzung der Interoperabilitätskomponenten an ihren nationalen Systemen vornehmen müssen, und für die von eu-LISA bereitgestellte NUI sowie ein Budget für die Schulung der zahlreichen Endnutzer.

3) Mittel in Höhe von 48,9 Mio. EUR für Europol für die Modernisierung der IT-Systeme von Europol im Hinblick auf die Menge der zu verarbeitenden Mitteilungen und die höheren Leistungsniveaus.[42] Die Interoperabilitätskomponenten werden vom ETIAS für die Abfrage der Europol-Daten genutzt.

[42] Die derzeitige Informationsverarbeitungskapazität von Europol ist nicht vereinbar mit den erwarteten beträchtlichen Mengen an Abfragen (durchschnittlich 100 000 täglich) und der verkürzten Reaktionszeit, die das ETIAS erfordern wird.

4) Mittel in Höhe von 4,8 Mio. EUR für die Europäische Agentur für die Grenz- und Küstenwache für ein Team von Spezialisten, das ab Inbetriebnahme des Detektors für Mehrfachidentitäten während eines Jahres die Verknüpfungen zwischen Identitäten validieren soll.

5) Mittel in Höhe von 2,0 Mio. EUR für die Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL) für die Ausarbeitung und Durchführung von Schulungen für das Betriebspersonal.

6) Bereitstellung von 7,7 Mio. EUR für die GD HOME für eine begrenzte Personalaufstockung und zur Deckung der Kosten, die während des Zeitraums anfallen, in dem die verschiedenen Komponenten entwickelt werden, da die Kommission in diesem Zeitraum zusätzliche Aufgaben übernehmen muss und für den mit dem universellen Nachrichtenformat (UMF) befassten Ausschuss verantwortlich sein wird.

Die Verordnung über den Fonds für die innere Sicherheit (ISF) – Grenzen ist das Finanzierungsinstrument, das die Mittel für die Umsetzung der Interoperabilitätsinitiative enthält. Artikel 5 Absatz 5 Buchstabe b dieser Verordnung sieht vor, dass 791 Mio. EUR im Wege eines Programms für die Entwicklung von auf bestehenden und/oder neuen IT-Systemen basierenden IT-Systemen zur Unterstützung der Steuerung von Migrationsströmen über die Außengrenzen verwendet werden, sofern die entsprechenden Rechtsakte der Union angenommen werden und die in Artikel 15 festgelegten Bedingungen erfüllt sind. Von diesen 791 Mio. EUR sind 480,2 Mio. EUR für die Entwicklung des EES, 210 Mio. EUR für das ETIAS und 67,9 Mio. EUR für die Überarbeitung des SIS vorgesehen. Der Restbetrag (32,9 Mio. EUR) ist nach dem Verfahren des ISF – Grenzen neu zuzuweisen. Gemäß dem vorliegenden Vorschlag ist für den verbleibenden Zeitraum des derzeitigen mehrjährigen Finanzrahmens (2019/2020) ein Betrag von 32,1 Mio. EUR erforderlich, der somit aus den restlichen Haushaltsmitteln gedeckt werden kann.

5. WEITERE ANGABEN

- **Durchführungspläne sowie Monitoring-, Bewertungs- und Berichterstattungsmodalitäten**

Die Agentur eu-LISA ist für das Betriebsmanagement der IT-Großsysteme im Raum der Freiheit, der Sicherheit und des Rechts verantwortlich. In dieser Funktion ist sie bereits mit dem Betrieb und mit technischen und operativen Verbesserungen der bestehenden Systeme sowie mit der Entwicklung der schon geplanten künftigen Systeme betraut. Gemäß der vorgeschlagenen Verordnung wird eu-LISA die Architektur der Interoperabilitätskomponenten konzipieren und für die Entwicklung, die Implementierung und schließlich für das Hosting der Komponenten sorgen. Die jeweiligen Komponenten werden in Verbindung mit der Entwicklung der zugrunde liegenden Systeme schrittweise implementiert.

Die Kommission wird dafür sorgen, dass Verfahren zur Überwachung der Entwicklung und Funktionsweise der vier Komponenten (Europäisches Suchportal, gemeinsamer Dienst für den Abgleich biometrischer Daten, gemeinsamer Speicher für Identitätsdaten, Detektor für Mehrfachidentitäten) und des zentralen Speichers für Berichte und Statistiken eingeführt werden, und sie nach Maßgabe der wichtigsten politischen Ziele bewerten. Vier Jahre nach

Einführung und Inbetriebnahme der Funktionen und danach alle vier Jahre hat eu-LISA dem Europäischen Parlament, dem Rat und der Kommission einen Bericht über die technische Funktionsweise der Interoperabilitätskomponenten zu übermitteln. Darüber hinaus hat die Kommission fünf Jahre nach Einführung und Inbetriebnahme der Funktionen und danach alle vier Jahre eine Gesamtbewertung der Komponenten zu erstellen, die auch die direkten oder indirekten Auswirkungen der Komponenten und ihrer praktischen Umsetzung auf die Grundrechte beinhaltet. Darin sollten die Ergebnisse an den Zielen gemessen werden, und es sollte beurteilt werden, ob die grundlegenden Prinzipien weiterhin Gültigkeit haben; außerdem sollten etwaige Schlussfolgerungen für künftige Optionen gezogen werden. Die Kommission sollte dem Europäischen Parlament und dem Rat die Bewertungsberichte vorlegen.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Kapitel I enthält die allgemeinen Bestimmungen dieser Verordnung. In dem Kapitel wird Folgendes erläutert: die der Verordnung zugrunde liegenden Prinzipien, die durch die Verordnung eingeführten Komponenten, die mit der Interoperabilität verfolgten Ziele, der Anwendungsbereich der Verordnung, die für die Verordnung geltenden Begriffsbestimmungen und der Grundsatz der Nichtdiskriminierung in Bezug auf die im Rahmen der Verordnung erfolgende Datenverarbeitung.

Kapitel II enthält die Bestimmungen über das Europäische Suchportal (ESP). Dieses Kapitel betrifft die Schaffung des ESP und seiner technischen Architektur, die von eu-LISA zu entwickeln sind. Das Ziel des ESP, die Nutzungsberechtigten und die Nutzungsbedingungen nach Maßgabe der für die einzelnen Zentralsysteme geltenden Zugangsrechte sind angegeben. Es ist vorgesehen, dass eu-LISA für jede Nutzerkategorie Nutzerprofile erstellt. Das Kapitel enthält Bestimmungen zur Abfrage der Zentralsysteme über das ESP sowie zu Form und Inhalt der den Nutzern erteilten Antworten. Außerdem sieht Kapitel II vor, dass eu-LISA Protokolle über sämtliche Verarbeitungsvorgänge führt, und es enthält ein Ausweichverfahren für den Fall, dass das ESP nicht auf eines oder mehrere der Zentralsysteme zugreifen kann.

Kapitel III enthält die Bestimmungen über den gemeinsamen Dienst für den Abgleich biometrischer Daten (gemeinsamer BMS). Dieses Kapitel betrifft die Schaffung des gemeinsamen BMS und seiner technischen Architektur, die von eu-LISA zu entwickeln sind. Es wird festgelegt, welchem Ziel der gemeinsame BMS dient und welche Daten gespeichert werden. Ferner wird die Beziehung zwischen dem gemeinsamen BMS und den anderen Komponenten erläutert. Kapitel III sieht zudem vor, dass Daten im gemeinsamen BMS nur so lange gespeichert werden, wie sie in dem jeweiligen Zentralsystem erfasst sind, und dass eu-LISA Protokolle über sämtliche Verarbeitungsvorgänge führt.

Kapitel IV enthält die Bestimmungen über den gemeinsamen Speicher für Identitätsdaten (CIR). Dieses Kapitel betrifft die Schaffung des CIR und seiner technischen Architektur, die von eu-LISA zu entwickeln sind. Es wird festgelegt, welchem Ziel der CIR dient, welche Daten gespeichert werden und wie die Qualität der gespeicherten Daten sicherzustellen ist. Das Kapitel sieht vor, dass im CIR individuelle Dateien auf der Grundlage der in den Zentralsystemen erfassten Daten angelegt und die individuellen Dateien entsprechend den Änderungen in den einzelnen Zentralsystemen aktualisiert werden. In Kapitel IV wird auch angegeben, wie der CIR im Zusammenhang mit dem Detektor für Mehrfachidentitäten funktioniert. In dem Kapitel wird zudem angegeben, wer Zugang zum CIR hat und wie nach Maßgabe der Zugangsrechte auf die Daten zugegriffen werden darf. Außerdem enthält das Kapitel eingehendere Bestimmungen für den Fall, dass der Zugang zum CIR zu Identifizierungszwecken erfolgt, und für den Fall, dass – als erster Schritt im Rahmen des zweistufigen Verfahrens – das EES, das VIS, das ETIAS und Eurodac über den CIR zu

Strafverfolgungszwecken abgefragt werden. Kapitel IV sieht außerdem vor, dass eu-LISA Protokolle über sämtliche im CIR erfolgenden Verarbeitungsvorgänge führt.

Kapitel V enthält die Bestimmungen über den Detektor für Mehrfachidentitäten (MID). Dieses Kapitel betrifft die Schaffung des MID und seiner technischen Architektur, die von eu-LISA zu entwickeln sind. Es wird festgelegt, welchem Ziel der MID dient und wie er nach Maßgabe der für die einzelnen Zentralsysteme geltenden Zugangsrechte zu nutzen ist. In Kapitel V wird angegeben, wann und wie der MID eine Prüfung auf Mehrfachidentitäten durchführt, welche Ergebnisse möglich sind und welche Folgemaßnahmen jeweils zu treffen sind, unter anderem erforderlichenfalls durch manuelle Verifizierung. Kapitel V enthält die Arten von Verknüpfungen, die aus einer Abfrage resultieren können, je nachdem, ob eine einzige Identität, mehrere Identitäten oder gemeinsame Identitätsdaten angezeigt werden. Das Kapitel sieht vor, dass im MID in den Zentralsystemen erfasste verknüpfte Daten gespeichert werden, die Daten aber gleichzeitig in zwei oder mehr einzelnen Zentralsystemen erfasst bleiben. Kapitel V sieht außerdem vor, dass eu-LISA Protokolle über sämtliche im MID erfolgenden Verarbeitungsvorgänge führt.

Kapitel VI enthält Maßnahmen zur Unterstützung der Interoperabilität. Es sieht Folgendes vor: Maßnahmen zur Verbesserung der Datenqualität, die Einführung des universellen Nachrichtenformats als gemeinsamen Standard für den Informationsaustausch zur Unterstützung der Interoperabilität und die Einrichtung eines zentralen Speichers für Berichte und Statistiken.

Kapitel VII betrifft den Datenschutz. Dieses Kapitel enthält Bestimmungen, die gewährleisten, dass die im Rahmen der vorliegenden Verordnung verarbeiteten Daten gemäß den Bestimmungen der Verordnung (EG) Nr. 45/2001 rechtmäßig und ordnungsgemäß verarbeitet werden. Es wird angegeben, welche Stelle der Auftragsverarbeiter für die einzelnen in dieser Verordnung vorgeschlagenen Interoperabilitätsmaßnahmen sein wird. Außerdem werden die Maßnahmen festgelegt, die eu-LISA und die Behörden der Mitgliedstaaten ergreifen müssen, um die Sicherheit der Datenverarbeitung, die Vertraulichkeit der Daten, einen angemessenen Umgang mit Sicherheitsvorfällen und eine angemessene Überwachung der Einhaltung der in der Verordnung vorgesehenen Maßnahmen zu gewährleisten. Außerdem enthält das Kapitel Bestimmungen über die Rechte der betroffenen Personen, darunter das Recht, darüber informiert zu werden, dass sie betreffende Daten im Rahmen dieser Verordnung gespeichert und verarbeitet wurden, sowie das Recht auf Auskunft, Berichtigung und Löschung personenbezogener Daten, die im Rahmen dieser Verordnung gespeichert und verarbeitet wurden. Ferner wird der Grundsatz festgeschrieben, dass die im Rahmen dieser Verordnung verarbeiteten Daten nicht an Drittstaaten, internationale Organisationen oder private Stellen übermittelt oder diesen zur Verfügung gestellt werden dürfen; hiervon ausgenommen sind die Übermittlung an Interpol zu bestimmten Zwecken und Daten, die von Europol über das Europäische Suchportal übermittelt werden, nach Maßgabe der Bestimmungen der Verordnung (EU) 2016/794 über die nachfolgende Datenverarbeitung. Und schließlich enthält das Kapitel Bestimmungen über Kontrolle und Überprüfung in Bezug auf den Datenschutz.

Kapitel VIII regelt die Verantwortlichkeiten von eu-LISA vor und nach Inbetriebnahme der vorgeschlagenen Maßnahmen sowie die Verantwortlichkeiten der Mitgliedstaaten, von Europol und der ETIAS-Zentralstelle.

Kapitel IX enthält Angaben zu folgenden Aspekten: Anforderungen an die Erstellung von Berichten und Statistiken in Bezug auf die im Rahmen dieser Verordnung verarbeiteten Daten; erforderliche Übergangsmaßnahmen; Regelungen für die sich aus dieser Verordnung ergebenden Kosten; Vorgaben für Mitteilungen; Verfahren für die Inbetriebnahme der in

dieser Verordnung vorgeschlagenen Maßnahmen; Befugnisübertragung und Ausschussverfahren, einschließlich der Einsetzung eines Ausschusses und einer Beratergruppe, Verantwortlichkeit von eu-LISA für Schulungen sowie Erstellung eines Handbuchs für die Umsetzung und den Betrieb der Interoperabilitätskomponenten; Verfahren für die Überwachung und Bewertung der in dieser Verordnung vorgeschlagenen Maßnahmen und Inkrafttreten dieser Verordnung.

2017/0352 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag zur Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16 Absatz 2, Artikel 74, Artikel 78 Absatz 2 Buchstabe e, Artikel 79 Absatz 2 Buchstabe c, Artikel 82 Absatz 1 Buchstabe d, Artikel 85 Absatz 1, Artikel 87 Absatz 2 Buchstabe a und Artikel 88 Absatz 2,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Anhörung des Europäischen Datenschutzbeauftragten,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses,[43]

nach Stellungnahme des Ausschusses der Regionen,[44]

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Die Kommission hat in ihrer Mitteilung „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“ vom 6. April 2016[45] darauf hingewiesen, dass die Datenverwaltungsarchitektur der Union im Bereich der Grenzkontrolle und der Sicherheit verbessert werden muss. Durch die Mitteilung wurde ein Prozess eingeleitet, durch den die Interoperabilität zwischen den EU-Informationssystemen für die Bereiche Sicherheit, Grenzmanagement und Migrationssteuerung hergestellt werden soll, um die strukturellen, die Arbeit der nationalen Behörden behindernden Mängel dieser Systeme zu beheben und sicherzustellen, dass Grenzschutzbeamten, Zollbehörden, Polizeibediensteten und Justizbehörden die erforderlichen Informationen zur Verfügung stehen.

(2) Der Rat hat in seinem Fahrplan zur Verbesserung des Informationsaustauschs und des Informationsmanagements einschließlich von Interoperabilitätslösungen im Bereich Justiz und Inneres vom 6. Juni 2016[46] verschiedene rechtliche, technische und praktische Probleme auf dem Weg zur Interoperabilität der Informationssysteme der EU aufgezeigt und diesbezügliche Lösungen gefordert.

---

[43] ABl. C ... vom ... , S. ....

[44]

[45] COM(2016)205 vom 6.4.2016.

[46] Fahrplan vom 6. Juni 2016 zur Verbesserung des Informationsaustauschs und des Informationsmanagements einschließlich von Interoperabilitätslösungen im Bereich Justiz und Inneres (9368/1/16, REV 1).

(3) Das Europäische Parlament hat die Kommission in seiner Entschließung vom 6. Juli 2016 zu den strategischen Prioritäten für das Arbeitsprogramm der Kommission für 2017[47] aufgefordert, Vorschläge zur Verbesserung und Weiterentwicklung der bestehenden Informationssysteme der EU, zur Schließung von Informationslücken, für Maßnahmen zur Herstellung der Interoperabilität dieser Systeme sowie zur Einführung eines obligatorischen Informationsaustausches auf EU-Ebene nebst den erforderlichen Datenschutzvorkehrungen vorzulegen.

(4) Der Europäische Rat hat auf seiner Tagung vom 15. Dezember 2016[48] kontinuierliche Ergebnisse bei der Interoperabilität von Informationssystemen und Datenbanken der EU gefordert.

(5) Die hochrangige Expertengruppe für Informationssysteme und Interoperabilität kam in ihrem Abschlussbericht vom 11. Mai 2017[49] zu dem Schluss, dass es notwendig und technisch möglich ist, auf Lösungen für die Interoperabilität hinzuarbeiten, und dass diese Lösungen grundsätzlich sowohl operative Verbesserungen bewirken als auch im Einklang mit den Datenschutzvorschriften umgesetzt werden können.

(6) Im Einklang mit ihrer Mitteilung vom 6. April 2016 und mit den Erkenntnissen und Empfehlungen der Expertengruppe für Informationssysteme und Interoperabilität hat die Kommission in ihrer Mitteilung „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Siebter Fortschrittsbericht“ vom 16. Mai 2017[50] ein neues Konzept für die Verwaltung grenz-, sicherheits- und migrationsrelevanter Daten vorgestellt, durch das unter uneingeschränkter Achtung der Grundrechte die Interoperabilität aller EU-Informationssysteme für die Bereiche Sicherheit, Grenzmanagement und Migrationssteuerung gewährleistet werden soll.

(7) Der Rat hat die Kommission in seinen Schlussfolgerungen vom 9. Juni 2017[51] zum weiteren Vorgehen zur Verbesserung des Informationsaustauschs und zur Sicherstellung der Interoperabilität der EU-Informationssysteme aufgefordert, die von der hochrangigen Expertengruppe vorgeschlagenen Lösungen zur Verbesserung der Interoperabilität umzusetzen.

(8) Der Europäische Rat hat auf seiner Tagung vom 23. Juni 2017[52] die Notwendigkeit einer besseren Interoperabilität zwischen den Datenbanken betont und die Kommission aufgefordert, so rasch wie möglich Legislativvorschläge zur Umsetzung der Lösungen zu unterbreiten, die die hochrangige Expertengruppe für Informationssysteme und Interoperabilität vorgeschlagen hat.

(9) Um das Außengrenzenmanagement zu verbessern und um zur Verhütung und Bekämpfung irregulärer Migration und zur Gewährleistung eines hohen Maßes an Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts der Union einschließlich der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie des Schutzes der inneren Sicherheit im Hoheitsgebiet der Mitgliedstaaten beizutragen, sollte Interoperabilität zwischen den Informationssystemen der EU – d.h. zwischen [dem Einreise-/Ausreisesystem (EES)], dem Visa-Informationssystem (VIS), [dem Europäischen Reiseinformations- und -genehmigungssystem (ETIAS)], Eurodac, dem

---

47 Entschließung des Europäischen Parlaments vom 6. Juli 2016 zu den strategischen Prioritäten für das Arbeitsprogramm der Kommission für 2017 (2016/2773(RSP)).

48 http://www.consilium.europa.eu/de/press/press-releases/2016/12/15/euco-conclusions-final/

49 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1

50 COM(2017) 261 final vom 16.5.2017.

51 http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf

52 Schlussfolgerungen des Europäischen Rates vom 22./23 Juni 2017.

Schengener Informationssystem (SIS) und [dem Europäischen Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN)] – hergestellt werden, damit diese Informationssysteme der EU und ihre Daten einander ergänzen können. Als Interoperabilitätskomponenten sollten zu diesem Zweck ein Europäisches Suchportal (European search portal - ESP), ein gemeinsamer Dienst für den Abgleich biometrischer Daten (biometric matching service - BMS), ein gemeinsamer Speicher für Identitätsdaten (common identity repository - CIR) und ein Detektor für Mehrfachidentitäten (multiple-identity detector - MID) geschaffen werden.

(10) Die Informationssysteme der EU sollten so miteinander verbunden werden, dass sie einander ergänzen, damit die korrekte Identifizierung von Personen vereinfacht und ein Beitrag zur Bekämpfung von Identitätsbetrug geleistet wird, damit die Datenqualitätsanforderungen der verschiedenen Informationssysteme der EU verbessert und harmonisiert werden, damit den Mitgliedstaaten die technische und die operative Umsetzung bestehender und künftiger Informationssysteme der EU erleichtert wird, damit die für die einzelnen Informationssysteme der EU geltenden Sicherheitsvorkehrungen für die Sicherheit und den Schutz der Daten verschärft und vereinfacht werden und damit der Zugang der Strafverfolgungsbehörden zum EES, zum VIS, [zum ETIAS] und zu Eurodac einheitlich geregelt wird und die Zwecke des EES, des VIS, [des ETIAS], von Eurodac, des SIS [und des ECRIS-TCN] gefördert werden.

(11) Die Interoperabilitätskomponenten sollten sich auf das EES, das VIS, [das ETIAS], Eurodac, das SIS [und das ECRIS-TCN] erstrecken. Zudem sollten sie sich in dem Maße auf Europol-Daten erstrecken, wie es erforderlich ist, diese gleichzeitig zu diesen Informationssystemen der EU abzufragen.

(12) Die Interoperabilitätskomponenten sollten sich auf Personen beziehen, deren personenbezogene Daten in den Informationssystemen der EU und von Europol verarbeitet werden können, d. h. auf Drittstaatsangehörige, deren personenbezogene Daten in den Informationssystemen der EU und von Europol verarbeitet werden, und auf EU-Bürger, deren personenbezogene Daten im SIS und von Europol verarbeitet werden.

(13) Das ESP sollte mit dem Ziel geschaffen werden, den Behörden der Mitgliedstaaten und den EU-Stellen mit technischen Mitteln einen raschen, unterbrechungsfreien, effizienten, systematischen und kontrollierten Zugang zu den Informationssystemen der EU, den Europol-Daten und den Datenbanken von Interpol nach Maßgabe ihrer Zugangsrechte zu erleichtern, den sie benötigen, um ihren Aufgaben nachzukommen, und die Ziele des EES, des VIS, [des ETIAS], von Eurodac, des SIS, [des ECRIS-TCN] und der Europol-Daten zu unterstützen. Das ESP sollte die gleichzeitige, parallel erfolgende Abfrage aller einschlägigen Informationssysteme der EU sowie der Europol-Daten und der Interpol-Datenbanken ermöglichen und auf diese Weise als einzige Schnittstelle („Fenster“) für eine nahtlose, unter vollständiger Wahrung der Zugangskontroll- und Datenschutzanforderungen der zugrunde liegenden Systeme erfolgende Abfrage der erforderlichen Informationen in den verschiedenen Zentralsystemen dienen.

(14) Endnutzer des ESP, die gemäß der Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates[53] Zugang zu Europol-Daten haben, sollten die Europol-

[53] Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur

Daten gleichzeitig zu den Informationssystemen der EU, zu denen sie Zugang haben, abfragen dürfen. Jedwede sich an eine solche Anfrage anschließende Datenverarbeitung sollte in Übereinstimmung mit der Verordnung (EU) 2016/794 stehen und insbesondere etwaigen vom Datenlieferanten festgelegten Zugangs- oder Nutzungsbeschränkungen Rechnung tragen.

(15) Das Europäische Suchportal (ESP) sollte so konzipiert und konfiguriert werden, dass bei der Datenabfrage keine Suchfelder für Daten verwendet werden können, die sich nicht auf Personen oder Reisedokumente beziehen oder die nicht in einem Informationssystem der EU, in den Europol-Daten oder in der Interpol-Datenbank vorhanden sind.

(16) Um einen raschen und systematischen Rückgriff auf sämtliche Informationssysteme der EU zu ermöglichen, sollte das Europäische Suchportal für die Abfrage des gemeinsamen Speichers für Identitätsdaten, des EES, des VIS, [des ETIAS], von Eurodac und [des ECRIS-TCN] verwendet werden. Die nationalen Verbindungen zu den verschiedenen Informationssystemen der EU sollten gleichwohl aufrechterhalten werden, um eine technische Ausweichmöglichkeit zu haben. Das ESP sollte zudem von den EU-Stellen dazu genutzt werden, das zentrale SIS in Übereinstimmung mit ihren jeweiligen Zugangsrechten abzufragen und ihren Aufgaben nachzukommen. Das ESP sollte als zusätzliches, die bestehenden spezifischen Schnittstellen ergänzendes Werkzeug für die Abfrage des zentralen SIS, von Europol-Daten und der Interpol-Systeme dienen.

(17) Biometrische Daten wie Fingerabdrücke und Gesichtsbilder sind einmalig und daher für die Personenidentifizierung weit zuverlässiger als alphanumerische Daten. Der gemeinsame Dienst für den Abgleich biometrischer Daten (BMS) sollte als technisches Hilfsmittel für die Verstärkung und Vereinfachung der Funktion der einschlägigen Informationssysteme der EU und der anderen Interoperabilitätskomponenten dienen. Der Hauptzweck des gemeinsamen BMS sollte darin bestehen, die Identifizierung einer möglicherweise in unterschiedlichen Datenbanken erfassten Person anhand eines systemübergreifenden Abgleichs ihrer biometrischen Daten unter Rückgriff auf eine einzige technologische Komponente (anstatt auf fünf unterschiedliche technologische Komponenten der einzelnen zugrunde liegenden Systeme) zu ermöglichen. Durch den Rückgriff auf eine einzige technologische Komponente (anstatt auf fünf unterschiedliche technologische Komponenten der einzelnen zugrunde liegenden Systeme) sollte der gemeinsame BMS zur Sicherheit beitragen und finanzielle, wartungstechnische und operative Vorteile bieten. Alle automatischen Systeme zur Identifizierung von Fingerabdrücken einschließlich der derzeit für Eurodac, das VIS und das SIS eingesetzten Systeme arbeiten mit biometrischen Merkmalsdaten (Templates), die aus konkreten biometrischen Proben generiert werden. Sämtliche biometrischen Templates dieser Art sollten im gemeinsamen BMS an einem einzigen Ort zusammengefasst und gespeichert werden, um den systemübergreifenden Vergleich anhand biometrischer Daten zu vereinfachen und Größenvorteile bei der Entwicklung und Wartung der Zentralsysteme der EU zu ermöglichen.

(18) Bei biometrischen Daten handelt es sich um sensible personenbezogene Daten. Mit dieser Verordnung sollten die Grundlagen und die Garantien für die Verarbeitung

---

Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 24.5.2016, S. 53).

derartiger Daten für die Zwecke einer eindeutigen Identifizierung betroffener Personen festgelegt werden.

(19) Die Systeme, die durch die Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates[54], durch die Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates[55] und durch [die ETIAS-Verordnung] für das Grenzmanagement der Union errichtet wurden, das [durch die Eurodac-Verordnung] errichtete System für die Identifizierung von Personen, die internationalen Schutz beantragen, und für die Bekämpfung der irregulären Migration, sowie das durch die [ECRIS-TCN-Verordnung] errichtete System müssen sich, um wirksam sein zu können, auf eine genaue Identifizierung der Drittstaatsangehörigen, deren personenbezogene Daten in diesen Systemen erfasst werden, stützen können.

(20) Der CIR sollte daher die korrekte Identifizierung von im EES, im VIS, [im ETIAS], in Eurodac und [im ECRIS-TCN] erfassten Personen erleichtern und unterstützen.

(21) Die in diesen Informationssystemen der EU gespeicherten personenbezogenen Daten können sich auf unterschiedliche oder unvollständige Identitäten ein und derselben Person beziehen. Die Mitgliedstaaten verfügen über effiziente Möglichkeiten zur Identifizierung ihrer Staatsangehörigen oder von als dauerhaft in ihrem Hoheitsgebiet wohnhaft gemeldeten Personen; dies gilt jedoch nicht für Drittstaatsangehörige. Die Interoperabilität zwischen den Informationssystemen der EU sollte zur korrekten Identifizierung von Drittstaatsangehörigen beitragen. Im CIR sollten jene personenbezogenen Daten von in den Systemen erfassten Drittstaatsangehörigen gespeichert werden, die für eine genauere Identifizierung dieser Personen erforderlich sind (Identitätsdaten, Reisedokumentendaten und biometrische Daten) – und dies unabhängig davon, in welchem System die betreffenden Daten ursprünglich erfasst wurden. Im CIR sollten ausschließlich solche personenbezogenen Daten gespeichert werden, die für eine genaue Identitätsprüfung unbedingt erforderlich sind. Die im CIR erfassten personenbezogenen Daten sollten nicht länger als für die Zwecke der zugrunde liegenden Systeme unbedingt erforderlich gespeichert und entsprechend den Bestimmungen über die logische Trennung dieser Daten automatisch gelöscht werden, wenn die betreffenden Daten in den zugrunde liegenden Systemen gelöscht werden.

(22) Der neue Datenverarbeitungsvorgang, welcher darin besteht, dass derartige Daten anstatt in den einzelnen separaten Systemen im CIR gespeichert werden, ist erforderlich, um eine genauere Identifizierung zu gewährleisten, welche durch den automatischen Ver- und Abgleich dieser Daten ermöglicht wird. Die Tatsache, dass die Identitätsdaten und die biometrischen Daten von Drittstaatsangehörigen im CIR gespeichert werden, sollte die Datenverarbeitung für die Zwecke der Verordnungen über das EES, das VIS, das ETIAS, Eurodac oder das ECRIS-TCN in keiner Weise behindern, da der CIR eine neue gemeinsame Komponente dieser zugrunde liegenden Systeme darstellen sollte.

---

[54] 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 der Europäischen Union und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung der Verordnung (EG) Nr. 767/2008 und der Verordnung (EU) Nr. 1077/2011 (ABl. L 327 vom 9.12.2017, S. 20).

[55] 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).

(23) In diesem Zusammenhang ist es notwendig, im CIR für jede im EES, im VIS, im ETIAS, in Eurodac oder im ECRIS-TCN erfasste Person eine individuelle Datei anzulegen, um die bezweckte korrekte Identifizierung von Drittstaatsangehörigen im Schengen-Raum zu ermöglichen und den Detektor für Mehrfachidentitäten zu unterstützen, durch den zugleich die Identitätsprüfung von Bona-fide-Reisenden vereinfacht und Identitätsbetrug bekämpft werden soll. In der individuellen Datei sollten alle möglichen mit einer Person verknüpften Identitäten an einem Ort gespeichert und den ordnungsgemäß ermächtigten Endnutzern zugänglich gemacht werden.

(24) Der CIR sollte auf diese Weise das Funktionieren des Detektors für Mehrfachidentitäten unterstützen sowie den Zugang von Strafverfolgungsbehörden zu jenen Informationssystemen der EU, die nicht ausschließlich für die Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung schwerer Straftaten errichtet wurden, erleichtern und vereinfachen.

(25) Der CIR sollte eine gemeinsame Speichereinheit für Identitätsdaten und biometrische Daten von im EES, im VIS, [im ETIAS], in Eurodac und [im ECRIS-TCN] erfassten Drittstaatsangehörigen einschließen, die als gemeinsame Komponente dieser Systeme für die Speicherung und Abfrage derartiger Daten dient.

(26) Sämtliche Datensätze im CIR sollten logisch voneinander getrennt werden, indem jeder Datensatz durch eine entsprechende Kennzeichnung automatisch mit dem zugrunde liegenden System, zu dem er gehört, verknüpft wird. Das Zugangskontrollsystem des CIR sollte nach Maßgabe dieser Kennzeichnung den Zugang zu den betreffenden Datensätzen erteilen bzw. verweigern.

(27) Um die korrekte Identifizierung einer Person zu ermöglichen, sollte den für die Verhütung und Bekämpfung irregulärer Migration zuständigen mitgliedstaatlichen Behörden und den zuständigen Behörden im Sinne von Artikel 3 Absatz 7 der Richtlinie (EU) 2016/680 gestattet werden, im CIR eine Suchabfrage anhand der bei einer Identitätsprüfung erhobenen biometrischen Daten einer Person vorzunehmen.

(28) Falls die biometrischen Daten dieser Person nicht verwendet werden können oder die Abfrage anhand dieser Daten nicht erfolgreich ist, sollte die Abfrage mittels Identitätsdaten dieser Person in Verbindung mit Reisedokumentendaten vorgenommen werden. Falls die Abfrage ergibt, dass im CIR Daten über diese Person gespeichert sind, sollten die mitgliedstaatlichen Behörden in die im CIR gespeicherten Identitätsdaten dieser Person Einsicht nehmen können, ohne dass ihnen in irgendeiner Form angezeigt wird, aus welchem Informationssystem der EU die Daten stammen.

(29) Die Mitgliedstaaten sollten nationale Legislativmaßnahmen zur Benennung der zu Identitätsprüfungen unter Rückgriff auf den CIR befugten Behörden und zur Festlegung der Verfahren, Bedingungen und Kriterien für derartige Prüfungen in Übereinstimmung mit dem Grundsatz der Verhältnismäßigkeit erlassen. Insbesondere sollte durch nationale Legislativmaßnahmen die Befugnis eingeführt werden, dass Mitglieder dieser Behörden bei einer im Beisein einer Person erfolgenden Identitätsprüfung biometrische Daten dieser Person erheben dürfen.

(30) Durch diese Verordnung sollte zudem eine neue Möglichkeit zur Vereinfachung des Zugangs der von den Mitgliedstaaten benannten Strafverfolgungsbehörden und von Europol zu im EES, im VIS, [im ETIAS] oder in Eurodac gespeicherten, nicht identitätsbezogenen Daten geschaffen werden. Derartige in diesen Systemen gespeicherte Daten können nämlich im Einzelfall für die Verhütung, Aufdeckung,

Untersuchung und Verfolgung terroristischer Straftaten oder sonstiger schwerer Straftaten benötigt werden.

(31) Die Frage eines vollständigen Zugangs zu in den Informationssystemen der EU gespeicherten Daten, welche für die Zwecke der Verhütung, Aufdeckung und Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten erforderlich sind und über die im CIR gespeicherten einschlägigen Identitätsdaten, welche mittels bei einer Identitätsprüfung erhobener biometrischer Daten der betreffenden Person eingeholt wurden, hinausgehen, sollte weiterhin durch die einschlägigen Rechtsvorschriften geregelt werden. Die benannten Strafverfolgungsbehörden und Europol wissen nie im Voraus, in welchen Informationssystemen der EU Daten zu den Personen, die Gegenstand ihrer Ermittlungen sind, gespeichert sind. Dies führt dazu, dass sie ihren Aufgaben mitunter nur verzögert oder auf ineffiziente Weise nachkommen können. Den von der benannten Behörde ermächtigten Endnutzern sollte daher angezeigt werden, in welchem Informationssystem der EU die von ihnen abgefragten Daten gespeichert sind. Zu diesem Zweck sollte im Anschluss an die automatische Prüfung auf Vorliegen eines Treffers das betreffende Informationssystem automatisch gekennzeichnet werden („Trefferkennzeichnungsfunktion“).

(32) In den Protokollen der Datenabfragen im CIR sollte der jeweilige Abfragezweck aufgeführt werden. Bei Datenabfragen, die nach dem zweistufigen Datenabfrageverfahren erfolgen, sollte in den Protokollen das Aktenzeichen des betreffenden nationalen Untersuchungsdossiers bzw. Falls angegeben werden, um anzuzeigen, dass die Abfrage zu den Zwecken der Verhütung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten erfolgte.

(33) Von den benannten Behörden der Mitgliedstaaten oder von Europol vorgenommene Datenabfragen im CIR, die zu dem Zweck erfolgen, eine Antwort zu erhalten, in der angezeigt wird, dass die betreffenden Daten im EES, im VIS, [im ETIAS] oder in Eurodac gespeichert sind, erfordern eine automatische Verarbeitung personenbezogener Daten. Bei einer Trefferanzeige sollten außer dem Hinweis, dass Daten der betroffenen Person in einem der Informationssysteme der EU gespeichert sind, keine personenbezogenen Daten der betroffenen Person angezeigt werden. Ermächtigte Endnutzer sollten keine die betroffene Person beschwerenden Entscheidungen treffen, die sich allein auf das Vorliegen eines angezeigten Treffers gründen. Der durch den Endnutzer eines angezeigten Treffers erfolgende Datenzugriff würde somit einen nur sehr begrenzten Eingriff in das Recht der betroffenen Person auf Schutz ihrer personenbezogenen Daten bedeuten; gleichzeitig wäre es erforderlich, der benannten Behörde bzw. Europol zu erlauben, ihre Anträge auf Zugang zu personenbezogenen Daten effizienzhalber direkt an das Informationssystem der EU zu richten, in dem die betreffenden Daten wie angezeigt gespeichert sind.

(34) Das zweistufige Datenabfrageverfahren ist vor allem in Fällen sinnvoll, in denen der Verdächtige, der Täter oder das mutmaßliche Opfer einer terroristischen oder sonstigen schweren Straftat unbekannt ist. In derartigen Fällen sollte der CIR die Ermittlung des Informationssystems, in dem die betreffende Person erfasst ist, mittels eines einzigen Suchvorgangs ermöglichen. Für derartige Fälle sollte ein obligatorischer Rückgriff der Strafverfolgungsbehörden auf diese neue Zugriffsmöglichkeit vorgesehen werden, sodass für den Zugriff auf die im EES, im VIS, [im ETIAS] und in Eurodac gespeicherten personenbezogenen Daten künftig keine vorherige Abfrage der nationalen Datenbanken und der automatischen Fingerabdruckidentifizierungssysteme anderer Mitgliedstaaten gemäß dem Beschluss

2008/615/JI mehr erforderlich wäre. Durch die Vorgabe, dass grundsätzlich vorab eine Suchabfrage vorzunehmen ist, werden die mitgliedstaatlichen Behörden in ihren Möglichkeiten beschnitten, die betreffenden Systeme für berechtigte Strafverfolgungszwecke zu Rate zu ziehen, was im Hinblick auf die Aufdeckung notwendiger Informationen zu verpassten Gelegenheiten führen kann. Die Anforderung, dass vorab die nationalen Datenbanken und das automatische Fingerabdruckidentifizierungssystem gemäß dem Beschluss 2008/615/JI abzufragen sind, sollte erst ab dem Zeitpunkt nicht mehr gelten, ab dem das zweistufige Datenabfrageverfahren für den über den CIR erfolgenden Datenzugriff der Strafverfolgungsbehörden als sichere Alternative verwendbar ist.

(35) Der MID sollte mit dem Ziel geschaffen werden, das Funktionieren des CIR und die Ziele des EES, des VIS, [des ETIAS], von Eurodac, des SIS und [des ECRIS-TCN] zu unterstützen. Damit die jeweiligen Ziele dieser Informationssysteme der EU wirksam umgesetzt werden können, ist es erforderlich, dass die Personen, deren personenbezogene Daten in diesen Systemen gespeichert werden, genau ermittelt werden.

(36) Bisher werden die Möglichkeiten für die Verwirklichung der Ziele der Informationssysteme der EU insofern beeinträchtigt, als es den auf diese Systeme zurückgreifenden Behörden nicht möglich ist, die Identität von Drittstaatsangehörigen, deren Daten in den einzelnen Systemen gespeichert sind, mit hinreichender Zuverlässigkeit zu verifizieren. Dies ist darauf zurückzuführen, dass es sich bei den in einem gegebenen System gespeicherten Identitätsdaten um bewusst oder unbewusst gemachte Falschangaben oder um unvollständige Angaben handeln kann, die mit den bisher bestehenden Möglichkeiten nicht mittels Vergleich mit in anderen Systemen gespeicherten Daten als solche erkannt werden können. Um hier Abhilfe zu schaffen, ist es erforderlich, auf Unionsebene ein technisches Instrument einzuführen, das die genaue Identifizierung von Drittstaatsangehörigen zu diesen Zwecken ermöglicht.

(37) Der MID sollte Verknüpfungen zwischen den in den einzelnen Informationssystemen der EU erfassten Daten herstellen und speichern, damit Mehrfachidentitäten aufgedeckt werden können, um zugleich die Identitätsprüfung von Bona-fide-Reisenden zu vereinfachen und Identitätsbetrug zu bekämpfen. Der MID sollte ausschließlich Verknüpfungen zwischen Personen enthalten, die in mehr als einem Informationssystem der EU erfasst sind, wobei der diesbezügliche Datenzugriff strikt auf die Daten begrenzt werden sollte, welche erforderlich sind, um zu verifizieren, ob eine Person korrekt erfasst oder aber illegal mit mehreren biografischen Identitäten in unterschiedlichen Systemen erfasst ist, oder um zu überprüfen, ob es sich bei zwei Personen mit ähnlichen biografischen Daten um ein und dieselbe Person handelt. Die durch das ESP und den gemeinsamen BMS erfolgende Datenverarbeitung zum Zwecke der systemübergreifenden Verknüpfung von individuellen Dateien sollte ein absolutes Mindestmaß nicht überschreiten und zu diesem Zweck auf eine Prüfung auf Mehrfachidentitäten begrenzt werden, welche nur dann erfolgen sollte, wenn neue Daten in eines der in den CIR und das SIS integrierten Informationssysteme aufgenommen werden. Der MID sollte Absicherungen gegen eine mögliche Diskriminierung von Personen mit legalen Mehrfachidentitäten oder gegen derartige Personen beschwerende Entscheidungen einschließen.

(38) Diese Verordnung sieht die Einführung neuer Datenverarbeitungsverfahren vor, die die korrekte Identifizierung der betroffenen Personen ermöglichen sollen. Diese Verfahren bedeuten einen Eingriff in die nach den Artikeln 7 und 8 der Charta der Grundrechte geschützten Grundrechte dieser Personen. Da die Informationssysteme

der EU nur im Falle einer korrekten Identifizierung der betroffenen Personen wirksam genutzt werden können, ist ein solcher Eingriff aufgrund der Ziele, zu deren Erreichung die einzelnen Informationssysteme der EU errichtet wurden (wirksames Management der Unionsgrenzen, Wahrung der inneren Sicherheit der Union, wirksame Umsetzung der Asyl- und der Visapolitik der Union sowie Bekämpfung irregulärer Migration), gerechtfertigt.

(39) Das ESP und der gemeinsame BMS sollten immer dann, wenn von einer nationalen Behörde oder von einer EU-Stelle neue Datensätze angelegt werden, einen Datenabgleich mit den im CIR und im SIS erfassten personenbezogenen Daten vornehmen. Der Datenabgleich sollte automatisch erfolgen. Um etwaige Verknüpfungen anhand biometrischer Daten aufzudecken, sollten der CIR und das SIS auf den gemeinsamen BMS zurückgreifen. Um etwaige Verknüpfungen anhand alphanumerischer Daten aufzudecken, sollten der CIR und das SIS auf das ESP zurückgreifen. Der CIR und das SIS sollten dazu geeignet sein, identische oder ähnliche Daten über in verschiedenen Systemen erfasste Drittstaatsangehörige zu ermitteln. Werden solche Daten ermittelt, sollte eine Verknüpfung angelegt werden, die anzeigt, dass es sich jeweils um ein und dieselbe Person handelt. Der CIR und das SIS sollten so konfiguriert werden, dass etwaige kleinere Transliterations- oder Buchstabierfehler zwar aufgedeckt werden, aber keine nicht gerechtfertigten beschwerenden Maßnahmen für den betreffenden Drittstaatsangehörigen zur Folge haben.

(40) Die nationale Behörde oder die EU-Stelle, die die Daten in das betreffende Informationssystem der EU eingegeben hat, sollte diese Verknüpfungen bestätigen bzw. entsprechend ändern. Die Behörde sollte auf die im CIR oder im SIS und im MID gespeicherten Daten für die Zwecke einer manuellen Identitätsverifizierung zugreifen dürfen.

(41) Der Zugriff von mitgliedstaatlichen Behörden und EU-Stellen, die Zugang zu mindestens einem in den CIR oder das SIS integrierten Informationssystem der EU haben, auf den MID sollte auf sogenannte rote Verknüpfungen beschränkt werden; derartige Verknüpfungen werden angelegt, wenn die durch die Verknüpfung bezeichneten Daten identische biometrische Daten, aber unterschiedliche Identitätsdaten enthalten und die für die Verifizierung unterschiedlicher Identitäten zuständige Behörde festgestellt hat, dass eine Rechtswidrigkeit vorliegt und sich die Daten in Wirklichkeit auf ein und dieselbe Person beziehen, oder aber, wenn die durch die Verknüpfung bezeichneten Daten ähnliche Identitätsdaten enthalten und die für die Verifizierung unterschiedlicher Identitäten zuständige Behörde festgestellt hat, dass diese Daten illegalerweise ein und dieselbe Person bezeichnen. In Fällen, in denen die durch die Verknüpfung bezeichneten Identitätsdaten einander nicht ähnlich sind, sollte eine gelbe Verknüpfung angelegt und von Hand verifiziert werden, ob die Verknüpfung korrekt ist oder aber ihre Farbe entsprechend geändert werden muss.

(42) Die manuelle Verifizierung von Mehrfachidentitäten sollte von der Behörde vorgenommen werden, die die Daten eingegeben bzw. aktualisiert hat, welche zu dem Treffer geführt haben, aufgrund dessen eine Verknüpfung zu bereits in einem anderen Informationssystem der EU gespeicherten Daten angelegt wurde. Die für die Verifizierung von Mehrfachidentitäten zuständige Behörde sollte jeweils prüfen, ob legale oder illegale Mehrfachidentitäten vorliegen. Diese Prüfung sollte nach Möglichkeit im Beisein des betreffenden Drittstaatsangehörigen erfolgen, der bei Bedarf um zusätzliche Präzisierungen oder Auskünfte gebeten werden sollte. Die Prüfung sollte unverzüglich und in Übereinstimmung mit den im Unionsrecht und im

nationalen Recht festgelegten Anforderungen an die Genauigkeit von Informationen vorgenommen werden.

(43) In Bezug auf angezeigte Verknüpfungen zum SIS, die sich auf Ausschreibungen von Personen zum Zwecke der Übergabe- oder Auslieferungshaft, von Vermissten oder Schutzbedürftigen oder von im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesuchten Personen, auf Personenausschreibungen zum Zwecke der verdeckten oder der gezielten Kontrolle oder auf Ausschreibungen von unbekannten gesuchten Personen beziehen, sollte das SIRENE-Büro des Mitgliedstaats, der die Ausschreibung vorgenommen hat, für die Verifizierung etwaiger Mehrfachidentitäten zuständig sein. Diese Kategorien von SIS-Ausschreibungen haben einen sensiblen Charakter und sollten daher nicht notwendigerweise gegenüber den Behörden, die die betreffenden Daten in einem anderen Informationssystem der EU eingegeben bzw. aktualisiert haben, offengelegt werden. Durch die Erstellung einer Verknüpfung zu SIS-Daten sollte den nach Maßgabe der [SIS-Verordnungen] zu ergreifenden Maßnahmen nicht vorgegriffen werden.

(44) Die Agentur eu-LISA sollte automatische Datenqualitätskontrollmechanismen und gemeinsame Datenqualitätsindikatoren konzipieren. Ferner sollte sie dafür verantwortlich sein, Kapazitäten für die zentrale Überwachung der Datenqualität zu entwickeln und regelmäßige Datenanalyseberichte zu erstellen, um eine bessere Kontrolle der Implementierung und Anwendung der Informationssysteme der EU in den Mitgliedstaaten zu ermöglichen. Die gemeinsamen Qualitätsindikatoren sollten Mindestqualitätsstandards für die Datenspeicherung in den Informationssystemen der EU oder in den Interoperabilitätskomponenten einschließen. Ziel dieser Datenqualitätsstandards sollte sein, dass die Informationssysteme der EU und die Interoperabilitätskomponenten die automatische Ermittlung anscheinend falscher oder unstimmiger Dateneinträge ermöglichen und so dem Mitgliedstaat, der die Daten eingegeben hat, die Möglichkeit gegeben wird, die betreffenden Daten zu überprüfen und etwaige erforderliche Abhilfemaßnahmen zu ergreifen.

(45) Die Kommission sollte die von eu-LISA erstellten Qualitätsberichte auswerten und gegebenenfalls entsprechende Empfehlungen an die Mitgliedstaaten richten. Die Mitgliedstaaten sollten dafür verantwortlich sein, einen Aktionsplan aufzustellen, in dem Maßnahmen zur Behebung etwaiger Mängel in Bezug auf die Datenqualität beschrieben werden, und der Kommission regelmäßig über diesbezüglich erzielte Fortschritte Bericht erstatten.

(46) Das universelle Nachrichtenformat (Universal Message Format – UMF) sollte als Standard für den strukturierten grenzübergreifenden Informationsaustausch zwischen Informationssystemen, Behörden und/oder Organisationen im Bereich Justiz und Inneres festgelegt werden. Durch das UMF sollten ein gemeinsames Vokabular und logische Strukturen für üblicherweise ausgetauschte Informationen vorgegeben werden, damit die ausgetauschten Inhalte einheitlich und semantisch gleichwertig erstellt und gelesen werden können und somit die Interoperabilität verbessert wird.

(47) Es sollte ein zentraler Speicher für Berichte und Statistiken (central repository for reporting and statistics – CRRS) eingerichtet werden, der die systemübergreifende Erhebung statistischer Daten und die Erstellung von Analyseberichten zu politischen und operativen Zwecken sowie für die Zwecke der Datenqualität ermöglicht. Der CRRS sollte von eu-LISA konzipiert, implementiert und an ihren technischen Standorten installiert werden und anonyme statistische Daten aus den oben genannten Systemen, dem CIR, dem MID und dem gemeinsamen BMS enthalten. Die im CRRS

enthaltenen Daten sollten keine Identifizierung von Einzelpersonen ermöglichen. Die Daten sollten von eu-LISA anonymisiert und als solche im CRRS gespeichert werden. Die Anonymisierung sollte automatisch erfolgen, und den Bediensteten von eu-LISA sollte kein direkter Zugang zu den in den Informationssystemen der EU oder in den Operabilitätskomponenten gespeicherten personenbezogenen Daten gewährt werden.

(48) Die im Rahmen dieser Verordnung erfolgende Verarbeitung personenbezogener Daten durch nationale Behörden sollte den Bestimmungen der Verordnung (EU) 2016/679 unterliegen, sofern sie nicht durch benannte Behörden oder zentrale Anlaufstellen der Mitgliedstaaten zum Zwecke der Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten erfolgt; im letztgenannten Fall sollte die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates maßgeblich sein.

(49) Die einschlägigen Datenschutzbestimmungen [der Eurodac-Verordnung,] [der Verordnung über das SIS im Bereich der Strafverfolgung,] [der Verordnung über das SIS im Bereich der Rückkehr illegal aufhältiger Drittstaatsangehöriger] und [der ECRIS-TCN-Verordnung] sollten für die jeweils in diesen Systemen erfolgende Verarbeitung personenbezogener Daten gelten.

(50) Die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates[56] sollte für die Verarbeitung personenbezogener Daten durch die Agentur eu-LISA und andere EU-Stellen bei der Wahrnehmung ihrer Aufgaben aufgrund dieser Verordnung gelten und die Verordnung (EU) 2016/794 unberührt lassen, welche ihrerseits für die Verarbeitung personenbezogener Daten durch Europol maßgeblich sein sollte.

(51) Die gemäß [der Verordnung (EU) 2016/679] eingerichteten nationalen Aufsichtsbehörden sollten die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten überwachen, während der gemäß der Verordnung (EG) Nr. 45/2001 eingesetzte Europäische Datenschutzbeauftragte die Tätigkeiten der Organe und Einrichtungen der Union in Bezug auf die Verarbeitung personenbezogener Daten kontrollieren sollte. Der Europäische Datenschutzbeauftragte und die Aufsichtsbehörden sollten bei der Überwachung der Verarbeitung personenbezogener Daten durch Interoperabilitätskomponenten zusammenarbeiten.

(52) „(...) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 angehört und hat seine Stellungnahme am […] abgegeben."

(53) In Bezug auf die Geheimhaltung unterliegen die Beamten und sonstigen Bediensteten, die in Verbindung mit dem SIS eingesetzt oder tätig werden, den einschlägigen Bestimmungen des Statuts der Beamten und der Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union.

(54) Die Mitgliedstaaten und eu-LISA sollten über Sicherheitspläne verfügen, die die Erfüllung der Sicherheitsanforderungen erleichtern; ferner sollten sie Sicherheitsfragen gemeinsam angehen. Zudem sollte eu-LISA sicherstellen, dass zur Gewährleistung der Datenintegrität bei Konzeption, Entwicklung und Betrieb der Interoperabilitätskomponenten fortwährend auf die neuesten technologischen Entwicklungen zurückgegriffen wird.

---

[56] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

(55) Zu statistischen Zwecken und für die Berichterstattung ist es erforderlich, ermächtigten Bediensteten der in der vorliegenden Verordnung genannten zuständigen Behörden, Organe, Einrichtungen, Ämter und Agenturen Zugang zu bestimmten Daten aus bestimmten Interoperabilitätskomponenten ohne die Möglichkeit einer Identifizierung von Einzelpersonen zu erteilen.

(56) Damit sich die zuständigen Behörden und EU-Stellen an die neuen Anforderungen in Bezug auf die Nutzung des ESP anpassen können, ist es erforderlich, einen Übergangszeitraum vorzusehen. Ebenso sollten, um ein kohärentes und optimales Funktionieren des MID zu ermöglichen, Übergangsmaßnahmen für die Inbetriebnahme des MID vorgesehen werden.

(57) Die im laufenden Mehrjährigen Finanzrahmen veranschlagten Kosten für die Entwicklung der Interoperabilitätskomponenten sind geringer als die Mittel, die nach der Verordnung (EU) Nr. 515/2014 des Europäischen Parlaments und des Rates[57] für intelligente Grenzen vorgesehen sind. Nach Erlass der vorliegenden Verordnung sollte daher der derzeit für die Entwicklung von IT-Systemen zur Unterstützung der Steuerung von Migrationsströmen über die Außengrenzen zugewiesene Betrag gemäß Artikel 5 Absatz 5 Buchstabe b der Verordnung (EU) Nr. 515/2014 neu zugewiesen werden.

(58) Um bestimmte technische Einzelaspekte dieser Verordnung zu ergänzen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union Rechtsakte über die Profile der Nutzer des ESP sowie über Form und Inhalt der vom ESP ausgegebenen Antworten zu erlassen. Besonders wichtig ist, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen – auch auf Sachverständigenebene — durchführt und dass diese Konsultationen mit den Grundsätzen im Einklang stehen, die in der Interinstitutionellen Vereinbarung über bessere Rechtsetzung vom 13. April 2016[58] niedergelegt wurden. Um für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, sollten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten erhalten, und ihre Sachverständigen sollten systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission haben, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(59) Um einheitliche Bedingungen für die Durchführung dieser Verordnung zu gewährleisten, sollten der Kommission Durchführungsbefugnisse zum Erlass detaillierter Bestimmungen über folgende Aspekte übertragen werden: Mechanismen und Verfahren für die automatische Datenqualitätskontrolle sowie gemeinsame Datenqualitätsindikatoren, Entwicklung des UMF-Standards, Verfahren zur Ermittlung ähnlicher Identitäten, Betrieb des CRRS und Zusammenarbeit bei Sicherheitsvorfällen. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates[59] ausgeübt werden.

---

[57] Verordnung (EU) Nr. 515/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 zur Schaffung eines Instruments für die finanzielle Unterstützung für Außengrenzen und Visa im Rahmen des Fonds für die innere Sicherheit und zur Aufhebung der Entscheidung Nr. 574/2007/EG (ABl. L 150 vom 20.5.2014, S. 143).

[58] http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016Q0512(01)&from=DE

[59] Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

(60) Die Verordnung (EU) 2016/794 sollte für die für die Zwecke dieser Verordnung erfolgende Verarbeitung personenbezogener Daten durch Europol gelten.

(61) Diese Verordnung gilt unbeschadet der Anwendung der Richtlinie 2004/38/EG.

(62) Auf der Grundlage des Artikels 3 des Abkommens zwischen der Europäischen Gemeinschaft und dem Königreich Dänemark über die Kriterien und Verfahren zur Bestimmung des Staates, der für die Prüfung eines in Dänemark oder in einem anderen Mitgliedstaat der Europäischen Union gestellten Asylantrags zuständig ist, sowie über „Eurodac“ für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens[60], muss Dänemark der Kommission mitteilen, ob es den Inhalt dieser Verordnung umsetzen wird, soweit sie sich auf Eurodac [und das automatisierte System für die Erfassung und Überwachung von Anträgen und den Zuweisungsmechanismus für Anträge auf internationalen Schutz, auf das in Artikel 44 der Verordnung (EU) XX/XX zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist (Neufassung), verwiesen wird] bezieht.

(63) Im Einklang mit Artikel 5 Absatz 1 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls (Nr. 19) über den in den Rahmen der Europäischen Union einbezogenen Schengen-Besitzstand (im Folgenden „Protokoll über den Schengen-Besitzstand“) sowie Artikel 8 Absatz 2 des Beschlusses 2000/365/EG des Rates vom 29. Mai 2000 zum Antrag des Vereinigten Königreichs Großbritannien und Nordirland, einzelne Bestimmungen des Schengen-Besitzstands auf sie anzuwenden[61], beteiligt sich das Vereinigte Königreich an dieser Verordnung, soweit sich ihre Bestimmungen auf das durch den Beschluss 2007/533/JI eingerichtete SIS beziehen. Soweit sich ihre Bestimmungen auf Eurodac [und das automatisierte System für die Erfassung und Überwachung von Anträgen und den Zuweisungsmechanismus für Anträge auf internationalen Schutz nach Artikel 44 der Verordnung (EU) XX/XX zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist (Neufassung)] beziehen, kann das Vereinigte Königreich dem Präsidenten des Rates mitteilen, dass es sich gemäß Artikel 3 des dem EUV und dem AEUV beigefügten Protokolls (Nr. 21) über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts (im Folgenden „Protokoll über die Position des Vereinigten Königreichs und Irlands“) an der Annahme und Anwendung dieser Verordnung beteiligen möchte. Soweit sich ihre Bestimmungen auf das [ECRIS-TCN] beziehen, beteiligt sich das Vereinigte Königreich nach den Artikeln 1 und 2 und Artikel 4a Absatz 1 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls (Nr. 21) über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts nicht an der Annahme dieser Verordnung, die daher für das Vereinigte Königreich weder bindend noch ihm gegenüber anwendbar ist. Im Einklang mit Artikel 3 und Artikel 4a Absatz 1 des Protokolls Nr. 21 kann das Vereinigte Königreich mitteilen, dass es sich an der Annahme dieser Verordnung beteiligen möchte.

60

61

(64) Im Einklang mit Artikel 5 Absatz 1 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls (Nr. 19) über den in den Rahmen der Europäischen Union einbezogenen Schengen-Besitzstand (im Folgenden „Protokoll über den Schengen-Besitzstand“) sowie Artikel 6 Absatz 2 des Beschlusses 2002/192/EG des Rates vom 28. Februar 2002 zum Antrag Irlands, einzelne Bestimmungen des Schengen-Besitzstands auf es anzuwenden[62], beteiligt sich Irland an dieser Verordnung, soweit sich ihre Bestimmungen auf das durch den Beschluss 2007/533/JI eingerichtete SIS beziehen. Soweit sich ihre Bestimmungen auf Eurodac [und das automatisierte System für die Erfassung und Überwachung von Anträgen und den Zuweisungsmechanismus für Anträge auf internationalen Schutz nach Artikel 44 der Verordnung (EU) XX/XX zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist (Neufassung)] beziehen, kann Irland dem Präsidenten des Rates mitteilen, dass es sich gemäß Artikel 3 des dem EUV und dem AEUV beigefügten Protokolls (Nr. 21) über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts (im Folgenden „Protokoll über die Position des Vereinigten Königreichs und Irlands“) an der Annahme und Anwendung dieser Verordnung beteiligen möchte. Soweit sich ihre Bestimmungen auf das [ECRIS-TCN] beziehen, beteiligt sich Irland nach den Artikeln 1 und 2 und Artikel 4a Absatz 1 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls (Nr. 21) über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts nicht an der Annahme dieser Verordnung, die daher für Irland weder bindend noch ihm gegenüber anwendbar ist. Im Einklang mit Artikel 3 und Artikel 4a Absatz 1 des Protokolls Nr. 21 kann Irland mitteilen, dass es sich an der Annahme dieser Verordnung beteiligen möchte.

(65) Soweit sich ihre Bestimmungen auf Eurodac [und das automatisierte System für die Erfassung und Überwachung von Anträgen und den Zuweisungsmechanismus für Anträge auf internationalen Schutz nach Artikel 44 der Verordnung (EU) XX/XX zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist (Neufassung)] beziehen, stellt diese Verordnung für Island und Norwegen eine neue Maßnahme im Sinne des Übereinkommens zwischen der Europäischen Gemeinschaft und der Republik Island und dem Königreich Norwegen über die Kriterien und Regelungen zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in Island oder Norwegen gestellten Asylantrags dar.

(66) Soweit sich ihre Bestimmungen auf Eurodac [und das automatisierte System für die Erfassung und Überwachung von Anträgen und den Zuweisungsmechanismus für Anträge auf internationalen Schutz nach Artikel 44 der Verordnung (EU) XX/XX zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist (Neufassung)] beziehen, stellt diese Verordnung für die Schweiz eine neue Maßnahme im Sinne des Abkommens zwischen der Europäischen Gemeinschaft und der Schweizerischen

62

Eidgenossenschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags dar.

(67) Soweit sich ihre Bestimmungen auf Eurodac [und das automatisierte System für die Erfassung und Überwachung von Anträgen und den Zuweisungsmechanismus für Anträge auf internationalen Schutz nach Artikel 44 der Verordnung (EU) XX/XX zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist (Neufassung)] beziehen, stellt diese Verordnung für Liechtenstein eine neue Maßnahme im Sinne des Protokolls zwischen der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zum Abkommen zwischen der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags dar.

(68) Diese Verordnung steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden, und sollte unter Wahrung dieser Rechte und Grundsätze angewandt werden —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I
Allgemeine Bestimmungen

Artikel 1
Gegenstand

(1) Durch diese Verordnung [und durch die analog für die Bereiche Grenzen und Visa geltende Verordnung 2018/xx] wird ein Rahmen für die Sicherstellung der Interoperabilität zwischen dem Einreise-/Ausreisesystem (EES), dem Visa-Informationssystem (VIS), [dem Europäischen Reiseinformations- und -genehmigungssystem (ETIAS)], Eurodac, dem Schengener Informationssystem (SIS) und [dem Europäischen Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN)] geschaffen, damit diese Systeme und die darin erfassten Daten einander ergänzen.

(2) Dieser Rahmen umfasst folgende Interoperabilitätskomponenten:

a) Europäisches Suchportal – ESP (European search portal),

b) gemeinsamer Dienst für den Abgleich biometrischer Daten – gemeinsamer BMS (biometric matching service),

c) gemeinsamer Speicher für Identitätsdaten – CIR (common identity repository),

d) Detektor für Mehrfachidentitäten – MID (multiple-identity detector).

(3) Zudem werden in dieser Verordnung Bestimmungen über die Datenqualitätsanforderungen, ein universelles Nachrichtenformat (Universal

Message Format – UMF), einen zentralen Speicher für Berichte und Statistiken (central repository for reporting and statistics – CRRS) sowie die Verantwortlichkeiten der Mitgliedstaaten und der Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (eu-LISA) in Bezug auf die Konzipierung und den Betrieb der Interoperabilitätskomponenten festgelegt.

(4) Diese Verordnung regelt ferner die Verfahren und Bedingungen für den Zugang der Strafverfolgungsbehörden der Mitgliedstaaten und der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) zum EES, zum VIS, [zum ETIAS] und zu Eurodac zum Zwecke der Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten, die in ihre Zuständigkeit fallen.

Artikel 2
Ziele der Interoperabilität

(1) Durch die mittels dieser Verordnung sichergestellte Interoperabilität sollen folgende Ziele erreicht werden:

a) Verbesserung des Außengrenzenmanagements,

b) Beitrag zur Verhütung und Bekämpfung irregulärer Migration,

c) Gewährleistung eines hohen Maßes an Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts der Union einschließlich der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie des Schutzes der inneren Sicherheit im Hoheitsgebiet der Mitgliedstaaten,

d) verbesserte Umsetzung der gemeinsamen Visumpolitik und

e) Unterstützung bei der Prüfung von Anträgen auf internationalen Schutz.

(2) Diese Ziele sollen durch folgende Maßnahmen erreicht werden:

a) Sicherstellung der korrekten Identifizierung von Personen,

b) Beitrag zur Bekämpfung von Identitätsbetrug,

c) Verbesserung und Harmonisierung der Datenqualitätsanforderungen der einzelnen Informationssysteme der EU,

d) Erleichterung der technischen und der operativen Umsetzung bestehender und künftiger Informationssysteme der EU durch die Mitgliedstaaten,

e) Verschärfung, Vereinfachung und Vereinheitlichung der für die einzelnen Informationssysteme der EU geltenden Bedingungen für die Sicherheit und den Schutz der Daten,

f) Vereinheitlichung der Bedingungen für den Zugang von Strafverfolgungsbehörden zum EES, zum VIS, [zum ETIAS] und zu Eurodac sowie

g) Unterstützung der Zwecke des EES, des VIS, [des ETIAS], von Eurodac, des SIS [und des ECRIS-TCN].

Artikel 3
Anwendungsbereich

(1) Diese Verordnung gilt für Eurodac, das Schengener Informationssystem (SIS) und [das Europäische Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN)].

(2) Diese Verordnung gilt zudem in dem Maße für Europol-Daten, wie es erforderlich ist, diese gleichzeitig zu den in Absatz 1 genannten Informationssystemen der EU in Übereinstimmung mit dem EU-Recht abzufragen.

(3) Diese Verordnung gilt für Personen, deren personenbezogene Daten in den in Absatz 1 genannten Informationssystemen der EU und in den in Absatz 2 genannten Europol-Daten verarbeitet werden können.

Artikel 4
Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Außengrenzen“ die Außengrenzen im Sinne des Artikels 2 Absatz 2 der Verordnung (EU) 2016/399;
2. „Grenzübertrittskontrollen“ die Grenzübertrittskontrollen im Sinne des Artikels 2 Absatz 11 der Verordnung (EU) 2016/399;
3. „Grenzschutzbehörde“ die Grenzschutzbeamten, die nach nationalem Recht angewiesen sind, Grenzübertrittskontrollen durchzuführen;
4. „Aufsichtsbehörden“ die Aufsichtsbehörde im Sinne des Artikels 51 Absatz 1 der Verordnung (EU) 2016/679 und die Aufsichtsbehörde im Sinne des Artikels 41 Absatz 1 der Richtlinie (EU) 2016/680;
5. „Verifizierung“ den Abgleich von Datensätzen zur Überprüfung einer Identitätsangabe (1:1-Abgleich);
6. „Identifizierung“ die Feststellung der Identität einer Person durch den Abgleich mit vielen Datensätzen in der Datenbank (1:n-Abgleich);
7. „Drittstaatsangehöriger“ eine Person, die kein Unionsbürger im Sinne des Artikels 20 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union ist, oder einen Staatenlosen oder eine Person, deren Staatsangehörigkeit unbekannt ist;
8. „alphanumerische Daten“ Daten in Form von Buchstaben, Ziffern, Sonderzeichen, Leerzeichen und Satzzeichen;
9. „Identitätsdaten“ die in Artikel 27 Absatz 3 Buchstaben a bis h genannten Daten;
10. „Fingerabdruckdaten“ die Daten zu den Fingerabdrücken einer Person;
11. „Gesichtsbild“ eine digitale Aufnahme des Gesichts;
12. „biometrische Daten“ Fingerabdruckdaten und/oder das Gesichtsbild;
13. „biometrisches Template“ eine mathematische Repräsentation, die mittels Merkmalsauszug aus biometrischen Daten generiert wird, welche auf die für Identifizierungs- und Verifizierungszwecke erforderlichen Merkmale begrenzt sind;

14. „Reisedokument“ einen Reisepass oder ein anderes gleichwertiges Dokument, das seinen Inhaber zum Überschreiten der Außengrenzen berechtigt und in dem ein Visum angebracht werden kann;

15. „Reisedokumentendaten“ die Art, die Nummer und das Ausstellungsland des Reisedokuments, das Datum des Ablaufs der Gültigkeitsdauer des Reisedokuments und den aus drei Buchstaben bestehenden Code des Landes, das das Reisedokument ausgestellt hat;

16. „Reisegenehmigung“ die Reisegenehmigung im Sinne des Artikels 3 der [ETIAS-Verordnung];

17. „Visum für einen kurzfristigen Aufenthalt“ das Visum im Sinne des Artikels 2 Absatz 2 Buchstabe a der Verordnung (EG) Nr. 810/2009;

18. „Informationssysteme der EU“ die von eu-LISA verwalteten IT-Großsysteme;

19. „Europol-Daten“ die personenbezogenen Daten, die zu dem in Artikel 18 Absatz 2 Buchstabe a der Verordnung (EU) 2016/794 genannten Zweck an Europol übermittelt werden;

20. „Interpol-Datenbanken“ die Interpol-Datenbank für gestohlene und verlorene Reisedokumente (SLTD) und die Interpol-Datenbank zur Erfassung von Ausschreibungen zugeordneten Reisedokumenten (TDAWN);

21. „Übereinstimmung“ eine Übereinstimmung, die anhand eines Abgleichs von zwei oder mehr zuvor oder zeitgleich in einem Informationssystem oder in einer Datenbank erfassten personenbezogenen Daten festgestellt wird;

22. „Treffer“ eine oder mehrere bestätigte Übereinstimmungen;

23. „Polizeibehörde“ eine zuständige Behörde im Sinne des Artikels 3 Absatz 7 der Richtlinie (EU) 2016/680;

24. „benannte Behörden“ die benannten Behörden der Mitgliedstaaten gemäß Artikel 29 Absatz 1 der Verordnung (EU) 2017/2226, Artikel 3 Absatz 1 des Beschlusses 2008/633/JI des Rates, [Artikel 43 der ETIAS-Verordnung] und [Artikel 6 der Eurodac-Verordnung];

25. „terroristische Straftat“ eine Straftat nach nationalem Recht, die einer der in der Richtlinie (EU) 2017/541 aufgeführten Straftaten entspricht oder dieser gleichwertig ist;

26. „schwere Straftat“ eine Straftat, die einer der in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI aufgeführten Straftaten entspricht oder dieser gleichwertig ist, wenn die Straftat nach dem nationalen Recht mit einer freiheitsentziehenden Strafe oder Sicherungsmaßnahme für eine Höchstdauer von mindestens drei Jahren geahndet werden kann;

27. „EES“ das Einreise-/Ausreisesystem gemäß der Verordnung (EU) 2017/2226;

28. „VIS“ das Visa-Informationssystem gemäß der Verordnung (EG) Nr. 767/2008;

29. [„ETIAS“ das Europäische Reiseinformations- und -genehmigungssystem gemäß der ETIAS-Verordnung];

30. „Eurodac“ das Eurodac-System gemäß der [Eurodac-Verordnung];

31. „SIS“ das Schengener Informationssystem gemäß den [Verordnungen über das SIS im Bereich der Grenzkontrollen, über das SIS im Bereich der Strafverfolgung und über das SIS im Bereich der Rückkehr illegal aufhältiger Drittstaatsangehöriger];

32. [„ECRIS-TCN“ das durch die ECRIS-TCN-Verordnung eingerichtete Europäische Strafregisterinformationssystem für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen vorliegen];

33. „ESP“ das Europäische Suchportal gemäß Artikel 6;

34. „gemeinsamer BMS“ den gemeinsamen Dienst für den Abgleich biometrischer Daten gemäß Artikel 15;

35. „CIR“ den gemeinsamen Speicher für Identitätsdaten gemäß Artikel 17;

36. „MID“ den Detektor für Mehrfachidentitäten gemäß Artikel 25;

37. „CRRS“ den zentralen Speicher für Berichte und Statistiken gemäß Artikel 39.

Artikel 5
Nichtdiskriminierung

Bei der Verarbeitung personenbezogener Daten für die Zwecke dieser Verordnung dürfen keine Personen aufgrund des Geschlechts, der Rasse oder der ethnischen Herkunft, der Religion oder der Weltanschauung, einer Behinderung, des Alters oder der sexuellen Ausrichtung diskriminiert werden. Die Menschenwürde und die Integrität der Betroffenen müssen uneingeschränkt gewahrt werden. Besonderer Aufmerksamkeit bedürfen Kinder, ältere Menschen und Menschen mit Behinderungen.

KAPITEL II
Europäisches Suchportal

Artikel 6
Europäisches Suchportal

(1) Es wird ein Europäisches Suchportal (European Search Portal - ESP) geschaffen, das den Behörden der Mitgliedstaaten und den EU-Stellen einen raschen, unterbrechungsfreien, effizienten, systematischen und kontrollierten Zugang zu den Informationssystemen der EU, den Europol-Daten und den Datenbanken von Interpol nach Maßgabe ihrer Zugangsrechte erleichtern soll, den sie benötigen, um ihren Aufgaben nachzukommen, und die Ziele des EES, des VIS, [des ETIAS], von Eurodac, des SIS, [des ECRIS-TCN] und der Europol-Daten zu unterstützen.

(2) Das ESP umfasst

a) eine zentrale Infrastruktur einschließlich eines Suchportals, das die gleichzeitige Abfrage des EES, des VIS, [des ETIAS], von Eurodac, des SIS, [des ECRIS-TCN], der Europol-Daten und der Interpol-Datenbanken ermöglicht;

b) einen sicheren Kommunikationskanal zwischen dem ESP und denjenigen Mitgliedstaaten und EU-Stellen, die nach dem Unionsrecht berechtigt sind, das ESP zu nutzen;

c) eine sichere Kommunikationsinfrastruktur zwischen dem ESP und dem EES, dem VIS, [dem ETIAS], Eurodac, dem zentralen SIS, [dem ECRIS-TCN], den Europol-Daten und den Interpol-Datenbanken sowie zwischen dem ESP und den zentralen Infrastrukturen des gemeinsamen Speichers für Identitätsdaten (CIR) und des Detektors für Mehrfachidentitäten (MID).

(3) Die Agentur eu-LISA entwickelt das ESP und sorgt für seine technische Verwaltung.

Artikel 7
Nutzung des Europäischen Suchportals

(1) Die Nutzung des ESP ist Behörden der Mitgliedstaaten und EU-Stellen vorbehalten, die nach Maßgabe der einschlägigen Bestimmungen des Unionsrechts beziehungsweise des nationalen Rechts auf das EES, [das ETIAS], das VIS, das SIS, Eurodac, [das ECRIS-TCN], den CIR, den MID, die Europol-Daten und die Interpol-Datenbanken zugreifen können.

(2) Die in Absatz 1 genannten Behörden können das ESP für die Abfrage von Daten zu Personen oder deren Reisedokumenten in den Zentralsystemen von Eurodac [und des ECRIS-TCN] nach Maßgabe ihrer jeweiligen Zugangsrechte nach dem Unionsrecht beziehungsweise nach nationalem Recht nutzen. Sie können das ESP zudem nach Maßgabe ihrer in dieser Verordnung festgelegten Zugangsrechte für die Abfrage des CIR für die in den Artikeln 20, 21 und 22 genannten Zwecke nutzen.

(3) Die in Absatz 1 genannten Behörden der Mitgliedstaaten können das ESP für die Abfrage von Daten zu Personen oder deren Reisedokumenten im [in den Verordnungen über das SIS im Bereich der Grenzkontrollen beziehungsweise im Bereich der Strafverfolgung genannten] zentralen SIS nutzen. Der Zugriff auf das zentrale SIS über das ESP erfolgt im Wege der nationalen Systeme (N.SIS) der einzelnen Mitgliedstaaten gemäß [Artikel 4 Absatz 2 der Verordnungen über das SIS im Bereich der Grenzkontrollen beziehungsweise im Bereich der Strafverfolgung].

(4) Zugangsberechtigte EU-Stellen können das ESP für die Abfrage von Daten zu Personen oder deren Reisedokumenten im zentralen SIS nutzen.

(5) Die in Absatz 1 genannten Behörden können das ESP für die Abfrage von Daten zu Personen oder deren Reisedokumenten in den Europol-Daten nach Maßgabe ihrer jeweiligen Zugangsrechte nach dem Unionsrecht beziehungsweise nach nationalem Recht nutzen.

Artikel 8
Erstellung von ESP-Nutzerprofilen

(1) Um die Nutzung des ESP zu ermöglichen, erstellt eu-LISA für jede Kategorie von ESP-Nutzern ein Profil, das den in Absatz 2 genannten technischen Details und Zugangsrechten Rechnung trägt, und legt dabei nach Maßgabe des Unionsrechts und des nationalen Rechts folgende Einzelheiten fest:

a) die für die Datenabfrage zu verwendenden Suchfelder,

b) die Informationssysteme der EU, die Europol-Daten und die Interpol-Datenbanken, die für die Datenabfrage herangezogen werden dürfen beziehungsweise müssen und zu denen dem Nutzer ein Abfrageergebnis ausgegeben werden muss, und

c) die Art der als Abfrageergebnis auszugebenden Daten.

(2) Die Kommission erlässt gemäß Artikel 63 delegierte Rechtsakte zur Festlegung der technischen Details der in Absatz 1 genannten Profile der in Artikel 7 Absatz 1 genannten Nutzer des ESP nach Maßgabe ihrer jeweiligen Zugangsrechte.

Artikel 9
Abfragen

(1) Die Nutzer des ESP können, um Abfragen vorzunehmen, in Übereinstimmung mit ihrem Nutzerprofil und ihren Zugangsrechten Daten in das ESP eingeben. Bei einer Abfrage fragt das ESP anhand der vom Nutzer des ESP eingegebenen Daten gleichzeitig das EES, [das ETIAS], das VIS, das SIS, Eurodac, [das ECRIS-TCN], den CIR, die Europol-Daten und die Interpol-Datenbanken ab.

(2) Die Suchfelder für die Datenabfrage über das ESP entsprechen den Suchfeldern für Personen oder Reisedokumente, die für die Abfrage der verschiedenen Informationssysteme der EU, der Europol-Daten und der Interpol-Datenbanken nach Maßgabe der einschlägigen Rechtsvorschriften verwendet werden können.

(3) Die Agentur eu-LISA erstellt für das ESP eine Dokumentation zur Schnittstellenansteuerung in dem in Artikel 38 genannten universellen Nachrichtenformat (UMF).

(4) Die der über das ESP erfolgten Abfrage entsprechenden Daten werden aus dem EES, [aus dem ETIAS], aus dem VIS, aus dem SIS, aus Eurodac, [aus dem ECRIS-TCN], aus dem CIR, aus dem MID sowie aus den Europol-Daten beziehungsausweise aus den Interpol-Datenbanken bereitgestellt.

(5) Das ESP wird so konzipiert, dass bei der Abfrage der Interpol-Datenbanken sichergestellt ist, dass die vom Nutzer des ESP für die Abfrage eingegebenen Daten nicht mit den Eigentümern der Interpol-Daten geteilt werden.

(6) Die dem ESP-Nutzer erteilte Antwort muss eindeutig sein und sämtliche Daten enthalten, auf die der Nutzer nach dem Unionsrecht zugreifen darf. Erforderlichenfalls wird in der vom ESP erteilten Antwort angegeben, aus welchem Informationssystem beziehungsweise aus welcher Datenbank die betreffenden Daten stammen.

(7) Die Kommission erlässt einen delegierten Rechtsakt nach Artikel 63, um den Inhalt und das Format der vom ESP erteilten Antworten festzulegen.

Artikel 10
Führen von Protokollen

(1) Unbeschadet des [Artikels 39 der Eurodac-Verordnung], der [Artikel 12 und 18 der Verordnung über das SIS im Bereich der Strafverfolgung], des [Artikels 29 der ECRIS-TCN-Verordnung] und des Artikels 40 der Verordnung (EU) 2016/794 führt die Agentur eu-LISA Protokolle sämtlicher im ESP erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten insbesondere folgende Angaben:

a) mitgliedstaatliche Behörde und betreffender ESP-Nutzer einschließlich ESP-Nutzerprofil nach Artikel 8,

b) Datum und Uhrzeit der Abfrage,

c) abgefragte Informationssysteme der EU und Europol-Daten,

d) Kennung der Person, die die Abfrage vorgenommen hat (nach Maßgabe der nationalen Rechtsvorschriften beziehungsweise der Verordnung (EU) 2016/794 oder, falls anwendbar, der Verordnung (EU) 45/2001).

(2) Die Protokolle dürfen nur zur datenschutzrechtlichen Kontrolle einschließlich der Prüfung der Zulässigkeit einer Anfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit gemäß Artikel 42 verwendet werden. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und ein Jahr nach ihrer Erstellung gelöscht, sofern sie nicht für ein bereits eingeleitetes Kontrollverfahren benötigt werden.

Artikel 11

Ausweichverfahren für den Fall, dass eine Nutzung des ESP technisch nicht möglich ist

(1) Wenn es wegen eines Ausfalls des ESP technisch nicht möglich ist, das ESP für die Abfrage eines oder mehrerer der in Artikel 9 Absatz 1 genannten Informationssysteme oder des CIR zu nutzen, werden die Nutzer des ESP von eu-LISA entsprechend benachrichtigt.

(2) Wenn es wegen eines Ausfalls der nationalen Infrastruktur eines Mitgliedstaats technisch nicht möglich ist, das ESP für die Abfrage eines oder mehrerer der in Artikel 9 Absatz 1 genannten Informationssysteme oder des CIR zu nutzen, benachrichtigt die zuständige Behörde des betroffenen Mitgliedstaats die Agentur eu-LISA und die Kommission.

(3) In beiden Fällen gilt die in Artikel 7 Absätze 2 und 4 festgelegte Pflicht nicht, bis das technische Versagen behoben ist, und die Mitgliedstaaten können die in Artikel 9 Absatz 1 genannten Informationssysteme oder das CIR auf direktem Wege über ihre jeweiligen einheitlichen nationalen Schnittstellen oder über ihre nationalen Kommunikationsinfrastrukturen abfragen.

KAPITEL III
Gemeinsamer Dienst für den Abgleich biometrischer Daten

Artikel 12

Gemeinsamer Dienst für den Abgleich biometrischer Daten

(1) Es wird ein gemeinsamer Dienst für den Abgleich biometrischer Daten (shared biometric matching service - gemeinsamer BMS) eingerichtet, der die Aufgabe hat, biometrische Merkmalsdaten (Templates) zu speichern und die systemübergreifende Abfrage mehrerer Informationssysteme der EU anhand biometrischer Daten zu ermöglichen, um den gemeinsamen Speicher für Identitätsdaten (CIR) und den Detektor für Mehrfachidentitäten (MID) sowie die Ziele des EES, des VIS, von Eurodac, des SIS und [des ECRIS-TCN] zu unterstützen.

(2) Der gemeinsame BMS umfasst

a) eine zentrale Infrastruktur einschließlich einer Suchmaschine und eines Speichers für die in Artikel 13 genannten Daten,

b) eine sichere Kommunikationsinfrastruktur zwischen dem gemeinsamen BMS, dem zentralen SIS und dem CIR.

(3) Die Agentur eu-LISA entwickelt den gemeinsamen BMS und sorgt für seine technische Verwaltung.

Artikel 13

Vom gemeinsamen Dienst für den Abgleich biometrischer Daten gespeicherte Daten

(1) Der gemeinsame BMS speichert die biometrischen Templates, die er aus folgenden biometrischen Daten generiert:

a) Daten nach Artikel 16 Absatz 1 Buchstabe d und Artikel 17 Absatz 1 Buchstaben b und c der Verordnung (EU) Nr. 2017/2226,

b) Daten nach Artikel 9 Absatz 6 der Verordnung (EG) Nr. 767/2008,

c) [Daten nach Artikel 20 Absatz 2 Buchstaben w und x der Verordnung über das SIS im Bereich der Grenzkontrollen,

d) Daten nach Artikel 20 Absatz 3 Buchstaben w und x der Verordnung über das SIS im Bereich der Strafverfolgung,

e) Daten nach Artikel 4 Absatz 3 Buchstaben t und u der Verordnung über das SIS im Bereich der Rückkehr illegal aufhältiger Drittstaatsangehöriger],

f) [Daten nach Artikel 13 Buchstabe a der Eurodac-Verordnung],

g) [Daten nach Artikel 5 Absatz 1 Buchstabe b und Artikel 5 Absatz 2 der ECRIS-TCN-Verordnung].

(2) Der gemeinsame BMS fügt jedem biometrischen Template einen Verweis auf die Informationssysteme, in dem die betreffenden biometrischen Daten gespeichert sind, hinzu.

(3) Die biometrischen Templates dürfen erst in den gemeinsamen BMS eingegeben werden, nachdem der gemeinsame BMS die einem der Informationssysteme hinzugefügten biometrischen Daten einer automatischen Qualitätskontrolle unterzogen hat, um sicherzustellen, dass ein Mindestdatenqualitätsstandard eingehalten wird.

(4) Bei der Speicherung der in Absatz 1 genannten Daten sind die in Artikel 37 Absatz 2 genannten Qualitätsstandards einzuhalten.

Artikel 14

Abfrage biometrischer Daten mithilfe des gemeinsamen Dienstes für den Abgleich biometrischer Daten

Die Abfrage von im CIR und im SIS gespeicherten Daten durch den CIR und das SIS wird anhand der im gemeinsamen BMS gespeicherten biometrischen Templates durchgeführt. Die Abfragen anhand biometrischer Daten dürfen ausschließlich zu den Zwecken vorgenommen werden, die in dieser Verordnung sowie in der EES-Verordnung, der VIS-Verordnung, der Eurodac-Verordnung, [der SIS-Verordnung] und [der ECRIS-TCN-Verordnung] vorgesehen sind.

Artikel 15
Datenspeicherung im gemeinsamen Dienst für den Abgleich biometrischer Daten

Die in Artikel 13 genannten Daten werden im gemeinsamen BMS nur so lange gespeichert, wie die entsprechenden biometrischen Daten im CIR beziehungsweise im SIS gespeichert werden.

Artikel 16
Führen von Protokollen

(1) Unbeschadet des [Artikels 39 der Eurodac-Verordnung], der [Artikel 12 und 18 der Verordnung über das SIS im Bereich der Strafverfolgung] und des [Artikels 29 der ECRIS-TCN-Verordnung] führt die Agentur eu-LISA Protokolle sämtlicher im gemeinsamen BMS erfolgenden Datenverarbeitungsvorgänge. Diese Protokolle umfassen insbesondere folgende Angaben:

a) Chronik der Erstellung und der Speicherung biometrischer Templates,

b) Informationssysteme der EU, die mit den im gemeinsamen BMS gespeicherten biometrischen Templates abgefragt wurden,

c) Datum und Uhrzeit der Abfrage,

d) Art der für die Abfrage verwendeten biometrischen Daten,

e) Dauer der Abfrage,

f) Abfrageergebnisse sowie Datum und Uhrzeit der Ergebnisanzeige,

g) Kennung der Person, die die Abfrage vorgenommen hat (nach Maßgabe der nationalen Rechtsvorschriften beziehungsweise der Verordnung (EU) 2016/794 oder, falls anwendbar, der Verordnung (EU) 45/2001).

(2) Die Protokolle dürfen nur zur datenschutzrechtlichen Kontrolle einschließlich der Prüfung der Zulässigkeit einer Anfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit gemäß Artikel 42 verwendet werden. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und ein Jahr nach ihrer Erstellung gelöscht, sofern sie nicht für ein bereits eingeleitetes Kontrollverfahren benötigt werden. Die in Absatz 1 Buchstabe a genannten Protokolle werden gelöscht, sobald die betreffenden Daten gelöscht werden.

KAPITEL IV
Gemeinsamer Speicher für Identitätsdaten

Artikel 17
Gemeinsamer Speicher für Identitätsdaten

(1) Es wird ein gemeinsamer Speicher für Identitätsdaten (common identity repository - CIR) geschaffen, in dem für jede im EES, im VIS, [im ETIAS], in Eurodac oder [im ECRIS-TCN] erfasste Person eine individuelle Datei mit den in Artikel 18 genannten Daten angelegt wird und der dazu dient, die korrekte Identifizierung von im EES, im VIS, [im ETIAS], in Eurodac und [im ECRIS-TCN] erfassten Personen zu erleichtern und zu unterstützen, das Funktionieren des Detektors für

Mehrfachidentitäten (MID) zu unterstützen und den etwaig erforderlichen Zugang von Strafverfolgungsbehörden zu den Informationssystemen anderer Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung terroristischer und anderer schwerer Straftaten zu erleichtern und einheitlich zu regeln.

(2) Der CIR umfasst

a) eine zentrale Infrastruktur, die die einzelnen Zentralsysteme des EES, des VIS, [des ETIAS], von Eurodac und [des ECRIS-TCN] insoweit ersetzt, als in ihr die in Artikel 18 genannten Daten gespeichert werden,

b) einen sicheren Kommunikationskanal zwischen dem CIR und den Mitgliedstaaten und EU-Stellen, die nach dem Unionsrecht berechtigt sind, das Europäische Suchportal (ESP) zu nutzen,

c) eine sichere Kommunikationsinfrastruktur zwischen dem CIR und dem EES, [dem ETIAS], dem VIS, Eurodac und [dem ECRIS-TCN] sowie den zentralen Infrastrukturen des ESP, des gemeinsamen Dienstes für den Abgleich biometrischer Daten (BMS) und des MID.

(3) Die Agentur eu-LISA entwickelt den CIR und sorgt für seine technische Verwaltung.

Artikel 18

Im gemeinsamen Speicher für Identitätsdaten gespeicherte Daten

(1) Im CIR werden folgende Daten logisch von einander getrennt nach den Informationssystemen, aus denen sie stammen, gespeichert:

a) – (entfällt);

b) – (entfällt);

c) – (entfällt);

d) [Daten nach Artikel 13 Buchstaben a bis e, g und h der Eurodac-Verordnung],

e) [Daten nach Artikel 5 Absatz 1 Buchstabe b und Artikel 5 Absatz 2 der ECRIS-TCN-Verordnung sowie folgende Daten nach Artikel 5 Absatz 1 Buchstabe a der ECRIS-TCN-Verordnung: Nachname oder Familienname, Vorname(n), Geschlecht, Geburtsdatum, Geburtsort und -land, Staatsangehörigkeit(en), Gender sowie gegebenenfalls frühere Namen, Pseudonym(e) und/oder Aliasname(n)].

(2) Für jeden Satz der in Absatz 1 genannten Daten wird im CIR vermerkt, aus welchen Informationssystemen die betreffenden Daten stammen.

(3) Bei der Speicherung der in Absatz 1 genannten Daten sind die in Artikel 37 Absatz 2 genannten Qualitätsstandards einzuhalten.

Artikel 19

Hinzufügung, Änderung und Löschung von Daten im gemeinsamen Speicher für Identitätsdaten

(1) Bei jeder Hinzufügung, Änderung oder Löschung von Daten in Eurodac [oder im ECRIS-TCN] werden die in den individuellen Dateien im CIR gespeicherten Daten nach Artikel 18 automatisch entsprechend hinzugefügt, geändert oder gelöscht.

(2) Wird vom MID nach Maßgabe der Artikel 32 und 33 eine weiße oder eine rote Verknüpfung zwischen Daten von zwei oder mehr Informationssystemen der EU, die

Bestandteil des CIR sind, erstellt, werden vom CIR keine neuen individuellen Dateien angelegt, sondern die neuen Daten der individuellen Datei der verknüpften Daten hinzugefügt.

Artikel 20
Zugang zum gemeinsamen Speicher für Identitätsdaten

(1) Mitgliedstaatliche Polizeibehörden, denen mittels nationaler Legislativmaßnahmen die in Absatz 2 genannten Befugnisse übertragen wurden, dürfen ausschließlich zum Zwecke der Identifizierung einer Person anhand der bei einer Identitätskontrolle erhobenen biometrischen Daten dieser Person Abfragen im CIR vornehmen.

Falls eine solche Abfrage ergibt, dass im CIR Daten zu der betreffenden Person gespeichert sind, darf die betreffende mitgliedstaatliche Behörde die in Artikel 18 Absatz 1 genannten Daten einsehen.

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.

(2) Mitgliedstaaten, die die in diesem Artikel vorgesehene Zugangsmöglichkeit nutzen möchten, erlassen entsprechende nationale Legislativmaßnahmen. Durch derartige Legislativmaßnahmen sind die genauen Zwecke der zu den in Artikel 2 Absatz 1 Buchstaben b und c genannten Zwecken erfolgenden Identitätskontrollen festzulegen. Durch derartige Legislativmaßnahmen sind zudem die hierzu befugten Polizeibehörden zu benennen sowie die Verfahren, Bedingungen und Kriterien derartiger Kontrollen festzulegen.

Artikel 21
Zugang zum gemeinsamen Speicher für Identitätsdaten zwecks Aufdeckung etwaiger Mehrfachidentitäten

(1) Falls bei der Abfrage des CIR eine gelbe Verknüpfung gemäß Artikel 28 Absatz 4 angezeigt wird, darf die Behörde, welche für die Verifizierung unterschiedlicher, nach Artikel 29 ermittelter Identitäten zuständig ist, ausschließlich zu Verifizierungszwecken auf die im CIR gespeicherten Identitätsdaten aus den verschiedenen angeschlossenen, durch die gelbe Verknüpfung bezeichneten Informationssystemen zugreifen.

(2) Falls bei der Abfrage des CIR eine rote Verknüpfung gemäß Artikel 32 angezeigt wird, dürfen die in Artikel 26 Absatz 2 genannten Behörden ausschließlich zur Bekämpfung von Identitätsbetrug auf die im CIR gespeicherten Identitätsdaten aus den verschiedenen angeschlossenen, durch die rote Verknüpfung bezeichneten Informationssystemen zugreifen.

Artikel 22
Abfrage des gemeinsamen Speichers für Identitätsdaten zu Strafverfolgungszwecken

(1) Die benannten Behörden der Mitgliedstaaten und Europol können den CIR abfragen, um terroristische und sonstige schwere Straftaten im konkreten Einzelfall zu

verhüten, aufzudecken oder zu untersuchen oder um in Erfahrung zu bringen, ob in Eurodac Daten zu einer spezifischen Person gespeichert sind.

(2) Die benannten Behörden der Mitgliedstaaten und Europol sind, wenn sie den CIR zu den in Absatz 1 aufgeführten Zwecken zurate ziehen, nicht befugt, aus dem [ECRIS-TCN] stammende Daten abzufragen.

(3) Falls die Abfrage im CIR ergibt, dass in Eurodac Daten zu der betreffenden Person gespeichert sind, wird den benannten Behörden der Mitgliedstaaten und Europol in Übereinstimmung mit Artikel 18 Absatz 2 vom CIR angezeigt, in welchem dieser Informationssysteme die betreffenden Daten gespeichert sind. Alle vom CIR ausgegebenen Antworten müssen so beschaffen sein, dass die Sicherheit der Daten nicht gefährdet wird.

(4) Der vollständige Zugang zu den in den Informationssystemen der EU gespeicherten Daten, welche für die Zwecke der Verhütung, Aufdeckung und Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten erforderlich sind, unterliegt weiterhin den Bedingungen und Verfahren, die in den einschlägigen Rechtsvorschriften festgelegt sind.

Artikel 23
Datenspeicherung im gemeinsamen Speicher für Identitätsdaten

(1) Die in Artikel 18 Absätze 1 und 2 genannten Daten werden im CIR nach Maßgabe der Datenspeicherungsbestimmungen [der Eurodac-Verordnung] beziehungsweise [der ECRIS-TCN-Verordnung] gelöscht.

(2) Die individuellen Dateien werden im CIR so lange gespeichert, wie die entsprechenden Daten in mindestens einem der Informationssysteme gespeichert werden, aus dem die Daten stammen. Durch die Erstellung einer Verknüpfung wird die Speicherfrist der einzelnen durch die Verknüpfung bezeichneten Daten nicht berührt.

Artikel 24
Führen von Protokollen

(1) Unbeschadet des [Artikels 39 der Eurodac-Verordnung] und [des Artikels 29 der ECRIS-TCN-Verordnung] führt die Agentur eu-LISA Protokolle sämtlicher im CIR erfolgenden Datenverarbeitungsvorgänge gemäß den Absätzen 2, 3 und 4.

(2) Bezüglich eines etwaigen nach Artikel 20 erfolgenden Zugriffs auf den CIR führt eu-LISA Protokolle sämtlicher im CIR erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten insbesondere folgende Angaben:

a) Zweck des Zugriffs vonseiten des Nutzers,

b) Datum und Uhrzeit der Abfrage,

c) Art der für die Abfrage verwendeten Daten,

d) Ergebnisse der Abfrage,

e) Kennung der Person, die die Abfrage vorgenommen hat (nach Maßgabe der nationalen Rechtsvorschriften beziehungsweise der Verordnung (EU) 2016/794 oder, falls anwendbar, der Verordnung (EU) 45/2001).

(3) Bezüglich eines etwaigen nach Artikel 21 erfolgenden Zugriffs auf den CIR führt eu-LISA Protokolle sämtlicher im CIR erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten insbesondere folgende Angaben:

a) Zweck des Zugriffs vonseiten des Nutzers,

b) Datum und Uhrzeit der Abfrage,

c) Art der für die Abfrage verwendeten Daten (falls relevant),

d) Ergebnisse der Abfrage (falls relevant),

e) Kennung der Person, die die Abfrage vorgenommen hat (nach Maßgabe der nationalen Rechtsvorschriften beziehungsweise der Verordnung (EU) 2016/794 oder, falls anwendbar, der Verordnung (EU) 45/2001).

(4) Bezüglich eines etwaigen nach Artikel 22 erfolgenden Zugriffs auf den CIR führt eu-LISA Protokolle sämtlicher im CIR erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten insbesondere folgende Angaben:

a) nationales Aktenzeichen,

b) Datum und Uhrzeit der Abfrage,

c) Art der für die Abfrage verwendeten Daten,

d) Ergebnisse der Abfrage,

e) Name der Behörde, die die Daten abgefragt hat,

f) Kennung des Beamten, der die Abfrage vorgenommen hat, und des Beamten, der die Abfrage veranlasst hat (nach Maßgabe der nationalen Rechtsvorschriften beziehungsweise der Verordnung (EU) 2016/794 oder, falls anwendbar, der Verordnung (EU) 45/2001).

Die zuständige Aufsichtsbehörde nach Artikel 51 der Verordnung (EU) 2016/679 beziehungsweise nach Artikel 41 der Richtlinie (EU) 2016/680 überprüft regelmäßig, spätestens jedoch alle sechs Monate, die betreffenden Zugangsprotokolle darauf, ob die Verfahren und Bedingungen nach Artikel 22 Absätze 1 bis 3 eingehalten wurden.

(5) Jeder Mitgliedstaat führt Protokolle über die Abfragen vonseiten der zur Nutzung des CIR gemäß den Artikeln 20, 21 und 22 ermächtigten Bediensteten.

(6) Die in den Absätzen 1 und 5 genannten Protokolle dürfen ausschließlich zur datenschutzrechtlichen Kontrolle, einschließlich zur Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit gemäß Artikel 42 verwendet werden. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und ein Jahr nach ihrer Erstellung gelöscht, sofern sie nicht für ein bereits eingeleitetes Kontrollverfahren benötigt werden.

(7) Die Agentur eu-LISA führt für die in Absatz 6 genannten Zwecke Protokolle über die Chronik der in den individuellen Dateien gespeicherten Daten. Die Protokolle über die Chronik der Daten werden gelöscht, sobald die Daten gelöscht wurden.

KAPITEL V
Detektor für Mehrfachidentitäten

Artikel 25
Detektor für Mehrfachidentitäten

(1) Zur Unterstützung des Funktionierens des CIR und der Ziele des EES, des VIS, [des ETIAS], von Eurodac, des SIS und [des ECRIS-TCN] wird ein Detektor für Mehrfachidentitäten (MID) eingerichtet, der Verknüpfungen zwischen in den EU-Informationssystemen einschließlich des gemeinsamen Speichers für Identitätsdaten (CIR) und des SIS enthaltenen Daten erstellt und speichert und in der Folge Mehrfachidentitäten aufdeckt, um Identitätsprüfungen zu vereinfachen und Identitätsbetrug zu bekämpfen.

(2) Der MID umfasst

a) eine zentrale Infrastruktur, die Verknüpfungen und Angaben zu Informationssystemen speichert;

b) eine sichere Kommunikationsinfrastruktur, über die der MID mit dem SIS und den zentralen Infrastrukturen des Europäischen Suchportals und des CIR verbunden ist.

(3) eu-LISA entwickelt den MID und sorgt für seine technische Verwaltung.

Artikel 26
Zugriff auf den Detektor für Mehrfachidentitäten

(1) Für die Zwecke der manuellen Identitätsverifizierung nach Artikel 29 erhalten folgende Stellen Zugriff auf die im MID gespeicherten Daten nach Artikel 34:

a) – (entfällt);

b) – (entfällt);

c) – (entfällt);

d) die gemäß der Eurodac-Verordnung für die Prüfung eines Antrags auf internationalen Schutz zuständigen Behörden bei der Prüfung eines neuen Antrags auf internationalen Schutz;

e) die SIRENE-Büros des Mitgliedstaats, der eine [SIS-Ausschreibung gemäß den Verordnungen über das SIS im Bereich der Strafverfolgung beziehungsweise im Bereich der Rückkehr illegal aufhältiger Drittstaatsangehöriger] eingibt;

f) [die Zentralbehörden des Urteilsmitgliedstaats bei der Eingabe oder Aktualisierung von Daten im ECRIS-TCN nach Artikel 5 der ECRIS-TCN-Verordnung.]

(2) Die Behörden der Mitgliedstaaten und die EU-Stellen, die Zugang zu mindestens einem in den CIR integrierten Informationssystem der EU oder zum SIS haben, erhalten über rote Verknüpfungen nach Artikel 32 Zugang zu den in Artikel 34 Buchstaben a und b genannten Daten.

Artikel 27
Prüfung auf Mehrfachidentitäten

(1) Im gemeinsamen Speicher für Identitätsdaten und im SIS wird eine Prüfung auf Mehrfachidentitäten eingeleitet, wenn

a) – (entfällt);

b) – (entfällt);

c) – (entfällt);

d) [in Eurodac nach Artikel 10 der Eurodac-Verordnung ein Antrag auf internationalen Schutz erstellt oder aktualisiert wird;]

e) [im SIS nach den Kapiteln VI, VII, VIII und IX der Verordnung über das SIS im Bereich der Strafverfolgung und Artikel 3 der Verordnung über das SIS im Bereich der Rückkehr illegal aufhältiger Drittstaatsangehöriger eine Ausschreibung zu einer Person erstellt oder aktualisiert wird];

f) [im ECRIS-TCN nach Artikel 5 der ECRIS-TCN-Verordnung ein Datensatz angelegt oder aktualisiert wird.]

(2) Wenn die in einem Informationssystem enthaltenen Daten nach Absatz 1 biometrische Daten umfassen, nutzen der CIR und das zentrale SIS den gemeinsamen BMS für die Prüfung auf Mehrfachidentitäten. Der gemeinsame BMS vergleicht die aus neuen biometrischen Daten generierten biometrischen Templates mit den bereits im gemeinsamen BMS vorhandenen biometrischen Templates, um zu überprüfen, ob die zu demselben Drittstaatsangehörigen gehörenden Daten bereits im CIR oder im zentralen SIS gespeichert sind.

(3) Zusätzlich zu dem in Absatz 2 genannten Vorgang nutzen der CIR und das zentrale SIS das Europäische Suchportal, um anhand der folgenden Daten die im CIR und im zentralen SIS gespeicherten Daten zu durchsuchen:

a) – (entfällt);

b) – (entfällt);

c) – (entfällt);

d) [Nachname(n), Vorname(n), Geburtsname(n), frühere Namen und Aliasnamen, Geburtsdatum, Geburtsort, Staatsangehörigkeit(en) und Geschlecht gemäß Artikel 12 der Eurodac-Verordnung];

e) – (entfällt);

f) [Nachname(n), Vorname(n), Geburtsname(n), frühere Namen und Aliasnamen, Geburtsdatum, Geburtsort, Geschlecht und Staatsangehörigkeit(en) gemäß Artikel 20 Absatz 3 der Verordnung über das SIS im Bereich der Strafverfolgung;]

g) [Nachname(n), Vorname(n), Geburtsname(n), frühere Namen und Aliasnamen, Geburtsdatum, Geburtsort, Geschlecht und Staatsangehörigkeit(en) gemäß Artikel 4 der Verordnung über das SIS im Bereich der Rückkehr illegal aufhältiger Drittstaatsangehöriger;]

h) [Nachname (Familienname), Vorname(n), Geburtsdatum, Geburtsort, Staatsangehörigkeit(en) und Geschlecht gemäß Artikel 5 Absatz 1 Buchstabe a der ECRIS-TCN-Verordnung.]

(4) Die Prüfung auf Mehrfachidentitäten wird nur durchgeführt, um Daten, die in einem Informationssystem vorhanden sind, mit Daten, die in anderen Informationssystemen vorhanden sind, zu vergleichen.

Artikel 28
Ergebnisse der Prüfung auf Mehrfachidentitäten

(1) Wenn die Abfragen nach Artikel 27 Absätze 2 und 3 keinen Treffer ergeben, werden die in Artikel 27 Absatz 1 genannten Verfahren gemäß den einschlägigen Verordnungen fortgesetzt.

(2) Wenn die Abfrage nach Artikel 27 Absätze 2 und 3 einen oder mehrere Treffer ergibt, erstellen der CIR und gegebenenfalls das SIS eine Verknüpfung zwischen den für die Abfrage verwendeten Daten und den Daten, die zu dem Treffer geführt haben.

Wenn mehrere Treffer gemeldet werden, wird eine Verknüpfung zwischen allen Daten, die zu dem Treffer geführt haben, erstellt. Wenn Daten bereits verknüpft waren, wird die bestehende Verknüpfung auf die zur Abfrage verwendeten Daten ausgeweitet.

(3) Wenn die Abfrage nach Artikel 27 Absatz 2 oder 3 einen oder mehrere Treffer ergibt und die Identitätsdaten der verknüpften Dateien identisch oder ähnlich sind, wird eine weiße Verknüpfung nach Artikel 33 erstellt.

(4) Wenn die Abfrage nach Artikel 27 Absatz 2 oder 3 einen oder mehrere Treffer ergibt und die Identitätsdaten der verknüpften Dateien nicht als ähnlich angesehen werden können, wird eine gelbe Verknüpfung nach Artikel 30 erstellt, und das Verfahren nach Artikel 29 gelangt zur Anwendung.

(5) Die Kommission legt die Verfahren zur Ermittlung der Fälle, in denen Identitätsdaten als identisch oder ähnlich angesehen werden können, in Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 64 Absatz 2 genannten Prüfverfahren erlassen.

(6) Die Verknüpfungen werden in der Identitätsbestätigungsdatei gemäß Artikel 34 gespeichert.

Die Kommission legt die technischen Vorschriften für die Verknüpfung von Daten aus unterschiedlichen Informationssystemen im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 64 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 29
Manuelle Verifizierung verschiedener Identitäten

(1) Unbeschadet von Absatz 2 sind für die Verifizierung verschiedener Identitäten folgende Behörden zuständig:

a) – (entfällt);

b) – (entfällt);

c) – (entfällt);

d) bei Treffern, die bei der Prüfung eines Antrags auf internationalen Schutz gemäß der Eurodac-Verordnung erzielt wurden, die Behörde, die einen solchen Antrag prüft;

e) bei Treffern, die bei der Eingabe einer SIS-Ausschreibung gemäß den [Verordnungen über das SIS im Bereich der Strafverfolgung beziehungsweise im Bereich der Rückkehr illegal aufhältiger Drittstaatsangehöriger] erzielt wurden, die SIRENE-Büros des Mitgliedstaats;

f) bei Treffern, die bei der Erfassung oder Aktualisierung von Daten im ECRIS-TCN nach Artikel 5 der [ECRIS-TCN-Verordnung] erzielt wurden, die Zentralbehörden des Urteilsmitgliedstaats.

Der Detektor für Mehrfachidentitäten gibt die für die Verifizierung verschiedener Identitäten zuständige Behörde in der Identitätsbestätigungsdatei an.

(2) Die für die Verifizierung verschiedener Identitäten in der Identitätsbestätigungsdatei zuständige Behörde ist das SIRENE-Büro des Mitgliedstaats, der die Ausschreibung eingegeben hat, wenn eine Verknüpfung zu Daten erstellt wird, die

a) in einer Personenausschreibung zum Zwecke der Übergabe- oder Auslieferungshaft nach Artikel 26 der [Verordnung über das SIS im Bereich der Strafverfolgung] enthalten sind;

b) in einer Ausschreibung von Vermissten oder gefährdeten Personen nach Artikel 32 der [Verordnung über das SIS im Bereich der Strafverfolgung] enthalten sind;

c) in einer Ausschreibung von Personen, die im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesucht werden, nach Artikel 34 der [Verordnung über das SIS im Bereich der Strafverfolgung] enthalten sind;

d) [in einer Ausschreibung zur Rückkehr gemäß der Verordnung über das SIS im Bereich der Rückkehr illegal aufhältiger Drittstaatsangehöriger enthalten sind];

e) in einer Ausschreibung von Personen für verdeckte Kontrollen, Ermittlungsanfragen oder gezielte Kontrollen nach Artikel 36 der [Verordnung über das SIS im Bereich der Strafverfolgung] enthalten sind;

f) in einer Ausschreibung zu unbekannten gesuchten Personen zwecks Identifizierung nach Maßgabe des nationalen Rechts und Suche anhand biometrischer Daten nach Artikel 40 der [Verordnung über das SIS im Bereich der Strafverfolgung] enthalten sind.

(3) Die für die Verifizierung verschiedener Identitäten zuständige Behörde erhält unbeschadet des Absatzes 4 Zugriff auf die in der betreffenden Identitätsbestätigungsdatei enthaltenen einschlägigen Daten und auf die im CIR und gegebenenfalls im SIS verknüpften Daten, prüft die verschiedenen Identitäten, aktualisiert die Verknüpfung gemäß den Artikeln 31, 32 und 33 und fügt diese unverzüglich zur Identitätsbestätigungsdatei hinzu.

(4) – (entfällt).

(5) Wenn mehr als eine Verknüpfung angezeigt wird, prüft die für die Verifizierung verschiedener Identitäten zuständige Behörde jede Verknüpfung gesondert.

(6) Wenn Daten, die zu einem Treffer geführt haben, bereits verknüpft sind, berücksichtigt die für die Verifizierung verschiedener Identitäten zuständige Behörde die bestehenden Verknüpfungen bei der Prüfung, ob neue Verknüpfungen erstellt werden müssen.

Artikel 30
Gelbe Verknüpfung

(1) Eine Verknüpfung zwischen Daten aus zwei oder mehr Informationssystemen wird in folgenden Fällen als gelb klassifiziert:

a) Die verknüpften Daten enthalten dieselben biometrischen Daten, aber unterschiedliche Identitätsdaten, und es wurde keine manuelle Verifizierung verschiedener Identitäten vorgenommen;

b) die verknüpften Daten enthalten unterschiedliche Identitätsdaten, und es wurde keine manuelle Verifizierung verschiedener Identitäten vorgenommen.

(2) Wenn eine Verknüpfung gemäß Absatz 1 als gelb klassifiziert wird, gelangt das Verfahren nach Artikel 29 zur Anwendung.

Artikel 31
Grüne Verknüpfung

(1) Eine Verknüpfung zwischen Daten aus zwei oder mehr Informationssystemen wird als grün klassifiziert, wenn die verknüpften Daten nicht dieselben biometrischen Daten, aber ähnliche Identitätsdaten enthalten und die für die Verifizierung verschiedener Identitäten zuständige Behörde festgestellt hat, dass sich diese Daten auf zwei unterschiedliche Personen beziehen.

(2) Wenn eine Abfrage im CIR oder im SIS durchgeführt wird und eine grüne Verknüpfung zwischen Daten aus zwei oder mehr Informationssystemen, die Bestandteil des CIR sind, oder zum SIS besteht, zeigt der MID an, dass die Identitätsdaten der verknüpften Daten nicht ein und dieselbe Person bezeichnen. In der Antwort des abgefragten Informationssystems werden nur die Daten der Person angezeigt, deren Daten für die Abfrage verwendet wurden, ohne dass ein Treffer aufgrund der Daten, die Gegenstand der grünen Verknüpfung sind, ausgelöst wird.

Artikel 32
Rote Verknüpfung

(1) Eine Verknüpfung zwischen Daten aus zwei oder mehr Informationssystemen wird in folgenden Fällen als rot klassifiziert:

a) Die verknüpften Daten enthalten dieselben biometrischen Daten, aber unterschiedliche Identitätsdaten, und die für die Verifizierung verschiedener Identitäten zuständige Behörde hat festgestellt, dass diese Daten illegalerweise ein und dieselbe Person bezeichnen;

b) die verknüpften Daten enthalten ähnliche Identitätsdaten, und die für die Verifizierung verschiedener Identitäten zuständige Behörde hat festgestellt, dass diese Daten illegalerweise ein und dieselbe Person bezeichnen.

(2) Wenn eine Abfrage im CIR oder im SIS durchgeführt wird und eine rote Verknüpfung zwischen zwei oder mehr Informationssystemen, die Bestandteil des CIR sind, oder zum SIS besteht, zeigt der MID die in Artikel 34 genannten Daten an. Bei etwaigen Folgemaßnahmen zu einer roten Verknüpfung sind die einschlägigen Bestimmungen des Unionsrechts und der nationalen Rechtsvorschriften einzuhalten.

(3) Wenn eine rote Verknüpfung zwischen Daten aus dem EES, dem VIS, [dem ETIAS], Eurodac oder [dem ECRIS-TCN] erstellt wird, wird die im CIR gespeicherte individuelle Datei gemäß Artikel 19 Absatz 1 aktualisiert.

(4) Unbeschadet der Bestimmungen für die Handhabung von Ausschreibungen im SIS in den [Verordnungen über das SIS im Bereich der Grenzkontrollen, über das SIS im Bereich der Strafverfolgung und über das SIS im Bereich der Rückkehr illegal aufhältiger Drittstaatsangehöriger] und unbeschadet der erforderlichen Einschränkungen zum Schutz der Sicherheit und der öffentlichen Ordnung, zur Verhütung von Kriminalität und zur Gewährleistung, dass bei der Erstellung einer roten Verknüpfung keine nationalen Ermittlungen beeinträchtigt werden, teilt die für die Verifizierung verschiedener Identitäten zuständige Behörde der Person mit, dass illegale Mehrfachidentitäten vorliegen.

(5) Wenn eine rote Verknüpfung erstellt wird, gibt die für die Verifizierung verschiedener Identitäten zuständige Behörde an, welche Behörden für die verknüpften Daten zuständig sind.

Artikel 33
Weiße Verknüpfung

(1) Eine Verknüpfung zwischen Daten aus zwei oder mehr Informationssystemen wird in folgenden Fällen als weiß klassifiziert:

a) Die verknüpften Daten enthalten dieselben biometrischen Daten und dieselben oder ähnliche Identitätsdaten;

b) die verknüpften Daten enthalten dieselben oder ähnliche Identitätsdaten, und in mindestens einem der Informationssysteme liegen keine biometrischen Daten zu der Person vor;

c) die verknüpften Daten enthalten dieselben biometrischen Daten, aber unterschiedliche Identitätsdaten, und die für die Verifizierung verschiedener Identitäten zuständige Behörde hat festgestellt, dass diese Daten ein und dieselbe Person bezeichnen, zu der rechtmäßig verschiedene Identitätsdaten vorliegen.

(2) Wenn eine Abfrage im CIR oder im SIS durchgeführt wird und eine weiße Verknüpfung zwischen zwei oder mehr Informationssystemen, die Bestandteil des CIR sind, oder zum SIS besteht, zeigt der MID an, dass die Identitätsdaten der verknüpften Daten ein und dieselbe Person bezeichnen. In der Antwort der abgefragten Informationssysteme werden gegebenenfalls alle verknüpften Daten zu der betreffenden Person angezeigt, das heißt, es erfolgt ein Treffer auf Basis der Daten, die Gegenstand der weißen Verknüpfung sind, sobald die Behörde, welche die Abfrage durchführt, nach dem Unionsrecht oder nationalen Rechtsvorschriften Zugriff auf die verknüpften Daten nimmt.

(3) Wenn eine weiße Verknüpfung zwischen Daten aus dem EES, dem VIS, [dem ETIAS], Eurodac oder [dem ECRIS-TCN] erstellt wird, wird die im CIR gespeicherte individuelle Datei gemäß Artikel 19 Absatz 1 aktualisiert.

(4) Wenn nach einer manuellen Verifizierung von Mehrfachidentitäten eine weiße Verknüpfung erstellt wird, teilt die für die Verifizierung verschiedener Identitäten zuständige Behörde der betreffenden Person unbeschadet der Bestimmungen für die Handhabung von Ausschreibungen im SIS in den [Verordnungen über das SIS im Bereich der Grenzkontrollen, über das SIS im Bereich der Strafverfolgung und über

das SIS im Bereich der Rückkehr illegal aufhältiger Drittstaatsangehöriger] mit, dass bei ihren personenbezogenen Daten Abweichungen zwischen den Systemen bestehen und welche Behörden für die verknüpften Daten zuständig sind.

Artikel 34
Identitätsbestätigungsdatei

Die Identitätsbestätigungsdatei enthält folgende Daten:

a) die in den Artikeln 30 bis 33 genannten farblich markierten Verknüpfungen;

b) eine Angabe der Informationssysteme, deren Daten miteinander verknüpft sind;

c) eine einmalige Kennnummer, die das Abrufen der Daten entsprechender verknüpfter Dateien aus den Informationssystemen ermöglicht;

d) gegebenenfalls eine Angabe der für die Verifizierung verschiedener Identitäten zuständigen Behörde.

Artikel 35
Datenspeicherung im Detektor für Mehrfachidentitäten

Die Identitätsbestätigungsdateien und die in ihnen enthaltenen Daten einschließlich der Verknüpfungen werden im MID nur so lange gespeichert, wie die verknüpften Daten in zwei oder mehr Informationssystemen der EU gespeichert werden.

Artikel 36
Führen von Protokollen

(1) eu-LISA führt Protokolle über alle Datenverarbeitungsvorgänge im MID. Diese Protokolle umfassen insbesondere folgende Angaben:

a) Zweck des Zugriffs des Nutzers und seine Zugangsrechte;

b) Datum und Uhrzeit der Abfrage;

c) Art der für die Abfrage(n) verwendeten Daten;

d) verknüpfte Daten;

e) Chronik der Identitätsbestätigungsdatei;

f) Kennung der Person, die die Abfrage vorgenommen hat.

(2) Jeder Mitgliedstaat führt Protokolle über die zur Nutzung des MID ermächtigten Bediensteten.

(3) Die Protokolle dürfen nur zur datenschutzrechtlichen Kontrolle, einschließlich zur Prüfung der Zulässigkeit eines Antrags und der Rechtmäßigkeit der Datenverarbeitung sowie zum Zweck der Sicherstellung und der Datensicherheit gemäß Artikel 42 verwendet werden. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und ein Jahr nach ihrer Erstellung gelöscht, sofern sie nicht für ein bereits eingeleitetes Kontrollverfahren benötigt werden. Die Protokolle über die Chronik der Identitätsbestätigungsdatei werden gelöscht, nachdem die Daten in der Identitätsbestätigungsdatei gelöscht wurden.

KAPITEL VI
Maßnahmen zur Unterstützung der Interoperabilität

Artikel 37
Datenqualität

(1) eu-LISA führt für die im SIS, in Eurodac, [im ECRIS-TCN], im gemeinsamen Dienst für den Abgleich biometrischer Daten (gemeinsamer BMS), im gemeinsamen Speicher für Identitätsdaten (CIR) und im Detektor für Mehrfachidentitäten (MID) gespeicherten Daten Mechanismen und Verfahren für die automatische Datenqualitätskontrolle ein.

(2) eu-LISA legt gemeinsame Datenqualitätsindikatoren und die Mindestqualitätsstandards für die Speicherung von Daten im SIS, in Eurodac, [im ECRIS-TCN], im gemeinsamen BMS, im CIR und im MID fest.

(3) eu-LISA legt den Mitgliedstaaten regelmäßig Berichte über die Mechanismen und Verfahren für die automatische Datenqualitätskontrolle sowie die gemeinsamen Datenqualitätsindikatoren vor. Ferner legt eu-LISA der Kommission regelmäßig Berichte über die festgestellten Probleme und die betroffenen Mitgliedstaaten vor.

(4) Die Einzelheiten der Mechanismen und Verfahren für die automatische Datenqualitätskontrolle sowie der gemeinsamen Datenqualitätsindikatoren und der Mindestqualitätsstandards für die Speicherung von Daten im SIS, in Eurodac, [im ECRIS-TCN], im gemeinsamen BMS, im CIR und im MID, insbesondere in Bezug auf biometrische Daten, werden in Durchführungsrechtsakten festgelegt. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 64 Absatz 2 genannten Prüfverfahren erlassen.

(5) Ein Jahr nach der Einführung der Mechanismen und Verfahren für die automatische Datenqualitätskontrolle sowie der gemeinsamen Datenqualitätsindikatoren und danach jedes Jahr evaluiert die Kommission die Umsetzung der Datenqualität durch die Mitgliedstaaten und gibt erforderlichenfalls Empfehlungen ab. Die Mitgliedstaaten legen der Kommission einen Aktionsplan zur Beseitigung etwaiger im Evaluierungsbericht festgestellter Mängel vor und erstatten Bericht über die Fortschritte bei der Umsetzung dieses Aktionsplans, bis dieser vollständig umgesetzt ist. Die Kommission übermittelt den Evaluierungsbericht dem Europäischen Parlament, dem Rat, dem Europäischen Datenschutzbeauftragten und der durch die Verordnung (EG) Nr. 168/2007 des Rates[63] eingerichteten Agentur der Europäischen Union für Grundrechte.

Artikel 38
Universelles Nachrichtenformat (Universal Message Format)

(1) Das universelle Nachrichtenformat (Universal Message Format – UMF) wird hiermit eingeführt. Mit dem UMF werden Standards für bestimmte inhaltliche Elemente des grenzüberschreitenden Informationsaustauschs zwischen Informationssystemen, Behörden und/oder Organisationen im Bereich Justiz und Inneres festgelegt.

[63] Verordnung (EG) Nr. 168/2007 des Rates vom 15. Februar 2007 zur Errichtung einer Agentur der Europäischen Union für Grundrechte (ABl. L 53 vom 22.2.2007, S. 1).

(2) Der UMF-Standard ist bei der Entwicklung von [Eurodac], des [ECRIS-TCN], des Europäischen Suchportals (ESP), des CIR und des MID sowie gegebenenfalls bei der Entwicklung neuer Modelle für den Informationsaustausch und neuer Informationssysteme im Bereich Justiz und Inneres durch eu-LISA oder eine andere EU-Stelle zu verwenden.

(3) Im SIS sowie in allen bestehenden oder neuen Modellen für den grenzübergreifenden Informationsaustausch und Informationssystemen im Bereich Justiz und Inneres, die von Mitgliedstaaten oder assoziierten Ländern entwickelt wurden oder werden, kann die Umsetzung des UMF-Standards in Betracht gezogen werden.

(4) Die Kommission erlässt einen Durchführungsrechtsakt zur Festlegung und Entwicklung des in Absatz 1 genannten UMF-Standards. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 64 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 39
Zentraler Speicher für Berichte und Statistiken

(1) Es wird ein zentraler Speicher für Berichte und Statistiken (central repository for reporting and statistics – CRRS) eingerichtet, um die Ziele von Eurodac, des SIS sowie [des ECRIS-TCN] zu unterstützen und systemübergreifende statistische Daten und analytische Berichte für politische und operative Zwecke sowie für die Zwecke der Datenqualität zu erstellen.

(2) eu-LISA sorgt an ihren technischen Standorten für die Einrichtung, die Implementierung und das Hosting des CRRS, das logisch getrennt die Daten nach [Artikel 42 Absatz 8 der Eurodac-Verordnung], [Artikel 71 der Verordnung über das SIS im Bereich der Strafverfolgung] und [Artikel 30 des ECRIS-TCN-Verordnung] enthält. Die im CRRS enthaltenen Daten dürfen nicht die Identifizierung einzelner Personen ermöglichen. Der Zugang zum Speicher erfolgt in Form eines gesicherten Zugangs über das TESTA-Netz (transeuropäische Telematikdienste für Behörden) mit Zugangskontrollen und spezifischen Nutzerprofilen und wird den in [Artikel 42 Absatz 8 der Eurodac-Verordnung], [Artikel 71 der Verordnung über das SIS im Bereich der Strafverfolgung] und [Artikel 30 des ECRIS-TCN-Verordnung] genannten Behörden ausschließlich zu Berichterstattungs- und Statistikzwecken gewährt.

(3) eu-LISA anonymisiert die Daten und speichert diese anonymen Daten im CRRS. Die Anonymisierung der Daten erfolgt nach einem automatisierten Verfahren.

(4) Der CRRS umfasst

a) eine zentrale Infrastruktur, die aus einem Datenregister besteht, das die Ausgabe anonymisierter Daten ermöglicht;

b) eine sichere Kommunikationsinfrastruktur, über die der CRRS mit dem SIS, Eurodac und [dem ECRIS-TCN] sowie den zentralen Infrastrukturen des gemeinsamen BMS, des CIR und des MID verbunden ist.

(5) Die Kommission legt detaillierte Bestimmungen über den Betrieb des CRRS, einschließlich spezifischer Garantien für die Verarbeitung der in den Absätzen 2 und 3 genannten personenbezogenen Daten und der für den Speicher geltenden Sicherheitsvorschriften, im Wege von Durchführungsrechtsakten fest. Diese

Durchführungsrechtsakte werden gemäß dem in Artikel 64 Absatz 2 genannten Prüfverfahren erlassen.

KAPITEL VII
Datenschutz

Artikel 40
Für die Datenverarbeitung Verantwortlicher

(1) Für die Verarbeitung von Daten im gemeinsamen Dienst für den Abgleich biometrischer Daten (gemeinsamer BMS) gelten die Behörden der Mitgliedstaaten, die jeweils für die Verarbeitung in Eurodac, im SIS und [im ECRIS-TCN] verantwortlich sind, ebenfalls als Verantwortliche im Sinne des Artikels 4 Absatz 7 der Verordnung (EU) 2016/679 für die aus den in Artikel 13 genannten Daten generierten biometrischen Templates, die sie in die jeweiligen Systeme eingeben, und tragen die Verantwortung für die Verarbeitung der biometrischen Templates im gemeinsamen BMS.

(2) Für die Verarbeitung von Daten im gemeinsamen Speicher für Identitätsdaten (CIR) gelten die Behörden der Mitgliedstaaten, die jeweils für die Verarbeitung in Eurodac und [im ECRIS-TCN] verantwortlich sind, ebenfalls als Verantwortliche im Sinne des Artikels 4 Absatz 7 der Verordnung (EU) 2016/679 für die in Artikel 18 genannten Daten, die sie in die jeweiligen Systeme eingeben, und tragen die Verantwortung für die Verarbeitung dieser personenbezogenen Daten im CIR.

(3) Für die Verarbeitung von Daten im Detektor für Mehrfachidentitäten (MID)

a) gilt die Europäische Agentur für die Grenz- und Küstenwache als für die Verarbeitung Verantwortlicher im Sinne des Artikels 2 Buchstabe b der Verordnung (EG) Nr. 45/2001 in Bezug auf die Verarbeitung personenbezogener Daten durch die ETIAS-Zentralstelle;

b) gelten die Behörden der Mitgliedstaaten, die Daten in der Identitätsbestätigungsdatei hinzufügen oder ändern, ebenfalls als Verantwortliche im Sinne des Artikels 4 Absatz 7 der Verordnung (EU) 2016/679 und tragen die Verantwortung für die Verarbeitung personenbezogener Daten im MID.

Artikel 41
Auftragsverarbeiter

Für die Verarbeitung personenbezogener Daten im CIR gilt eu-LISA als Auftragsverarbeiter im Sinne des Artikels 2 Buchstabe e der Verordnung (EG) Nr. 45/2001.

Artikel 42
Sicherheit der Verarbeitung

(1) Sowohl eu-LISA als auch die Behörden der Mitgliedstaaten stellen sicher, dass die Sicherheit der Verarbeitung personenbezogener Daten nach Maßgabe dieser Verordnung gewährleistet wird. Bei der Erfüllung sicherheitsbezogener Aufgaben arbeiten eu-LISA, [die ETIAS-Zentralstelle] und die Behörden der Mitgliedstaaten zusammen.

(2) Unbeschadet des Artikels 22 der Verordnung (EG) Nr. 45/2001 ergreift eu-LISA die erforderlichen Maßnahmen, um die Sicherheit der Interoperabilitätskomponenten und der mit ihnen verbundenen Kommunikationsinfrastruktur sicherzustellen.

(3) Insbesondere trifft eu-LISA die erforderlichen Maßnahmen, einschließlich der Annahme eines Sicherheitsplans sowie eines Betriebskontinuitätsplans und eines Notfallwiederherstellungsplans, um

a) die Daten physisch zu schützen, unter anderem durch Aufstellung von Notfallplänen für den Schutz kritischer Infrastrukturen;

b) zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden;

c) die unbefugte Dateneingabe sowie die unbefugte Kenntnisnahme, Änderung oder Löschung gespeicherter personenbezogener Daten zu verhindern;

d) die unbefugte Datenverarbeitung sowie das unbefugte Kopieren, Ändern oder Löschen von Daten zu verhindern;

e) sicherzustellen, dass die zum Zugang zu den Interoperabilitätskomponenten berechtigten Personen nur mittels einer persönlichen Benutzerkennung und vertraulicher Zugriffsverfahren ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können;

f) sicherzustellen, dass überprüft und festgestellt werden kann, welchen Stellen personenbezogene Daten durch Datenübertragungseinrichtungen übermittelt werden können;

g) sicherzustellen, dass überprüft und festgestellt werden kann, welche Daten wann, von wem und zu welchem Zweck in den Interoperabilitätskomponenten verarbeitet wurden;

h) das unbefugte Lesen, Kopieren, Ändern oder Löschen von personenbezogenen Daten während der Übermittlung personenbezogener Daten an die oder aus den Interoperabilitätskomponenten oder während des Transports von Datenträgern zu verhindern, insbesondere durch geeignete Verschlüsselungstechniken;

i) die Wirksamkeit der in diesem Absatz genannten Sicherheitsmaßnahmen zu überwachen und die erforderlichen organisatorischen Maßnahmen für die interne Überwachung zu treffen, um die Einhaltung dieser Verordnung sicherzustellen.

(4) Die Mitgliedstaaten treffen für die Verarbeitung personenbezogener Daten durch die Behörden, die das Recht auf Zugang zu Interoperabilitätskomponenten haben, Sicherheitsmaßnahmen, die den in Absatz 3 genannten entsprechen.

Artikel 43
Vertraulichkeit von SIS-Daten

(1) Jeder Mitgliedstaat wendet nach Maßgabe seines nationalen Rechts die einschlägigen Vorschriften über die berufliche Schweigepflicht beziehungsweise eine andere vergleichbare Geheimhaltungspflicht auf alle Personen und Stellen an, die mit SIS-Daten, auf die über eine Interoperabilitätskomponente zugegriffen wird, arbeiten müssen. Diese Pflicht besteht auch nach dem Ausscheiden dieser Personen aus dem Amt oder Dienstverhältnis oder nach der Beendigung der Tätigkeit dieser Stellen weiter.

(2) Unbeschadet des Artikels 17 des Statuts der Beamten und der Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union wendet eu-LISA geeignete Regeln für die berufliche Schweigepflicht beziehungsweise eine andere vergleichbare Geheimhaltungspflicht auf alle Mitarbeiter an, die mit SIS-Daten arbeiten müssen, wobei mit Absatz 1 vergleichbare Standards einzuhalten sind. Diese Pflicht besteht auch nach dem Ausscheiden dieser Personen aus dem Amt oder Dienstverhältnis oder nach der Beendigung ihrer Tätigkeit weiter.

Artikel 44
Sicherheitsvorfälle

(1) Jedes Ereignis, das sich auf die Sicherheit der Interoperabilitätskomponenten auswirkt oder auswirken und darin gespeicherte Daten beschädigen oder ihren Verlust herbeiführen kann, ist als Sicherheitsvorfall anzusehen; dies gilt insbesondere, wenn möglicherweise ein unbefugter Datenzugriff erfolgt ist oder die Verfügbarkeit, die Integrität und die Vertraulichkeit von Daten tatsächlich oder möglicherweise nicht mehr gewährleistet gewesen ist.

(2) Sicherheitsvorfällen ist durch eine rasche, wirksame und angemessene Reaktion zu begegnen.

(3) Unbeschadet der Meldung und Mitteilung einer Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 der Verordnung (EU) 2016/679, Artikel 30 der Richtlinie (EU) 2016/680 oder beiden Artikeln unterrichten die Mitgliedstaaten die Kommission, eu-LISA und den Europäischen Datenschutzbeauftragten über Sicherheitsvorfälle. Im Falle eines Sicherheitsvorfalls in Verbindung mit der zentralen Infrastruktur der Interoperabilitätskomponenten unterrichtet eu-LISA die Kommission und den Europäischen Datenschutzbeauftragten.

(4) Informationen über einen Sicherheitsvorfall, der sich auf den Betrieb der Interoperabilitätskomponenten oder die Verfügbarkeit, die Integrität und die Vertraulichkeit der Daten auswirkt oder auswirken kann, werden den Mitgliedstaaten übermittelt und nach Maßgabe des von eu-LISA bereitzustellenden Plans für die Bewältigung von Sicherheitsvorfällen gemeldet.

(5) Die betroffenen Mitgliedstaaten und eu-LISA arbeiten im Falle eines Sicherheitsvorfalls zusammen. Die Kommission legt die genauen Modalitäten dieser Zusammenarbeit im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 64 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 45
Eigenkontrolle

Die Mitgliedstaaten und die zuständigen EU-Stellen stellen sicher, dass jede zum Zugriff auf die Interoperabilitätskomponenten berechtigte Behörde die erforderlichen Maßnahmen zur Überwachung der Einhaltung dieser Verordnung trifft und erforderlichenfalls mit der Aufsichtsbehörde zusammenarbeitet.

Die für die Datenverarbeitung Verantwortlichen im Sinne des Artikels 40 treffen die erforderlichen Maßnahmen, um die Ordnungsgemäßheit der Datenverarbeitung gemäß dieser Verordnung zu überwachen, einschließlich der häufigen Überprüfung von Protokollen, und

arbeiten erforderlichenfalls mit den in den Artikeln 49 und 50 genannten Aufsichtsbehörden zusammen.

Artikel 46
Recht auf Information

(1) Unbeschadet des Rechts auf Erhalt von Informationen gemäß den Artikeln 11 und 12 der Verordnung (EG) Nr. 45/2001 und den Artikeln 13 und 14 der Verordnung (EU) 2016/679 werden Personen, deren Daten im gemeinsamen BMS, im CIR oder im MID gespeichert sind, von der Behörde, die ihre Daten erfasst, zum Zeitpunkt der Datenerfassung über die Verarbeitung personenbezogener Daten für die Zwecke dieser Verordnung, einschließlich der Identität und der Kontaktdaten der jeweiligen für die Verarbeitung Verantwortlichen, über die Verfahren für die Ausübung ihrer Rechte auf Auskunft, Berichtigung und Löschung ihrer Daten sowie über die Kontaktdaten des Europäischen Datenschutzbeauftragten und der nationalen Aufsichtsbehörde des für die Erfassung der Daten zuständigen Mitgliedstaats informiert.

(2) Personen, deren Daten in Eurodac oder [im ECRIS-TCN] gespeichert sind, werden über die Verarbeitung von Daten für die Zwecke dieser Verordnung gemäß Absatz 1 informiert, wenn

a) – (entfällt);

b) – (entfällt);

c) – (entfällt);

d) [in Eurodac nach Artikel 10 der Eurodac-Verordnung ein Antrag auf internationalen Schutz erstellt oder aktualisiert wird;]

e) [im ECRIS-TCN nach Artikel 5 der ECRIS-TCN-Verordnung ein Datensatz angelegt oder aktualisiert wird.]

Artikel 47
Recht auf Auskunft, Berichtigung und Löschung

(1) Personen, die von ihren Rechten nach den Artikeln 13, 14, 15 und 16 der Verordnung (EG) Nr. 45/2001 und den Artikeln 15, 16, 17 und 18 der Verordnung (EU) 2016/679 Gebrauch machen möchten, können sich an den für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaat oder einen anderen Mitgliedstaat wenden, der den Antrag prüft und beantwortet.

(2) Der für die manuelle Verifizierung verschiedener Identitäten zuständige Mitgliedstaat nach Artikel 29 oder der Mitgliedstaat, an den der Antrag gerichtet wurde, beantwortet den Antrag innerhalb von 45 Tagen nach Antragseingang.

(3) Wird ein Antrag auf Berichtigung oder Löschung personenbezogener Daten bei einem anderen Mitgliedstaat als dem zuständigen Mitgliedstaat gestellt, so kontaktiert der Mitgliedstaat, an den der Antrag gerichtet wurde, innerhalb von sieben Tagen die Behörden des zuständigen Mitgliedstaats, und der zuständige Mitgliedstaat überprüft die Richtigkeit der Daten und die Rechtmäßigkeit der Datenverarbeitung innerhalb einer Frist von 30 Tagen nach der Kontaktaufnahme.

(4) Falls bei einer Prüfung festgestellt wird, dass die im Detektor für Mehrfachidentitäten gespeicherten Daten sachlich unrichtig sind oder unrechtmäßig

erfasst wurden, werden sie vom zuständigen Mitgliedstaat oder gegebenenfalls von dem Mitgliedstaat, an der Antrag gerichtet wurde, berichtigt oder gelöscht.

(5) Falls Daten im MID während ihrer Geltungsdauer vom zuständigen Mitgliedstaat geändert werden, nimmt dieser die Verarbeitung nach Artikel 27 und gegebenenfalls die Verarbeitung nach Artikel 29 vor, um zu ermitteln, ob die geänderten Daten verknüpft werden müssen. Ergibt sich bei der Verarbeitung kein Treffer, so löscht der zuständige Mitgliedstaat oder gegebenenfalls der Mitgliedstaat, an den der Antrag gerichtet wurde, die Daten aus der Identitätsbestätigungsdatei. Falls bei der automatisierten Verarbeitung ein oder mehrere Treffer gemeldet werden, erstellt oder aktualisiert der zuständige Mitgliedstaat die betreffende Verknüpfung gemäß den einschlägigen Bestimmungen dieser Verordnung.

(6) Ist der zuständige Mitgliedstaat oder gegebenenfalls der Mitgliedstaat, an den der Antrag gerichtet wurde, nicht der Ansicht, dass die im MID gespeicherten Daten sachlich unrichtig sind oder unrechtmäßig gespeichert wurden, so erlässt er eine Verwaltungsentscheidung, in der er der betroffenen Person unverzüglich schriftlich erläutert, warum er nicht zu einer Berichtigung oder Löschung der sie betreffenden Daten bereit ist.

(7) In der Verwaltungsentscheidung wird die betroffene Person zudem darüber belehrt, dass sie die in Bezug auf ihren in Absatz 3 genannten Antrag ergangene Entscheidung anfechten und wie sie gegebenenfalls bei den zuständigen Behörden oder Gerichten einschließlich der zuständigen nationalen Aufsichtsbehörden Klage erheben oder Beschwerde einlegen kann.

(8) Jeder Antrag nach Absatz 3 enthält die zur Identifizierung der betroffenen Person notwendigen Informationen. Diese Informationen werden ausschließlich dazu verwendet, dem Antragsteller die Wahrnehmung der in Absatz 3 genannten Rechte zu ermöglichen, und anschließend unverzüglich gelöscht.

(9) Der zuständige Mitgliedstaat oder gegebenenfalls der Mitgliedstaat, an den der Antrag gerichtet wurde, führt eine schriftliche Aufzeichnung darüber, dass ein Antrag gemäß Absatz 3 gestellt und wie dieser bearbeitet wurde, und stellt diese Aufzeichnung unverzüglich den für den Datenschutz zuständigen nationalen Aufsichtsbehörden zur Verfügung.

Artikel 48
Übermittlung personenbezogener Daten an Drittstaaten, internationale Organisationen und private Stellen

Personenbezogene Daten, die in den Interoperabilitätskomponenten gespeichert sind oder auf die über die Interoperabilitätskomponenten zugegriffen wird, dürfen nicht an Drittstaaten, internationale Organisationen oder private Stellen übermittelt oder diesen zur Verfügung gestellt werden.

Artikel 49
Kontrolle durch die nationale Aufsichtsbehörde

(1) Die nach Artikel 49 der Verordnung (EU) 2016/679 bestimmte(n) Aufsichtsbehörde(n) gewährleistet beziehungsweise gewährleisten, dass mindestens alle vier Jahre die Datenverarbeitungsvorgänge der zuständigen nationalen Behörden nach den einschlägigen internationalen Prüfungsstandards überprüft werden.

(2) Die Mitgliedstaaten stellen sicher, dass ihre Aufsichtsbehörde über ausreichende Ressourcen zur Wahrnehmung der Aufgaben verfügt, die ihr gemäß dieser Verordnung übertragen werden.

Artikel 50
Kontrolle durch den Europäischen Datenschutzbeauftragten

Der Europäische Datenschutzbeauftragte trägt dafür Sorge, dass die durch eu-LISA erfolgende Verarbeitung personenbezogener Daten mindestens alle vier Jahre nach den einschlägigen internationalen Prüfungsstandards überprüft wird. Der Prüfbericht wird dem Europäischen Parlament, dem Rat, eu-LISA, der Kommission und den Mitgliedstaaten übermittelt. eu-LISA erhält vor der Annahme des Berichts Gelegenheit zur Stellungnahme.

Artikel 51
Zusammenarbeit zwischen den nationalen Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten

(1) Der Europäische Datenschutzbeauftragte arbeitet bei speziellen Fragen, die eine Einbeziehung der nationalen Ebene erfordern, eng mit den nationalen Aufsichtsbehörden zusammen, insbesondere wenn der Europäische Datenschutzbeauftragte oder eine nationale Aufsichtsbehörde größere Diskrepanzen zwischen den Verfahrensweisen der Mitgliedstaaten feststellt oder möglicherweise unrechtmäßige Übermittlungen über die Kommunikationskanäle der Interoperabilitätskomponenten bemerkt, oder bei Fragen einer oder mehrerer nationaler Aufsichtsbehörden zur Durchführung und Auslegung dieser Verordnung.

(2) In den in Absatz 1 genannten Fällen wird eine koordinierte Überwachung gemäß Artikel 62 der Verordnung (EU) XXXX/2018 [überarbeitete Verordnung (EG) Nr. 45/2001] sichergestellt.

KAPITEL VIII
Verantwortlichkeiten

Artikel 52
Verantwortlichkeiten von eu-LISA während der Konzept- und Entwicklungsphase

(1) eu-LISA stellt sicher, dass die zentralen Infrastrukturen der Interoperabilitätskomponenten im Einklang mit dieser Verordnung betrieben werden.

(2) Die Interoperabilitätskomponenten werden an den technischen Standorten von eu-LISA betrieben und bieten die in dieser Verordnung vorgesehenen Funktionen gemäß den in Artikel 53 Absatz 1 festgelegten Bedingungen in Bezug auf die Sicherheit, Verfügbarkeit, Qualität und Geschwindigkeit.

(3) eu-LISA ist verantwortlich für die Entwicklung der Interoperabilitätskomponenten sowie für jegliche Anpassungen, die erforderlich sind, um die Interoperabilität zwischen den Zentralsystemen des EES, des VIS, [des ETIAS,] des SIS und von Eurodac, [dem ECRIS-TCN], dem Europäischen Suchportal (ESP), dem gemeinsamen Dienst für den Abgleich biometrischer Daten (gemeinsamer BMS), dem gemeinsamen Speicher für Identitätsdaten (CIR) und dem Detektor für Mehrfachidentitäten (MID) herzustellen.

eu-LISA konzipiert die Architektur der Interoperabilitätskomponenten einschließlich ihrer Kommunikationsinfrastrukturen, legt ihre technischen Spezifikationen fest und bestimmt ihre Weiterentwicklung in Bezug auf die zentrale Infrastruktur und die sichere Kommunikationsinfrastruktur, die vom Verwaltungsrat der eu-LISA vorbehaltlich einer befürwortenden Stellungnahme der Kommission angenommen werden. eu-LISA nimmt zudem etwaige erforderliche Anpassungen am SIS, an Eurodac oder [am ECRIS-TCN] vor, die für die Herstellung der Interoperabilität notwendig und in dieser Verordnung vorgesehen sind.

eu-LISA entwickelt und implementiert die Interoperabilitätskomponenten so bald wie möglich nach dem Inkrafttreten dieser Verordnung und nach Erlass der in Artikel 8 Absatz 2, Artikel 9 Absatz 7, Artikel 28 Absätze 5 und 6, Artikel 37 Absatz 4, Artikel 38 Absatz 4, Artikel 39 Absatz 5 und Artikel 44 Absatz 5 vorgesehenen Maßnahmen durch die Kommission.

Die Entwicklung umfasst die Ausarbeitung und Umsetzung der technischen Spezifikationen, die Erprobung und die Projektgesamtkoordination.

(4) Während der Konzept- und Entwicklungsphase wird ein Programmverwaltungsrat eingerichtet, der aus höchstens zehn Mitgliedern besteht. Dem Programmverwaltungsrat gehören sieben Mitglieder, die vom Verwaltungsrat von eu-LISA aus dem Kreis seiner Mitglieder oder stellvertretenen Mitglieder ernannt werden, der Vorsitzende der Beratergruppe für Interoperabilität gemäß Artikel 65, ein vom Exekutivdirektor ernannter Vertreter von eu-LISA sowie ein von der Kommission ernanntes Mitglied an. Die vom Verwaltungsrat von eu-LISA ernannten Mitglieder werden ausschließlich aus dem Kreis derjenigen Mitgliedstaaten gewählt, die nach dem Unionsrecht in vollem Umfang durch die Rechtsinstrumente gebunden sind, welche für die Entwicklung, die Errichtung, den Betrieb und die Nutzung aller von eu-LISA verwalteten IT-Großsysteme gelten, und die sich an den Interoperabilitätskomponenten beteiligen werden.

(5) Der Programmverwaltungsrat tritt regelmäßig, mindestens jedoch dreimal pro Quartal zusammen. Er gewährleistet die angemessene Verwaltung der Konzept- und Entwicklungsphase der Interoperabilitätskomponenten.

Der Programmverwaltungsrat legt dem Verwaltungsrat monatlich schriftliche Berichte über den Fortschritt des Projekts vor. Der Programmverwaltungsrat hat keine Entscheidungsbefugnis und kein Mandat zur Vertretung der Mitglieder des Verwaltungsrats von eu-LISA.

(6) Der Verwaltungsrat von eu-LISA legt die Geschäftsordnung des Programmverwaltungsrats fest, in der insbesondere Folgendes geregelt ist:

a) der Vorsitz,

b) die Sitzungsorte,

c) die Vorbereitung von Sitzungen,

d) die Zulassung von Sachverständigen zu den Sitzungen,

e) Kommunikationspläne, die gewährleisten, dass nicht teilnehmende Mitglieder des Verwaltungsrats von eu-LISA lückenlos unterrichtet werden.

Den Vorsitz übernimmt ein Mitgliedstaat, der nach dem Unionsrecht in vollem Umfang durch die Rechtsinstrumente gebunden ist, die für die Entwicklung, die

Errichtung, den Betrieb und die Nutzung aller von eu-LISA verwalteten IT-Großsysteme gelten.

Sämtliche Reise- und Aufenthaltskosten, die den Mitgliedern des Programmverwaltungsrats entstehen, werden von der Agentur erstattet, wobei Artikel 10 der Geschäftsordnung von eu-LISA sinngemäß gilt. eu-LISA stellt das Sekretariat des Programmverwaltungsrats.

Die in Artikel 65 genannte Beratergruppe für Interoperabilität tritt bis zur Inbetriebnahme der Interoperabilitätskomponenten regelmäßig zusammen. Nach jeder Sitzung erstattet sie dem Programmverwaltungsrat Bericht. Sie stellt den technischen Sachverstand für die Unterstützung der Aufgaben des Programmverwaltungsrats bereit und überwacht den Stand der Vorbereitung in den Mitgliedstaaten.

Artikel 53
Verantwortlichkeiten von eu-LISA nach der Inbetriebnahme

(1) Nach der Inbetriebnahme der einzelnen Interoperabilitätskomponenten übernimmt eu-LISA die technische Verwaltung des Zentralsystems und der einheitlichen nationalen Schnittstellen. In Zusammenarbeit mit den Mitgliedstaaten gewährleistet eu-LISA, dass vorbehaltlich einer Kosten-Nutzen-Analyse jederzeit die beste verfügbare Technologie eingesetzt wird. eu-LISA ist zudem für die technische Verwaltung der in den Artikeln 6, 12, 17, 25 und 39 genannten Kommunikationsinfrastruktur verantwortlich.

Die technische Verwaltung der Interoperabilitätskomponenten umfasst alle Aufgaben, die erforderlich sind, um die Interoperabilitätskomponenten im Einklang mit dieser Verordnung täglich rund um die Uhr betriebsbereit zu halten; dazu gehören insbesondere die Wartungsarbeiten und technischen Anpassungen, die erforderlich sind, um sicherzustellen, dass die Komponenten gemäß den technischen Spezifikationen und insbesondere in Bezug auf die Reaktionszeit bei Abfragen der zentralen Infrastrukturen mit zufriedenstellender technischer Qualität arbeiten.

(2) Unbeschadet des Artikels 17 des Statuts der Beamten der Europäischen Union wendet eu-LISA angemessene Regeln zur Gewährleistung der beruflichen Schweigepflicht oder einer anderen vergleichbaren Geheimhaltungspflicht auf alle Bediensteten an, die mit in den Interoperabilitätskomponenten gespeicherten Daten arbeiten. Diese Pflicht besteht auch nach dem Ausscheiden dieser Bediensteten aus dem Amt oder Dienstverhältnis oder der Beendigung ihrer Tätigkeit weiter.

(3) eu-LISA entwickelt einen Mechanismus und Verfahren für die Qualitätskontrolle der im gemeinsamen BMS und im CIR gespeicherten Daten gemäß Artikel 37 und pflegt sie entsprechend.

(4) Ferner nimmt eu-LISA Aufgaben im Zusammenhang mit der Schulung in der technischen Nutzung der Interoperabilitätskomponenten wahr.

Artikel 54
Verantwortlichkeiten der Mitgliedstaaten

(1) Jeder Mitgliedstaat ist verantwortlich für

a) seine Anbindung an die Kommunikationsinfrastruktur des ESP und des CIR;

b) die Integration der bestehenden nationalen Systeme und Infrastrukturen in das ESP, den gemeinsamen BMS, den CIR und den MID;

c) die Organisation, die Verwaltung, den Betrieb und die Wartung seiner nationalen Infrastruktur und deren Anbindung an die Interoperabilitätskomponenten;

d) die Verwaltung und die Regelung des Zugangs der dazu ordnungsgemäß befugten beziehungsweise ermächtigten Mitarbeiter der zuständigen nationalen Behörden zum ESP, zum CIR und zum MID im Einklang mit dieser Verordnung und für die Erstellung und regelmäßige Aktualisierung eines Verzeichnisses dieser Bediensteten und ihrer Profile;

e) den Erlass der in Artikel 20 Absatz 3 genannten Legislativmaßnahmen zur Regelung des Zugriffs auf den CIR zu Identifizierungszwecken;

f) die manuelle Verifizierung verschiedener Identitäten gemäß Artikel 29;

g) die Umsetzung der Datenqualitätsanforderungen in den EU-Informationssystemen und den Interoperabilitätskomponenten;

h) die Beseitigung etwaiger Mängel, die im Evaluierungsbericht der Kommission über die Datenqualität nach Artikel 37 Absatz 5 festgestellt wurden.

(2) Jeder Mitgliedstaat bindet seine benannten Behörden im Sinne von Artikel 4 Nummer 24 an den CIR an.

Artikel 54a
Verantwortlichkeiten von Europol

(1) Europol sorgt dafür, dass über das ESP durchgeführte Abfragen von Europol-Daten verarbeitet werden, und passt seine Schnittstelle für die Abfrage von Europol-Systemen (Querying Europol Systems – QUEST) entsprechend für die Verwendung von BPL-Daten (BPL – basic protection level – Basisschutzniveau) an.

(2) Europol ist verantwortlich für die Verwaltung und die Regelung des Zugangs seiner dazu ordnungsgemäß befugten Mitarbeiter zum ESP beziehungsweise zum CIR und der Nutzung dieser Komponenten durch diese Mitarbeiter im Einklang mit dieser Verordnung sowie für die Erstellung und regelmäßige Aktualisierung eines Verzeichnisses dieser Bediensteten und ihrer Profile.

Artikel 55
Verantwortlichkeiten der ETIAS-Zentralstelle

Die ETIAS-Zentralstelle ist verantwortlich für

a) die manuelle Verifizierung verschiedener Identitäten gemäß Artikel 29;

b) die nach Maßgabe von Artikel 59 vorzunehmende Prüfung der im VIS, in Eurodac und im SIS gespeicherten Daten auf Mehrfachidentitäten.

KAPITEL IX
Schlussbestimmungen

Artikel 56
Berichte und Statistiken

(1) Die folgenden Daten zum Europäischen Suchportal (ESP) dürfen vom dazu ordnungsgemäß ermächtigten Personal der zuständigen Behörden der Mitgliedstaaten, der Kommission und von eu-LISA ausschließlich zur Erstellung von Berichten und Statistiken abgefragt werden, ohne die Identifizierung einzelner Personen zu ermöglichen:

a) Zahl der Abfragen pro Nutzer des ESP-Profils;

b) – (entfällt).

(2) Die folgenden Daten zum gemeinsamen Speicher für Identitätsdaten (CIR) dürfen von dem dazu ordnungsgemäß ermächtigten Personal der zuständigen Behörden der Mitgliedstaaten, der Kommission und von eu-LISA ausschließlich zur Erstellung von Berichten und Statistiken abgefragt werden, ohne die Identifizierung einzelner Personen zu ermöglichen:

a) Zahl der Abfragen für die Zwecke der Artikel 20, 21 und 22;

b) Staatsangehörigkeit, Geschlecht und Geburtsjahr der betreffenden Person;

c) Art des Reisedokuments und aus drei Buchstaben bestehender Code des ausstellenden Staates;

d) Zahl der Abfragen mit und ohne biometrische Daten.

(3) Die folgenden Daten zum Detektor für Mehrfachidentitäten (MID) dürfen von dem dazu ordnungsgemäß ermächtigten Personal der zuständigen Behörden der Mitgliedstaaten, der Kommission und von eu-LISA ausschließlich zur Erstellung von Berichten und Statistiken abgefragt werden, ohne die Identifizierung einzelner Personen zu ermöglichen:

a) Staatsangehörigkeit, Geschlecht und Geburtsjahr der betreffenden Person;

b) Art des Reisedokuments und aus drei Buchstaben bestehender Code des ausstellenden Staates;

c) Zahl der Abfragen mit und ohne biometrische Daten;

d) Zahl der Verknüpfungen, aufgeschlüsselt nach Verknüpfungsart.

(4) Das ordnungsgemäß ermächtigte Personal der gemäß der Verordnung (EU) 2016/1624 des Europäischen Parlaments und des Rates[64] eingerichteten Europäischen Agentur für die Grenz- und Küstenwache kann zur Durchführung von Risikoanalysen und Schwachstellenbeurteilungen nach den Artikeln 11 und 13 jener Verordnung auf die in den Absätzen 1, 2 und 3 genannten Daten zugreifen.

(5) Für die Zwecke von Absatz 1 dieses Artikels speichert eu-LISA die Daten nach Absatz 1 dieses Artikels im zentralen Speicher für Berichte und Statistiken nach

[64] Verordnung (EU) 2016/1624 des Europäischen Parlaments und des Rates vom 14. September 2016 über die Europäische Grenz- und Küstenwache und zur Änderung der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Verordnung (EG) Nr. 863/2007 des Europäischen Parlaments und des Rates, der Verordnung (EG) Nr. 2007/2004 des Rates und der Entscheidung des Rates 2005/267/EG (ABl. L 251 vom 16.9.2016, S. 1).

Kapitel VI dieser Verordnung. Die in dem Speicher enthaltenen Daten dürfen nicht die Identifizierung einzelner Personen ermöglichen, sondern sollen den in Absatz 1 dieses Artikels genannten Behörden die Möglichkeit geben, anpassbare Berichte und Statistiken abzurufen, die dazu beitragen, die Effizienz von Grenzübertrittskontrollen zu steigern, Behörden bei der Bearbeitung von Visumanträgen zu unterstützen und eine faktengestützte Gestaltung der Migrations- und Sicherheitspolitik der Union zu fördern.

Artikel 57
Übergangszeitraum für die Nutzung des Europäischen Suchportals

Während eines Zeitraums von zwei Jahren nach dem Datum der Inbetriebnahme des ESP gelten die Pflichten nach Artikel 7 Absätze 2 und 4 nicht, und die Benutzung des ESP ist fakultativ.

Artikel 58
Übergangszeit für die Bestimmungen über den Zugriff auf den gemeinsamen Speicher für Identitätsdaten zu Strafverfolgungszwecken

Artikel 22 gilt ab dem Tag der Inbetriebnahme gemäß Artikel 62 Absatz 1.

Artikel 59
Übergangszeitraum für die Prüfung auf Mehrfachidentitäten

(1) Für die Dauer eines Jahres, nachdem eu-LISA den Abschluss des in Bezug auf den MID durchgeführten Tests nach Artikel 62 Absatz 1 Buchstabe b mitgeteilt hat, und vor der Inbetriebnahme des MID ist die ETIAS-Zentralstelle im Sinne des [Artikels 33 Buchstabe a der Verordnung (EU) 2016/1624] für die Prüfung der im VIS, in Eurodac und im SIS gespeicherten Daten auf Mehrfachidentitäten zuständig. Die Prüfungen auf Mehrfachidentitäten werden ausschließlich anhand biometrischer Daten gemäß Artikel 27 Absatz 2 dieser Verordnung durchgeführt.

(2) Wenn die Abfrage einen oder mehrere Treffer ergibt und die Identitätsdaten der verknüpften Dateien identisch oder ähnlich sind, wird eine weiße Verknüpfung nach Artikel 33 erstellt.

Wenn die Abfrage einen oder mehrere Treffer ergibt und die Identitätsdaten der verknüpften Dateien nicht als ähnlich angesehen werden können, wird eine gelbe Verknüpfung nach Artikel 30 erstellt, und das Verfahren nach Artikel 29 gelangt zur Anwendung.

Wenn mehrere Treffer gemeldet werden, wird zu jedem Datenelement, das zu einem Treffer geführt hat, eine Verknüpfung erstellt.

(3) Wenn eine gelbe Verknüpfung gemäß Absatz 3 erstellt wird, gewährt der MID der ETIAS-Zentralstelle Zugang zu den in den verschiedenen Informationssystemen gespeicherten Identitätsdaten.

(4) Wenn eine Verknüpfung zu einer Ausschreibung im SIS erstellt wird, bei der es sich weder um eine Ausschreibung zur Einreiseverweigerung noch um eine Ausschreibung zu einem als verloren, gestohlen oder für ungültig erklärt gemeldeten Reisedokument nach Artikel 24 der Verordnung über das SIS im Bereich der Grenzkontrollen beziehungsweise Artikel 38 der Verordnung über das SIS im Bereich der Strafverfolgung handelt, gewährt der MID dem SIRENE-Büro des

Mitgliedstaats, der die Ausschreibung eingegeben hat, Zugang zu den in den verschiedenen Informationssystemen gespeicherten Identitätsdaten.

(5) Die ETIAS-Zentralstelle beziehungsweise das SIRENE-Büro des Mitgliedstaats, der die Ausschreibung eingegeben hat, greift auf die in der Identitätsbestätigungsdatei enthaltenen Daten zu, prüft die verschiedenen Identitäten, aktualisiert die Verknüpfung gemäß den Artikeln 31, 32 und 33 und fügt diese zur Identitätsbestätigungsdatei hinzu.

(6) eu-LISA unterstützt die ETIAS-Zentralstelle gegebenenfalls bei der Prüfung auf Mehrfachidentitäten gemäß diesem Artikel.

Artikel 60
Kosten

(1) Die Kosten im Zusammenhang mit der Einrichtung und dem Betrieb des ESP, des gemeinsamen BMS, des CIR und des MID gehen zulasten des Gesamthaushaltsplans der Union.

(2) Die Kosten im Zusammenhang mit der Integration der bestehenden nationalen Infrastrukturen, deren Anbindung an die einheitlichen nationalen Schnittstellen und dem Hosting der einheitlichen nationalen Schnittstellen gehen zulasten des Gesamthaushaltsplans der Union.

Hiervon ausgenommen sind die Kosten für

a) die Projektverwaltungsstelle der Mitgliedstaaten (Sitzungen, Dienstreisen, Büroräume),

b) das Hosting nationaler IT-Systeme (Räume, Implementierung, Stromversorgung, Kühlung),

c) den Betrieb nationaler IT-Systeme (Betreiber- und Unterstützungsverträge),

d) Konzipierung, Entwicklung, Implementierung, Betrieb und Wartung nationaler Kommunikationsnetze.

(3) Die Kosten im Zusammenhang mit den benannten Behörden im Sinne von Artikel 4 Nummer 24 gehen zulasten der einzelnen Mitgliedstaaten beziehungsweise von Europol. Die Kosten für die Anbindung der benannten Behörden an den CIR gehen zulasten der einzelnen Mitgliedstaaten beziehungsweise von Europol.

Artikel 61
Mitteilungen

(1) Die Mitgliedstaaten teilen eu-LISA die Behörden gemäß den Artikeln 7, 20, 21 und 26 mit, die das ESP, den CIR beziehungsweise den MID nutzen dürfen oder Zugang zum ESP, zum CIR beziehungsweise zum MID haben.

Innerhalb von drei Monaten nach dem Datum, an dem die einzelnen Interoperabilitätskomponenten gemäß Artikel 62 ihren Betrieb aufgenommen haben, wird eine konsolidierte Liste dieser Behörden im *Amtsblatt der Europäischen Union* veröffentlicht. Werden Änderungen an der Liste vorgenommen, so veröffentlicht eu-LISA einmal im Jahr eine aktualisierte konsolidierte Liste.

(2) eu-LISA teilt der Kommission den erfolgreichen Abschluss des Tests nach Artikel 62 Absatz 1 Buchstabe b mit.

(3) Die ETIAS-Zentralstelle teilt der Kommission den erfolgreichen Abschluss der Übergangsmaßnahme nach Artikel 59 mit.

(4) Die Kommission stellt den Mitgliedstaaten und der Öffentlichkeit über eine fortlaufend aktualisierte öffentliche Website die gemäß Absatz 1 mitgeteilten Informationen bereit.

Artikel 62
Aufnahme des Betriebs

(1) Die Kommission beschließt, zu welchem Zeitpunkt die einzelnen Interoperabilitätskomponenten ihren Betrieb aufnehmen, nachdem folgende Voraussetzungen erfüllt sind:

a) Die Maßnahmen nach Artikel 8 Absatz 2, Artikel 9 Absatz 7, Artikel 28 Absätze 5 und 6, Artikel 37 Absatz 4, Artikel 38 Absatz 4, Artikel 39 Absatz 5 und Artikel 44 Absatz 5 wurden angenommen;

b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests der jeweiligen Interoperabilitätskomponente, den eu-LISA in Zusammenarbeit mit den Mitgliedstaaten durchzuführen hat, festgestellt;

c) eu-LISA hat die technischen und rechtlichen Vorkehrungen für die Erhebung und Übermittlung der Daten nach Artikel 8 Absatz 1 sowie den Artikeln 13, 19, 34 und 39 validiert und der Kommission mitgeteilt;

d) die Mitgliedstaaten haben ihre Mitteilungen an die Kommission gemäß Artikel 61 Absatz 1 getätigt;

e) bezüglich des MID hat die ETIAS-Zentralstelle ihre Mitteilung an die Kommission gemäß Artikel 61 Absatz 3 getätigt.

(2) Die Kommission unterrichtet das Europäische Parlament und den Rat über die Ergebnisse des gemäß Absatz 1 Buchstabe b durchgeführten Tests.

(3) Der Beschluss der Kommission gemäß Absatz 1 wird im *Amtsblatt der Europäischen Union* veröffentlicht.

(4) Die Mitgliedstaaten und Europol beginnen mit der Nutzung der Interoperabilitätskomponenten ab dem von der Kommission gemäß Absatz 1 festgelegten Zeitpunkt.

Artikel 63
Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 8 Absatz 2 und Artikel 9 Absatz 7 wird der Kommission auf unbestimmte Zeit ab [*Datum des Inkrafttretens dieser Verordnung*] übertragen.

(3) Die Befugnisübertragung gemäß Artikel 8 Absatz 2 und Artikel 9 Absatz 7 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss genannten Befugnisse. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen

späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der Interinstitutionellen Vereinbarung über bessere Rechtsetzung vom 13. April 2016 festgelegten Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 8 Absatz 2 und Artikel 9 Absatz 7 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von [zwei Monaten] nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um [zwei Monate] verlängert.

Artikel 64
Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

Artikel 65
Beratergruppe

eu-LISA setzt eine Beratergruppe ein, die ihr mit Fachkenntnissen auf dem Gebiet der Interoperabilität insbesondere bei der Vorbereitung ihres Jahresarbeitsprogramms und ihres Jahrestätigkeitsberichts zur Seite steht. Während der Konzept- und Entwicklungsphase der Interoperabilitätsinstrumente findet Artikel 52 Absätze 4 bis 6 Anwendung.

Artikel 66
Schulung

eu-LISA nimmt Aufgaben im Zusammenhang mit Schulungen in der technischen Nutzung der Interoperabilitätskomponenten gemäß der Verordnung (EU) Nr. 1077/2011 wahr.

Artikel 67
Handbuch

Die Kommission stellt in enger Zusammenarbeit mit den Mitgliedstaaten, eu-LISA und anderen zuständigen Agenturen ein Handbuch für die Umsetzung und den Betrieb der Interoperabilitätskomponenten zur Verfügung. Das Handbuch enthält technische und operative Leitlinien, Empfehlungen und bewährte Verfahren. Die Kommission nimmt dieses Handbuch in Form einer Empfehlung an.

Artikel 68
Überwachung und Bewertung

(1) eu-LISA stellt sicher, dass geeignete Verfahren für die Überwachung der Entwicklung der Interoperabilitätskomponenten anhand von Zielen in Bezug auf Planung und Kosten sowie für die Überwachung der Funktionsweise der Interoperabilitätskomponenten anhand von Zielen in Bezug auf die technische Leistung, Kostenwirksamkeit, Sicherheit und Dienstleistungsqualität vorhanden sind.

(2) Bis zum [*sechs Monate nach Inkrafttreten dieser Verordnung* — bitte Datum einfügen] und danach alle sechs Monate während der Entwicklungsphase der Interoperabilitätskomponenten übermittelt eu-LISA dem Europäischen Parlament und dem Rat einen Bericht über den Stand der Entwicklung der Interoperabilitätskomponenten. Sobald die Entwicklung abgeschlossen ist, wird dem Europäischen Parlament und dem Rat ein Bericht übermittelt, in dem detailliert dargelegt wird, wie die Ziele, insbesondere in Bezug auf die Planung und die Kosten, erreicht wurden, und in dem etwaige Abweichungen begründet werden.

(3) Zum Zwecke der technischen Wartung hat eu-LISA Zugang zu den erforderlichen Informationen über die Datenverarbeitungsvorgänge in den Interoperabilitätskomponenten.

(4) Vier Jahre nach Inbetriebnahme der einzelnen Interoperabilitätskomponenten und danach alle vier Jahre übermittelt eu-LISA dem Europäischen Parlament, dem Rat und der Kommission einen Bericht über die technische Funktionsweise der Interoperabilitätskomponenten einschließlich der Sicherheit des Systems.

(5) Ferner erstellt die Kommission ein Jahr nach jedem Bericht von eu-LISA eine Gesamtbewertung der Komponenten, die Folgendes beinhaltet:

a) eine Beurteilung der Anwendung dieser Verordnung;

b) eine Analyse der Ergebnisse, gemessen an den Zielen, und der Auswirkungen auf die Grundrechte;

c) eine Beurteilung, ob die grundlegenden Prinzipien der Interoperabilitätskomponenten weiterhin Gültigkeit haben;

d) eine Beurteilung der Sicherheit der Interoperabilitätskomponenten;

e) eine Beurteilung etwaiger Auswirkungen, auch etwaiger unverhältnismäßiger Auswirkungen auf den Verkehrsfluss an den Grenzübergangsstellen, und der Auswirkungen auf den Haushalt der Union.

Die Bewertungen schließen erforderlichenfalls Empfehlungen ein. Die Kommission übermittelt den Bewertungsbericht dem Europäischen Parlament, dem Rat, dem Europäischen Datenschutzbeauftragten und der durch die Verordnung (EG) Nr. 168/2007 des Rates[65] eingerichteten Agentur der Europäischen Union für Grundrechte.

(6) Die Mitgliedstaaten und Europol stellen eu-LISA und der Kommission die für die Ausarbeitung der Berichte nach den Absätzen 4 und 5 erforderlichen Informationen zur Verfügung. Diese Informationen dürfen nicht zu einer Beeinträchtigung der Arbeitsverfahren führen oder Angaben enthalten, die Rückschlüsse auf Quellen, Bedienstete oder Ermittlungen der benannten Behörden ermöglichen.

[65] Verordnung (EG) Nr. 168/2007 des Rates vom 15. Februar 2007 zur Errichtung einer Agentur der Europäischen Union für Grundrechte (ABl. L 53 vom 22.2.2007, S. 1).

(7) eu-LISA stellt der Kommission die Informationen zur Verfügung, die zur Durchführung der in Absatz 5 genannten Bewertungen erforderlich sind.

(8) Die Mitgliedstaaten und Europol erstellen unter Einhaltung der nationalen Rechtsvorschriften über die Veröffentlichung von sensiblen Informationen Jahresberichte über die Wirksamkeit des Zugangs zu im CIR gespeicherten Daten für Strafverfolgungszwecke; diese Berichte enthalten Informationen und Statistiken über

a) den genauen Zweck der Abfrage, einschließlich über die Art der terroristischen oder sonstigen schweren Straftat;

b) hinreichende Anhaltspunkte für den begründeten Verdacht, dass der Verdächtige, der Täter oder das Opfer unter die Eurodac-Verordnung fällt;

c) die Zahl der Anträge auf Zugang zum CIR zu Strafverfolgungszwecken;

d) die Zahl und die Art von Fällen, in denen die Identität einer Person festgestellt werden konnte;

e) die Notwendigkeit und die Anwendung des Dringlichkeitsverfahrens in Ausnahmefällen, darunter in Fällen, in denen bei der nachträglichen Überprüfung durch die zentrale Zugangsstelle festgestellt wurde, dass das Dringlichkeitsverfahren nicht gerechtfertigt war.

Die Jahresberichte der Mitgliedstaaten und von Europol werden der Kommission bis zum 30. Juni des Folgejahres vorgelegt.

Artikel 69
Inkrafttreten und Anwendbarkeit

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt gemäß den Verträgen unmittelbar in den Mitgliedstaaten.

Geschehen zu Straßburg am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

1.2. Politikbereich(e)

1.3. Art des Vorschlags/der Initiative

1.4. Ziel(e)

1.5. Begründung des Vorschlags/der Initiative

1.6. Laufzeit der Maßnahme und Dauer ihrer finanziellen Auswirkungen

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung

2. VERWALTUNGSMASSNAHMEN

2.1. Monitoring und Berichterstattung

2.2. Verwaltungs- und Kontrollsystem

2.3. Prävention von Betrug und Unregelmäßigkeiten

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des mehrjährigen Finanzrahmens und Ausgabenlinie(n)

3.2. Geschätzte Auswirkungen auf die Ausgaben

3.2.1. Übersicht

3.2.2. Geschätzte Auswirkungen auf die operativen Mittel

3.2.3. Geschätzte Auswirkungen auf die Verwaltungsmittel

3.2.4. Vereinbarkeit mit dem mehrjährigen Finanzrahmen

3.2.5. Finanzierungsbeteiligung Dritter

3.3. Geschätzte Auswirkungen auf die Einnahmen

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung

1.2. Politikbereich(e)

Inneres (Titel 18)

1.3. Art des Vorschlags/der Initiative

X Der Vorschlag/Die Initiative betrifft **eine neue Maßnahme**

☐ Der Vorschlag/Die Initiative betrifft **eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**[66]

☐ Der Vorschlag/Die Initiative betrifft **die Verlängerung einer bestehenden Maßnahme**

☐ Der Vorschlag/Die Initiative betrifft **eine neu ausgerichtete Maßnahme**

1.4. Ziel(e)

1.4.1. Mit dem Vorschlag/der Initiative verfolgte mehrjährige strategische Ziele der Kommission

Grenzmanagement – Menschenleben retten und Außengrenzen sichern

Die Interoperabilitätskomponenten schaffen die Voraussetzungen für eine bessere Nutzung der in den bestehenden EU-Systemen in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung vorhandenen Informationen. Hauptsächlich wird durch diese Maßnahmen vermieden, dass ein und dieselbe Person in unterschiedlichen Systemen mit unterschiedlichen Identitäten erfasst ist. Derzeit ist die eindeutige Identifizierung einer Person innerhalb eines Systems möglich, jedoch nicht systemübergreifend. Dies kann zu Fehlentscheidungen von Behörden führen oder von Mala-fide-Reisenden zur Verschleierung ihrer tatsächlichen Identität genutzt werden.

Besserer Informationsaustausch

Die vorgeschlagenen Maßnahmen sehen auch einen vereinfachten, aber begrenzten Zugang der Strafverfolgungsbehörden zu diesen Daten vor. Für den Zugriff auf die einzelnen Datensammlungen werden jedoch im Gegensatz zum aktuellen Zustand einheitliche Bedingungen gelten.

1.4.2. Einzelziel(e) und Einzelziel Nr. [ ]

Mit der Einrichtung der Interoperabilitätskomponenten werden folgende allgemeine Ziele verfolgt:

[66] Im Sinne des Artikels 54 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

a) Verbesserung des Außengrenzenmanagements,

b) Beitrag zur Verhütung und Bekämpfung irregulärer Migration und

c) Gewährleistung eines hohen Maßes an Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts der Union einschließlich der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie des Schutzes der inneren Sicherheit im Hoheitsgebiet der Mitgliedstaaten.

Diese Ziele sollen durch folgende Maßnahmen erreicht werden:

a) Sicherstellung der korrekten Identifizierung von Personen,

b) Beitrag zur Bekämpfung von Identitätsbetrug,

c) Verbesserung und Harmonisierung der Datenqualitätsanforderungen der einzelnen Informationssysteme der EU,

d) Erleichterung der technischen und der operativen Umsetzung bestehender und künftiger Informationssysteme der EU durch die Mitgliedstaaten,

e) Verschärfung, Vereinfachung und Vereinheitlichung der für die einzelnen Informationssysteme der EU geltenden Bedingungen für die Sicherheit und den Schutz der Daten,

f) Vereinfachung und Vereinheitlichung der Bedingungen für den Zugang von Strafverfolgungsbehörden zum EES, zum VIS, zum ETIAS und zu Eurodac,

g) Unterstützung der Zwecke des EES, des VIS, des ETIAS, von Eurodac, des SIS und des ECRIS-TCN.

ABM-/ABB-Tätigkeit(en):

Kapitel Sicherheit und Schutz der Freiheitsrechte: innere Sicherheit

1.4.3. Erwartete Ergebnisse und Auswirkungen

Bitte geben Sie an, wie sich der Vorschlag/die Initiative auf die Begünstigten/Zielgruppen auswirken dürfte.

Die allgemeinen Ziele dieses Vorschlags ergeben sich aus den folgenden beiden im Vertrag verankerten Zielen:

1. Verbesserung des Grenzmanagements an den Schengen-Außengrenzen auf der Grundlage der Europäischen Migrationsagenda und der nachfolgenden Mitteilungen, unter anderem der Mitteilung „Schengen bewahren und stärken“,

2. Beitrag zur inneren Sicherheit der Europäischen Union auf der Grundlage der Europäischen Sicherheitsagenda und der Arbeiten der Kommission im Hinblick auf eine wirksame und echte Sicherheitsunion.

Spezifische politische Ziele dieser Interoperabilitätsinitiative:

Die Einzelziele dieses Vorschlags lauten:

1. Gewährleistung, dass die Endnutzer, insbesondere Grenzschutz- und Strafverfolgungsbeamte sowie Mitarbeiter von Einwanderungs- und Justizbehörden, einen raschen, unterbrechungsfreien, systematischen und kontrollierten Zugang zu den Informationen haben, die sie benötigen, um ihren Aufgaben nachzukommen,

2. Bereitstellung einer Lösung für die Aufdeckung von Mehrfachidentitäten, die mit ein und demselben Satz biometrischer Daten verknüpft sind, um zugleich eine korrekte Identifizierung von Bona-fide-Reisenden sicherzustellen und Identitätsbetrug zu bekämpfen,

3. Vereinfachung der Identitätsprüfung von Drittstaatsangehörigen im Hoheitsgebiet eines Mitgliedstaats durch Polizeibehörden und

4. Erleichterung und einheitliche Regelung des Zugangs der Strafverfolgungsbehörden zu den Informationssystemen anderer Behörden auf EU-Ebene, wenn dies für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung terroristischer und sonstiger schwerer Straftaten notwendig ist.

Damit das Einzelziel Nr. 1 erreicht wird, wird das Europäische Suchportal (ESP) entwickelt.

Damit das Einzelziel Nr. 2 erreicht wird, wird der Detektor für Mehrfachidentitäten (MID) eingerichtet, der durch den gemeinsamen Speicher für Identitätsdaten (CIR) und den gemeinsamen Dienst für den Abgleich biometrischer Daten (gemeinsamer BMS) unterstützt wird.

Damit das Einzelziel Nr. 3 erreicht wird, erhalten entsprechend befugte Beamte zu Identifizierungszwecken Zugang zum CIR.

Damit das Einzelziel Nr. 4 erreicht wird, enthält der CIR eine Trefferkennzeichnungsfunktion, die ein zweistufiges Verfahren für den Zugang der Strafverfolgungsbehörden zu Grenzmanagementsystemen ermöglicht.

Die in Abschnitt 1.4.2 beschriebenen Ziele werden nicht nur durch diese vier Interoperabilitätskomponenten unterstützt, sondern auch durch die Einführung und Regelung des universellen Nachrichtenformats (Universal Message Format – UMF) als EU-Standard für die Entwicklung von Informationssystemen im Bereich Justiz und Inneres sowie durch die Einrichtung eines zentralen Speichers für Berichte und Statistiken (CRRS).

1.4.4. Leistungs- und Erfolgsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren sich die Realisierung des Vorschlags/der Initiative verfolgen lässt.

Die vorgeschlagenen Maßnahmen erfordern die Entwicklung sowie anschließend die Wartung und den Betrieb der jeweiligen Komponente.

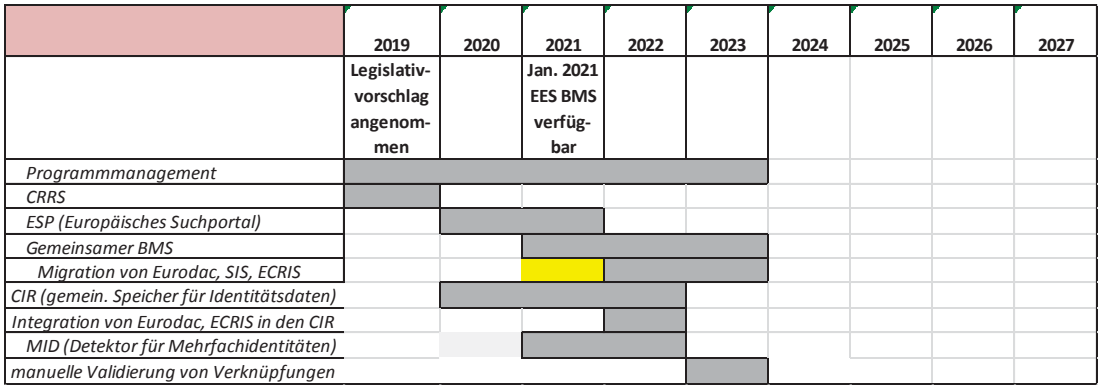
Entwicklungsphase

Die einzelnen Komponenten werden entwickelt, sobald die Voraussetzungen erfüllt sind, d. h. der Vorschlag für einen Rechtsakt wurde von den beiden gesetzgebenden Organen angenommen und die technischen Voraussetzungen sind erfüllt (einige Komponenten können erst eingerichtet werden, wenn eine andere Komponente verfügbar ist).

Einzelziel: Betriebsbereitschaft zum angestrebten Termin

Bis Ende 2017 wird der Vorschlag den gesetzgebenden Organen zur Annahme übermittelt. Es wird davon ausgegangen, dass die Annahme in etwa so viel Zeit wie bei anderen Vorschlägen auch erfordern und mithin noch im Laufe des Jahres 2018 erfolgen wird.

Aufgrund dieser Annahme wird als Beginn der Entwicklungsphase der Beginn des Jahres 2019 (= T0) festgelegt, um einen Bezugspunkt zu haben, ab dem Zeiträume und nicht konkrete Daten angegeben werden. Erfolgt die Annahme durch die beiden gesetzgebenden Organe zu einem späteren Zeitpunkt, verschiebt sich der gesamte Zeitplan entsprechend. Andererseits muss der gemeinsame BMS verfügbar sein, bevor der CIR und der MID abgeschlossen werden können. Die Zeitpläne für die Entwicklung sind in der nachstehenden Tabelle dargestellt:



(Das gelbe Feld bezieht sich auf eine bestimmte Aufgabe im Zusammenhang mit Eurodac.)

- zentraler Speicher für Berichte und Statistiken (CRRS): Fertigstellungstermin: T0 + 12 Monate (2019-2020)

- Europäisches Suchportal (ESP): Fertigstellungstermin: T0 + 36 Monate (2019-2021)

- Der gemeinsame Dienst für den Abgleich biometrischer Daten (gemeinsamer BMS) wird zunächst für das Einreise-/Ausreisesystem (EES) errichtet. Wenn dieses Etappenziel erreicht wird, müssen die Anwendungen, die den gemeinsamen BMS nutzen sollen, aktualisiert und die Daten in den automatisierten Fingerabdruck-Identifizierungssystemen (AFIS) des SIS und von Eurodac sowie die Daten des

ECRIS-TCN in den gemeinsamen BMS migriert werden. Der Termin für die Fertigstellung ist Ende 2023.

- Die Errichtung des gemeinsamen Speichers für Identitätsdaten (CIR) erfolgt bereits während der Implementierung des EES. Nach Fertigstellung des EES werden die Daten aus Eurodac und dem ECRIS in den CIR eingebunden. Der Termin für die Fertigstellung ist Ende 2022 (Verfügbarkeit des gemeinsamen BMS + 12 Monate).

- Der Detektor für Mehrfachidentitäten (MID) wird errichtet, sobald der CIR betriebsbereit ist. Der Termin für die Fertigstellung ist Ende 2022 (Verfügbarkeit des gemeinsamen BMS + 24 Monate), doch anschließend werden sämtliche vom MID angezeigten Verknüpfungen zwischen Identitäten validiert werden müssen, was sehr ressourcenaufwendig ist, weil jede einzelne Verknüpfung manuell validiert werden muss. Dies wird bis Ende 2023 dauern.

Die Betriebsphase beginnt, sobald die oben genannte Entwicklungsphase abgeschlossen ist.

Betrieb

Die Indikatoren für die einzelnen in Abschnitt 1.4.3 genannten Einzelziele sind folgende:

1. Einzelziel: rascher, unterbrechungsfreier und systematischer Zugang zu zulässigen Datenquellen

- Zahl der durchgeführten Vorgänge (Zahl der vom ESP verarbeiteten Abfragen) je Zeitraum;

- Zahl der vom ESP verarbeiteten Abfragen im Vergleich zur Gesamtzahl der Abfragen (über das ESP und direkt an die Systeme) je Zeitraum.

2. Einzelziel: Aufdeckung von Mehrfachidentitäten

- Zahl der mit ein und demselben Satz biometrischer Daten verknüpften Identitäten im Vergleich zur Zahl der Identitäten mit biografischen Angaben je Zeitraum;

- Zahl der ermittelten Fälle von Identitätsbetrug im Vergleich zur Zahl der verknüpften Identitäten und zur Gesamtzahl der Identitäten je Zeitraum.

3. Einzelziel: einfachere Identifizierung von Drittstaatsangehörigen

- Zahl der durchgeführten Identifizierungskontrollen im Vergleich zur Gesamtzahl der Vorgänge je Zeitraum.

4. Einzelziel: Vereinfachung des Zugangs zu zulässigen Datenquellen zu Strafverfolgungszwecken

- Zahl der „Stufe 1“-Zugriffe (Abfrage, ob Daten vorliegen) zu Strafverfolgungszwecken je Zeitraum;

- Zahl der „Stufe 2“-Zugriffe (tatsächliche Einsichtnahme in Daten aus Informationssystemen der EU im zulässigen Rahmen) zu Strafverfolgungszwecken je Zeitraum.

5. Übergreifendes zusätzliches Ziel: Verbesserung der Datenqualität und der Nutzung von Daten für eine bessere Politikgestaltung

- regelmäßige Veröffentlichung von Berichten über die Überwachung der Datenqualität.

- Zahl der Ad-hoc-Anfragen nach statistischen Angaben je Zeitraum.

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf

Wie in der diesem Vorschlag beiliegenden Folgenabschätzung dargelegt, sind die jeweiligen vorgeschlagenen Komponenten zur Herstellung der Interoperabilität notwendig:

- Zur Verwirklichung des Ziels, ermächtigten Nutzern einen raschen, unterbrechungsfreien, systematischen und kontrollierten Zugang zu den entsprechenden Informationssystemen zu ermöglichen, sollte ein Europäisches Suchportal (ESP) geschaffen werden, das sich auf einen gemeinsamen BMS stützt, damit alle Datenbanken abgedeckt werden.

- Zur Verwirklichung des Ziels, die Identitätsprüfung von Drittstaatsangehörigen im Hoheitsgebiet eines Mitgliedstaats durch dazu ermächtigte Bedienstete zu erleichtern, sollte ein gemeinsamer Speicher für Identitätsdaten (CIR) geschaffen werden, der den Mindestsatz an Identifizierungsdaten enthält und sich auf denselben gemeinsamen BMS stützt.

- Zur Verwirklichung des Ziels, Mehrfachidentitäten aufzudecken, die mit ein und demselben Satz biometrischer Daten verknüpft sind, um zugleich die Identitätsprüfung von Bona-fide-Reisenden zu vereinfachen und Identitätsbetrug zu bekämpfen, bedarf es eines Detektors für Mehrfachidentitäten (MID), der systemübergreifende Verknüpfungen zwischen Mehrfachidentitäten enthält.

- Zur Verwirklichung des Ziels, den Zugang der Strafverfolgungsbehörden zu den Informationssystemen anderer Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung terroristischer und sonstiger schwerer Straftaten zu erleichtern und einheitlich zu regeln, sollte in den CIR eine Trefferkennzeichnungsfunktion integriert werden.

Da alle Ziele erreicht werden müssen, ist die beste Lösung eine Kombination der allesamt auf den gemeinsamen BMS gestützten Komponenten ESP, CIR (mit Trefferkennzeichnung) und MID.

1.5.2. Mehrwert aufgrund des Tätigwerdens der Union (kann sich aus verschiedenen Faktoren ergeben, z. B. Vorteile durch Koordination, Rechtssicherheit, größere Wirksamkeit oder gegenseitige Ergänzungen). Im Sinne dieses Punkts ist der „Mehrwert aufgrund des Tätigwerdens der Union" der Nutzen, der sich aus dem Eingreifen der Union zusätzlich zu dem Nutzen ergibt, der ohnehin von den Mitgliedstaaten allein geschaffen worden wäre.

Maßnahmen auf europäischer Ebene sind erforderlich, da die Systeme, zwischen denen Interoperabilität hergestellt werden soll, von mehreren Mitgliedstaaten verwendet werden – sei es von allen Mitgliedstaaten (im Falle von Eurodac) oder aber von allen Mitgliedstaaten, die zum Schengen-Raum gehören (im Falle des EES, des VIS, des ETIAS und des SIS). Definitionsgemäß können Maßnahmen grundsätzlich nicht auf einer anderen Ebene ergriffen werden.

Der wichtigste erwartete Mehrwert besteht in der Beseitigung der Fälle von Identitätsbetrug, in der Erstellung einer Übersicht der Fälle, in denen eine Person verschiedene Identitäten genutzt hat, um in die EU zu gelangen, und in der

Vermeidung von Verwechslungen zwischen Bona-fide- und Mala-fide-Reisenden mit demselben Namen. Ein zusätzlicher Mehrwert besteht darin, dass die hier vorgeschlagene Interoperabilität die Implementierung und Wartung von IT-Großsystemen der EU erleichtert. Für die Strafverfolgungsbehörden dürften die vorgeschlagenen Maßnahmen zu häufigeren und erfolgreicheren Zugriffen auf spezifische Daten in IT-Großsystemen der EU führen. Auf operativer Ebene kann die Datenqualität nur aufrechterhalten und verbessert werden, wenn sie überwacht wird. Für die Politikgestaltung und Entscheidungsfindung ist es zudem notwendig, dass Ad-hoc-Abfragen anonymisierter Daten ermöglicht werden.

Teil der Folgenabschätzung ist eine Kosten-Nutzen-Analyse, die ausschließlich die quantifizierbaren Vorteile berücksichtigt und der zufolge die voraussichtlichen Vorteile nach vernünftigem Ermessen schätzungsweise 77,5 Mio. EUR pro Jahr betragen, die hauptsächlich den Mitgliedstaaten zugutekommen. Diese Vorteile ergeben sich im Wesentlichen aus

- geringeren Kosten für Änderungen an nationalen Anwendungen, sobald das Zentralsystem betriebsbereit ist (schätzungsweise 6 Mio. EUR pro Jahr für die IT-Abteilungen der betreffenden Stellen der Mitgliedstaaten);

- Kosteneinsparungen infolge der Nutzung eines zentralen gemeinsamen BMS statt eines BMS je Zentralsystem mit biometrischen Daten (schätzungsweise 1,5 Mio. EUR pro Jahr und einmalige Einsparung von 8 Mio. EUR für eu-LISA);

- Einsparungen bei den Kosten für die Aufdeckung von Mehrfachidentitäten im Vergleich zu einer Situation, in der das gleiche Ergebnis ohne die vorgeschlagenen Mittel erreicht würde. Dies entspräche einer Einsparung von mindestens 50 Mio. EUR pro Jahr für die Grenzmanagement-, Migrations- und Strafverfolgungsbehörden der Mitgliedstaaten.

- eingesparten Kosten für die Schulung einer großen Gruppe von Endnutzern im Vergleich zu einer Situation, in der wiederholte Schulungen erforderlich sind (schätzungsweise 20 Mio. EUR pro Jahr für die Grenzmanagement-, Migrations- und Strafverfolgungsbehörden der Mitgliedstaaten).

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

Die Erfahrungen mit der Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II) und des Visa-Informationssystems (VIS) haben Folgendes gezeigt:

1. Als mögliche Absicherung gegen Kostenüberschreitungen und Verzögerungen, die auf geänderte Anforderungen zurückzuführen sind, sollte jedes neue Informationssystem im Raum der Freiheit, der Sicherheit und des Rechts – vor allem, wenn es um ein IT-Großsystem geht – nicht entwickelt werden, so lange die grundlegenden Rechtsinstrumente, in denen Zweck, Anwendungsbereich, Funktion und technische Einzelheiten festgelegt sind, nicht endgültig angenommen wurden.

2. Beim SIS II und beim VIS konnten nationale Entwicklungen der Mitgliedstaaten im Rahmen des Außengrenzenfonds kofinanziert werden, doch war dies nicht zwingend erforderlich. Folglich war es nicht möglich, sich einen Überblick über die Fortschritte derjenigen Mitgliedstaaten zu verschaffen, die die jeweiligen Tätigkeiten nicht in ihrer Mehrjahresplanung vorgesehen hatten oder deren Planung nicht präzise genug war. Daher wird nunmehr vorgeschlagen, dass die Kommission alle in den

Mitgliedstaaten entstandenen Integrationskosten erstattet, um auf diese Weise den Fortschritt bei diesen Entwicklungen überwachen zu können.

3. Zur Erleichterung der Gesamtkoordinierung der Umsetzung werden für den gesamten vorgeschlagenen Austausch von Nachrichten zwischen nationalen Systemen und dem Zentralsystemen bereits bestehende Netze und die einheitlichen nationalen Schnittstellen verwendet.

1.5.4. Vereinbarkeit mit anderen Finanzierungsinstrumenten sowie mögliche Synergieeffekte

Vereinbarkeit mit dem derzeitigen mehrjährigen Finanzrahmen

Die Verordnung über den Fonds für die innere Sicherheit (ISF) – Grenzen ist das Finanzierungsinstrument, das die Mittel für die Umsetzung der Interoperabilitätsinitiative enthält.

Artikel 5 Absatz 5 Buchstabe b der genannten Verordnung sieht vor, dass 791 Mio. EUR im Wege eines Programms für die Entwicklung von auf bestehenden und/oder neuen IT-Systemen basierenden IT-Systemen zur Unterstützung der Steuerung von Migrationsströmen über die Außengrenzen verwendet werden, sofern die entsprechenden Rechtsakte der Union angenommen werden und die in Artikel 15 festgelegten Bedingungen erfüllt sind. Von diesen 791 Mio. EUR sind 480,2 Mio. EUR für die Entwicklung des EES, 210 Mio. EUR für das ETIAS und 67,9 Mio. EUR für die Überarbeitung des SIS II vorgesehen. Der Restbetrag (32,9 Mio. EUR) ist nach dem Verfahren des ISF – Grenzen neu zuzuweisen. Gemäß dem vorliegenden Vorschlag ist für den verbleibenden Zeitraum des derzeitigen mehrjährigen Finanzrahmens ein Betrag von 32,1 Mio. EUR erforderlich, der aus den restlichen Haushaltsmitteln gedeckt werden kann.

Insgesamt belaufen sich die während des Zeitraums von 2019 bis 2027 für diesen Vorschlag erforderlichen Haushaltsmittel auf 424,7 Mio. EUR (Rubrik 5 eingeschlossen). Der derzeitige mehrjährige Finanzrahmen (MFR) erstreckt sich nur noch auf die beiden Jahre 2019 und 2020. Ohne dem nächsten mehrjährigen Finanzrahmen vorzugreifen, wurden die Kosten jedoch bis einschließlich 2027 veranschlagt, um einen fundierten Überblick über die finanziellen Auswirkungen dieses Vorschlags zu geben.

Die für einen Zeitraum von neun Jahren beantragten Haushaltsmittel belaufen sich auf 424,7 Mio. EUR und decken auch die folgenden Posten ab:

1) 136,3 Mio. EUR für die Änderungen, die die Mitgliedstaaten im Hinblick auf die Nutzung der Interoperabilitätskomponenten an ihren nationalen Systemen vornehmen müssen, und für die von eu-LISA bereitgestellte NUI sowie ein Budget für die Schulung der zahlreichen Endnutzer. Es gibt keine Auswirkungen auf den derzeitigen MFR, da die Finanzmittel ab 2021 bereitgestellt werden.

2) 4,8 Mio. EUR für die Europäische Agentur für die Grenz- und Küstenwache für ein Team von Spezialisten, das ab Inbetriebnahme des MID während eines Jahres (2023) die Verknüpfungen zwischen Identitäten validieren soll. Die Tätigkeiten des Teams sind im Zusammenhang mit der Klärung von Identitäten zu sehen, für die die Europäische Agentur für die Grenz- und Küstenwache nach dem ETIAS-Vorschlag zuständig ist. Es gibt keine Auswirkungen auf den derzeitigen MFR, da die Finanzmittel ab 2021 bereitgestellt werden.

3) 48,9 Mio. EUR für Europol für die Modernisierung der IT-Systeme von Europol im Hinblick auf die Menge der zu verarbeitenden Mitteilungen und die höheren Leistungsniveaus. Die Interoperabilitätskomponenten werden vom ETIAS für die Abfrage der Europol-Daten genutzt. Die derzeitige Informationsverarbeitungskapazität von Europol ist jedoch nicht vereinbar mit den erwarteten beträchtlichen Mengen an Abfragen (durchschnittlich 100 000 täglich) und der künftig erforderlichen verkürzten Reaktionszeit. Auf der Grundlage des derzeitigen MFR werden hierfür 9,1 Mio. EUR verwendet.

4) 2,0 Mio. EUR für die Agentur CEPOL für die Ausarbeitung und Durchführung von Schulungen für das Betriebspersonal. Für das Jahr 2020 sind 0,1 Mio. EUR vorgesehen.

5) 225,0 Mio. EUR für eu-LISA, die Folgendes abdecken: die Gesamtkosten für die Entwicklung des Programms zur Bereitstellung der fünf Interoperabilitätskomponenten (68,3 Mio. EUR), die Wartungskosten ab dem Zeitpunkt der Bereitstellung der Komponenten bis zum Jahr 2027 (56,1 Mio. EUR), ein spezielles Budget von 25,0 Mio. EUR für die Migration der Daten aus den bestehenden Systemen in den gemeinsamen BMS und die zusätzlichen Kosten für die Aktualisierung der NUI, für das Netz sowie für Schulungen und Sitzungen. Ein spezielles Budget von 18,7 Mio. EUR deckt die Kosten für die Modernisierung des ECRIS-TCN und dessen ab 2022 vorgesehenen Betrieb im Hochverfügbarkeitsmodus. 23,0 Mio. EUR des Gesamtbetrags werden während der Laufzeit des derzeitigen MFR verwendet.

6) 7,7 Mio. EUR für die GD HOME für eine begrenzte Personalaufstockung und zur Deckung der Kosten, die während des Zeitraums anfallen, in dem die verschiedenen Komponenten entwickelt werden, da die Kommission auch für den mit dem einheitlichen Nachrichtenformat (UMF) befassten Ausschuss verantwortlich sein wird. Diese unter die Rubrik 5 fallenden Mittel sind nicht aus dem ISF-Haushalt zu decken. Informationshalber sei darauf hingewiesen, dass 2,0 Mio. EUR im Zeitraum 2019-2020 fällig sind.

Vereinbarkeit mit früheren Initiativen

Diese Initiative ist vereinbar mit folgendem Vorgehen:

Im April 2016 legte die Kommission die **Mitteilung *Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit*** vor, in der einige strukturelle Mängel der Informationssysteme aufgezeigt wurden. Daraus haben sich drei konkrete Maßnahmen ergeben:

Erstens wurde die Kommission **tätig, um den Nutzen der bestehenden Informationssysteme zu erhöhen und zu maximieren**. Im Dezember 2016 nahm sie Vorschläge zur weiteren Stärkung des bestehenden Schengener Informationssystems (SIS) an. Nach der Vorlage des Kommissionsvorschlags vom Mai 2016 wurden die Verhandlungen über die überarbeitete Rechtsgrundlage für Eurodac – die EU-Datenbank zum Abgleich der Fingerabdrücke von Asylbewerbern – beschleunigt. Ein Vorschlag für eine neue Rechtsgrundlage für das Visa-Informationssystem (VIS) wird ebenfalls ausgearbeitet und soll im zweiten Quartal 2018 vorgelegt werden.

Zweitens schlug die Kommission **zusätzliche Informationssysteme zur Schließung der Informationslücken** vor, die in der Datenverwaltungsarchitektur der EU festgestellt wurden. Die Verhandlungen über den Kommissionsvorschlag vom April

2016 über ein Einreise-/Ausreisesystem (EES)[67] – zur Verbesserung der Verfahren für die Grenzübertrittskontrollen von in die EU reisenden Drittstaatsangehörigen – wurden bereits im Juli 2017 abgeschlossen, als die beiden gesetzgebenden Organe eine politische Einigung erzielten, die im Oktober 2017 vom Europäischen Parlament bestätigt und im November 2017 vom Rat förmlich angenommen wurde. Im November 2016 unterbreitete die Kommission außerdem einen Vorschlag über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS)[68]. Ziel dieses Vorschlags ist es, die Sicherheitskontrollen von nicht visumpflichtigen Reisenden zu verschärfen, indem ermöglicht wird, vorab Kontrollen zu irregulärer Migration und Sicherheitskontrollen vorzunehmen. Derzeit verhandeln die beiden gesetzgebenden Organe über diesen Vorschlag. Im Juni 2017 wurde zudem das Europäische Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN)[69] vorgeschlagen, um die Lücke zu schließen, die in Bezug auf den Informationsaustausch der Mitgliedstaaten über verurteilte Drittstaatsangehörige festgestellt worden war.

Drittens arbeitete die Kommission auf die **Interoperabilität der Informationssysteme** hin und befasste sich dabei schwerpunktmäßig mit den vier Optionen, die in der Mitteilung vom April 2016[70] zur Herstellung der Interoperabilität dargelegt worden waren. Drei der vier Optionen sind das ESP, der CIR und der gemeinsame BMS. Wie sich anschließend herausstellte, musste zwischen dem CIR als Identitätsdatenbank und einer neuen Komponente unterschieden werden, die mit demselben biometrischen Identifikator verknüpfte Mehrfachidentitäten ermittelt (MID). Die vier Komponenten sind also nun: das ESP, der CIR, der MID und der gemeinsame BMS.

Synergieeffekte

Synergieeffekte sind hier als der Nutzen zu verstehen, der durch die Wiederverwendung bestehender Lösungen unter Vermeidung neuer Investitionen erzielt wird.

Erhebliche Synergieeffekte ergeben sich zwischen dieser Initiative und der Entwicklung des EES und des ETIAS.

Für das EES wird eine individuelle Datei für alle Drittstaatsangehörigen angelegt, die für einen Kurzaufenthalt in den Schengen-Raum einreisen. Zu diesem Zweck wird das derzeit für das VIS verwendete System für den Abgleich biometrischer Daten, das die Fingerabdruck-Templates für alle visumpflichtigen Reisenden enthält, dahin gehend erweitert, dass auch die biometrischen Daten von nicht visumpflichtigen Reisenden erfasst werden können. Der gemeinsame BMS stellt somit von seiner Konzeption her eine weitere Generalisierung des Systems für den Abgleich biometrischer Daten dar, das im Rahmen des EES errichtet wird. Die biometrischen Templates, die im System für den Abgleich biometrischer Daten des SIS und von Eurodac enthalten sind, werden in den gemeinsamen BMS „migriert“ (Fachbegriff für die Übertragung von Daten von einem System in ein anderes). Nach Angaben von Lieferanten belaufen sich die Kosten für die Speicherung in gesonderten Datenbanken auf durchschnittlich 1 EUR je Satz biometrischer Daten (insgesamt dürften 200 Millionen Datensätze vorhanden sein), wohingegen die

67 COM(2016) 194 vom 6. April 2016.
68 COM(2016) 731 vom 16. November 2016.
69 COM(2017) 344 vom 29. Juni 2017.
70 COM(2016) 205 vom 6. April 2016.

durchschnittlichen Kosten auf 0,35 EUR je Satz biometrischer Daten sinken werden, wenn ein gemeinsamer BMS eingerichtet wird. Die höheren Kosten der für ein großes Datenvolumen erforderlichen Hardware machen diesen Vorteil teilweise zunichte. Dennoch werden die Kosten eines gemeinsamen BMS Schätzungen zufolge letztlich um 30 % unter den Kosten liegen, die anfallen würden, wenn dieselben Daten in mehreren kleineren BMS-Systemen gespeichert würden.

Für das Funktionieren des ETIAS bedarf es einer Komponente für die Abfrage einer Reihe von EU-Systemen. Entweder wird hierfür das ESP genutzt oder eine bestimmte Komponente wird im Rahmen des ESP-Vorschlags errichtet. Nach dem Interoperabilitätsvorschlag ist die Verwendung einer einzigen Komponente anstelle von zweien möglich.

Weitere Synergieeffekte lassen sich durch die Wiederverwendung der für das EES und das ETIAS genutzten einheitlichen nationalen Schnittstelle (NUI) erzielen. Die NUI wird zwar aktualisiert werden müssen, kann aber weiterhin verwendet werden.

1.6. Laufzeit der Maßnahme und Dauer ihrer finanziellen Auswirkungen

☐ Vorschlag/Initiative mit **befristeter Laufzeit**

– ☐ Laufzeit: [TT/MM]JJJJ bis [TT/MM]JJJJ

– ☐ Finanzielle Auswirkungen: JJJJ bis JJJJ

☒ Vorschlag/Initiative mit **unbefristeter Laufzeit**

– Entwicklungsphase von 2019 bis einschließlich 2023, anschließend Vollbetrieb.

– Die finanziellen Auswirkungen werden daher für den Zeitraum von 2019 bis 2027 angegeben.

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung[71]

☒ **Direkte Verwaltung** durch die Kommission

– X durch ihre Dienststellen, einschließlich ihres Personals in den Delegationen der Union;

– ☐ durch Exekutivagenturen.

☒ **Geteilte Verwaltung** mit Mitgliedstaaten

☒ **Indirekte Verwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:

– ☐ Drittländer oder die von ihnen benannten Einrichtungen;

– ☐ internationale Einrichtungen und deren Agenturen (bitte angeben);

– ☐ die EIB und den Europäischen Investitionsfonds;

– ☒ Einrichtungen im Sinne der Artikel 208 und 209 der Haushaltsordnung;

– ☐ öffentlich-rechtliche Körperschaften;

– ☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern sie ausreichende Finanzsicherheiten bieten;

– ☐ privatrechtliche Einrichtungen eines Mitgliedstaats, die mit der Einrichtung einer öffentlich-privaten Partnerschaft betraut werden und die ausreichende Finanzsicherheiten bieten;

– ☐ Personen, die mit der Durchführung bestimmter Maßnahmen im Bereich der GASP im Rahmen des Titels V EUV betraut und in dem maßgeblichen Basisrechtsakt benannt sind.

– *Falls mehrere Methoden der Mittelverwaltung angegeben werden, ist dies unter „Bemerkungen" näher zu erläutern.*

Bemerkungen

Maßnahmenbündel	Entwicklungs-phase	Betriebsphase	Methode der Mittelver-waltung	Akteur
Entwicklung und Wartung (der Interoperabilitäts-	X	X	indirekt	eu-LISA Europol

[71] Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb (in französischer und englischer Sprache): https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

Maßnahmenbündel	Entwicklungs-phase	Betriebsphase	Methode der Mittelver-waltung	Akteur
komponenten für die Zentralsysteme, Systemschulungen)				CEPOL
Datenmigration (Übertragung biometrischer Templates in den gemeinsamen BMS), Netzkosten, Aktualisierung der NUI, Sitzungen und Schulungen	X	X	indirekt	eu-LISA
Validierung der Verknüpfungen bei Einrichtung des MID	X	-	indirekt	Europäische Grenz- und Küstenwache
Anpassung der NUI, Integration nationaler Systeme und Schulung der Endnutzer	X	X	geteilt (oder direkt) (1)	Kommission + Mitglied-staaten

(1) Für die in diesem Instrument vorgesehene Betriebsphase werden keine Beträge angegeben.

Die Entwicklungsphase beginnt 2019 und dauert bis zur Bereitstellung der einzelnen Komponenten im Zeitraum von 2019 bis 2023 (siehe Abschnitt 1.4.4).

1. Direkte Mittelverwaltung durch die GD HOME: Während der Entwicklungsphase können erforderlichenfalls auch Maßnahmen direkt von der Kommission durchgeführt werden. Dazu könnten insbesondere eine finanzielle Unterstützung der Union für Tätigkeiten in Form von Finanzhilfen (auch für Behörden der Mitgliedstaaten) bereitgestellt, öffentliche Aufträge vergeben und/oder die für externe Sachverständige anfallenden Kosten erstattet werden.

2. Geteilte Mittelverwaltung: Während der Entwicklungsphase werden die Mitgliedstaaten ihre nationalen Systeme so anpassen müssen, dass ihr Zugang zum ESP anstatt zu den einzelnen Systemen gewährleistet ist (dies betrifft die aus den Mitgliedstaaten abgehenden Mitteilungen) und dass den Änderungen bei den Antworten auf ihre Suchabfragen Rechnung getragen wird (in den Mitgliedstaaten eingehende Mitteilungen). Außerdem wird eine Aktualisierung der bestehenden, für das EES und das ETIAS implementierten NUI vorgenommen.

3. Indirekte Mittelverwaltung: Die Agentur eu-LISA wird für die Entwicklung aller IT-Teile des Projekts verantwortlich sein (d. h. für die Interoperabilitätskomponenten), für die Aktualisierung der einheitlichen nationalen Schnittstelle (NUI) in jedem Mitgliedstaat, für die Aktualisierung der Kommunikationsinfrastruktur zwischen den Zentralsystemen und den einheitlichen nationalen Schnittstellen, für die Migration der biometrischen Templates aus den bestehenden Systemen für den Abgleich biometrischer Daten des SIS und von Eurodac in den gemeinsamen BMS sowie für die damit verbundene Datenbereinigung.

Während der Betriebsphase wird eu-LISA alle technischen Tätigkeiten im Zusammenhang mit der Wartung der Komponenten ausführen.

Die Europäische Agentur für die Grenz- und Küstenwache wird ein zusätzliches Team einsetzen, das ab Inbetriebnahme des MID die Verknüpfungen validieren soll. Diese Aufgabe ist befristet.

Europol wird für die Entwicklung und Wartung seiner Systeme verantwortlich sein und für deren Interoperabilität mit dem ESP und dem ETIAS sorgen.

Die CEPOL ist für die Ausarbeitung und Durchführung von Schulungen für operative Dienste auf der Grundlage eines Konzepts für die Schulung des Schulungspersonals verantwortlich.

2. VERWALTUNGSMASSNAHMEN

2.1. Monitoring und Berichterstattung

Bitte geben Sie an, wie oft und unter welchen Bedingungen diese Tätigkeiten erfolgen.

Monitoring für die Entwicklung und Wartung anderer Systeme und diesbezügliche Berichterstattung:

1. Die Agentur eu-LISA stellt sicher, dass geeignete Verfahren für die Überwachung der Entwicklung der Interoperabilitätskomponenten anhand von Zielen in Bezug auf Planung und Kosten sowie für die Überwachung der Funktionsweise der Komponenten anhand von Zielen in Bezug auf die technische Leistung, Kostenwirksamkeit, Sicherheit und Dienstleistungsqualität vorhanden sind.

2. Innerhalb von sechs Monaten nach Inkrafttreten dieser Verordnung und danach alle sechs Monate während der Entwicklungsphase der Komponenten übermittelt eu-LISA dem Europäischen Parlament und dem Rat einen Bericht über den Stand der Entwicklung der einzelnen Komponenten. Sobald die Entwicklung abgeschlossen ist, wird dem Europäischen Parlament und dem Rat ein Bericht übermittelt, in dem detailliert dargelegt wird, wie die Ziele, insbesondere in Bezug auf die Planung und die Kosten, erreicht wurden, und in dem etwaige Abweichungen begründet werden.

3. Zum Zwecke der technischen Wartung erhält eu-LISA Zugang zu den erforderlichen Informationen über die Datenverarbeitungsvorgänge in den Komponenten.

4. Vier Jahre nach Inbetriebnahme der letzten implementierten Komponente und danach alle vier Jahre übermittelt eu-LISA dem Europäischen Parlament, dem Rat und der Kommission einen Bericht über die technische Funktionsweise der Komponenten.

5. Fünf Jahre nach Inbetriebnahme der letzten implementierten Komponente und danach alle vier Jahre erstellt die Kommission eine Gesamtbewertung und gibt erforderlichenfalls Empfehlungen ab. Diese Gesamtbewertung beinhaltet die durch die Komponenten erzielten Ergebnisse unter Berücksichtigung der Interoperabilitätsziele, der Wartungsfreundlichkeit, der Leistung und der finanziellen Auswirkungen sowie der Auswirkungen auf die Grundrechte.

Die Kommission übermittelt den Bewertungsbericht dem Europäischen Parlament und dem Rat.

6. Die Mitgliedstaaten und Europol stellen eu-LISA und der Kommission die Informationen zur Verfügung, die für die Ausarbeitung der in den Absätzen 4 und 5 genannten Berichte im Einklang mit den von der Kommission und/oder eu-LISA zuvor festgelegten quantitativen Indikatoren erforderlich sind. Diese Informationen dürfen nicht zu einer Beeinträchtigung der Arbeitsverfahren führen oder Angaben enthalten, die Rückschlüsse auf Quellen, die Identität von Bediensteten oder Ermittlungen der benannten Behörden ermöglichen.

7. eu-LISA stellt der Kommission die Informationen zur Verfügung, die zur Durchführung der in Absatz 5 genannten Gesamtbewertung erforderlich sind.

8. Die Mitgliedstaaten und Europol erstellen unter Einhaltung der nationalen Rechtsvorschriften über die Veröffentlichung von sensiblen Informationen Jahresberichte über die Wirksamkeit des Zugangs zu EU-Systemen für Strafverfolgungszwecke; diese Berichte enthalten Informationen und Statistiken über

- den genauen Zweck der Abfrage, einschließlich über die Art der terroristischen oder sonstigen schweren Straftat;

- hinreichende Anhaltspunkte für den begründeten Verdacht, dass der Verdächtige, der Täter oder das Opfer unter diese Verordnung fällt;

- die Zahl der Anträge auf Zugang zu den Komponenten zu Strafverfolgungszwecken;

- die Zahl und die Art von Fällen, in denen die Identität einer Person festgestellt werden konnte;

- die Notwendigkeit und die Anwendung des Dringlichkeitsverfahrens in Ausnahmefällen, darunter in Fällen, in denen bei der nachträglichen Überprüfung durch die zentrale Zugangsstelle festgestellt wurde, dass das Dringlichkeitsverfahren nicht gerechtfertigt war.

Die Jahresberichte der Mitgliedstaaten und von Europol werden der Kommission bis zum 30. Juni des Folgejahres vorgelegt.

2.2. Verwaltungs- und Kontrollsystem

2.2.1. Ermittelte Risiken

Es ergeben sich Risiken im Zusammenhang mit der IT-Entwicklung von fünf Komponenten durch einen von eu-LISA verwalteten externen Auftragnehmer. Typische Projektrisiken:

1. Risiko, dass das Projekt nicht fristgemäß abgeschlossen wird;

2. Risiko, dass das Projekt nicht innerhalb der Budgetvorgaben abgeschlossen wird;

3. Risiko, dass das Projekt nicht in vollem Umfang umgesetzt wird.

Das erste Risiko fällt am meisten ins Gewicht, denn eine Überschreitung der vorgesehenen Fristen führt zu höheren Kosten, da der Zeitfaktor bei den meisten Kosten (Personalkosten, jährlich zu zahlende Lizenzgebühren usw.) eine Rolle spielt.

Diese Risiken lassen sich durch Projektmanagementtechniken, einschließlich einer Notfallplanung bei Entwicklungsprojekten und einer für die Bewältigung von Arbeitsspitzen ausreichenden Personalausstattung, abfedern. Bei der Einschätzung des Aufwands wird in der Regel von einer über den vorgesehenen Zeitraum gleichmäßig verteilten Arbeitsbelastung ausgegangen, während es in Wirklichkeit bei Projekten zu ungleichmäßigen Arbeitsbelastungen kommt, die durch höhere Ressourcenzuweisungen ausgeglichen werden.

Das Hinzuziehen eines externen Auftragnehmers bei diesen Entwicklungsarbeiten birgt mehrere Risiken in sich:

1. insbesondere das Risiko, dass der Auftragnehmer nicht genügend Ressourcen für das Projekt zuweist oder dass das von ihm konzipierte und entwickelte System nicht dem neuesten Stand entspricht;

2. das Risiko, dass Verwaltungsverfahren und -methoden für IT-Großprojekte vom Auftragnehmer nicht lückenlos befolgt und angewandt werden, um die Kosten zu senken;

3. auch das Risiko, dass der Auftragnehmer aus projektunabhängigen Gründen in finanzielle Schwierigkeiten gerät, kann nicht vollkommen ausgeschlossen werden.

Diese Risiken lassen sich mindern, indem die Aufträge auf der Grundlage strenger Qualitätskriterien vergeben sowie die Referenzen der Auftragnehmer überprüft und enge Beziehungen zu ihnen unterhalten werden. Schließlich können als letztes Mittel strenge Straf- und Kündigungsklauseln in die entsprechenden Verträge aufgenommen und erforderlichenfalls angewandt werden.

2.2.2. Angaben zum Aufbau des Systems der internen Kontrolle

Die Agentur eu-LISA soll als Exzellenzzentrum im Bereich der Entwicklung und Verwaltung von IT-Großsystemen dienen. Sie soll mit den Tätigkeiten im Zusammenhang mit der Entwicklung und dem Betrieb der verschiedenen Interoperabilitätskomponenten und mit der Wartung der einheitlichen nationalen Schnittstellen in den Mitgliedstaaten betraut werden.

Während der Entwicklungsphase werden alle Entwicklungstätigkeiten von eu-LISA ausgeführt. Das betrifft sämtliche Teile des Projekts. Die während der Entwicklung anfallenden Kosten im Zusammenhang mit der Integration der Systeme in den Mitgliedstaaten werden von der Kommission im Wege der geteilten Mittelverwaltung oder mittels Finanzhilfen abgewickelt.

In der Betriebsphase wird eu-LISA für die technische und finanzielle Verwaltung der zentral genutzten Komponenten und insbesondere für die Vergabe und Verwaltung von Aufträgen verantwortlich sein. Die Kommission wird die für die Mitgliedstaaten vorgesehenen Mittel für die Ausgaben für die nationalen Stellen über den ISF – Grenzen (nationale Programme) verwalten.

Zur Vermeidung von Verzögerungen auf nationaler Ebene ist eine effiziente Steuerung auf Ebene aller Beteiligten bereits vor Beginn der Entwicklung zu planen. Die Kommission geht davon aus, dass zu Beginn des Projekts eine interoperable Architektur festgelegt wird, die auch bei den Projekten zur Erstellung des EES und des ETIAS Anwendung findet, da im Rahmen dieser Projekte der gemeinsame BMS, der gemeinsame Speicher für Identitätsdaten und das Europäische Suchportal fertiggestellt und genutzt werden sollen. Sowohl beim EES als auch beim ETIAS sollte je ein Mitglied des Projektmanagementteams des Interoperabilitätsprojekts der Projektleitung angehören.

2.2.3. Abschätzung der Kosten und des Nutzens der Kontrollen sowie Bewertung des voraussichtlichen Fehlerrisikos

Es wurde keine Abschätzung vorgenommen, da die Kontrolle und Minderung von Risiken eine inhärente Aufgabe der Projektleitung ist.

2.3. Prävention von Betrug und Unregelmäßigkeiten

Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen vorhanden oder vorgesehen sind.

Die geplanten Maßnahmen zur Betrugsbekämpfung sind in Artikel 35 der Verordnung (EU) Nr. 1077/2011 festgelegt:

1. Zur Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen findet die Verordnung (EG) Nr. 1073/1999 Anwendung.

2. Die Agenturen treten der Interinstitutionellen Vereinbarung über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) bei und erlassen unverzüglich die für alle Beschäftigten der Agenturen geltenden einschlägigen Vorschriften.

3. Die Finanzierungsbeschlüsse sowie die sich daraus ergebenden Durchführungsvereinbarungen und -instrumente sehen ausdrücklich vor, dass der Rechnungshof und das OLAF erforderlichenfalls Vor-Ort-Kontrollen bei den Empfängern der Mittel der Agenturen und bei den verteilenden Stellen durchführen können.

Gemäß diesen Bestimmungen fasste der Verwaltungsrat der Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts am 28. Juni 2012 den Beschluss über die Bedingungen und Modalitäten der internen Untersuchungen zur Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen zum Nachteil der Interessen der Union.

Es gilt die Strategie für die Betrugsaufdeckung und -bekämpfung der GD HOME.

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

DIE GESCHÄTZTEN AUSWIRKUNGEN AUF DIE AUSGABEN UND DEN PERSONALBESTAND FÜR DAS JAHR 2021 UND DIE JAHRE DANACH IN DIESEM FINANZBOGEN DIENEN LEDIGLICH DER VERANSCHAULICHUNG UND GREIFEN NICHT DEM NÄCHSTEN MEHRJÄHRIGEN FINANZRAHMEN VOR.

3.1. Betroffene Rubrik(en) des mehrjährigen Finanzrahmens und Ausgabenlinie(n)

- Bestehende Haushaltslinien

In der Reihenfolge der Rubriken des mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Beitrag			
	Nummer [Rubrik……...……]	GM/NGM [72]	von EFTA-Ländern[73]	von Kandidaten-ländern[74]	von Drittländern	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
3	18 02 01 03 (Intelligente Grenzen)	GM	Nein	Nein	Ja	Nein
3	18 02 03 (Europäische Agentur für die Grenz- und Küstenwache - Frontex)	GM	Nein	Nein	Ja	Nein
3	18 02 04 (Europol)	GM	Nein	Nein	Nein	Nein
3	18 02 05 (CEPOL)	NGM	Nein	Nein	Nein	Nein
3	18 02 07 (Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts - eu-LISA)	GM	Nein	Nein	Ja	Nein

72 GM = getrennte Mittel / NGM = nicht getrennte Mittel.
73 EFTA: Europäische Freihandelsassoziation.
74 Kandidatenländer und gegebenenfalls potenzielle Kandidaten des Westbalkans.

3.2. Geschätzte Auswirkungen auf die Ausgaben

[Dieser Abschnitt sollte mit dem **Faltblatt über Haushaltsdaten administrativer Art** (zweites Dokument im Anhang zu diesem Finanzbericht) ausgefüllt und zu Entscheidungszwecken für dienstübergreifende Konsultationen hochgeladen werden.]

3.2.1. Übersicht

in Mio. EUR (3 Dezimalstellen)

Rubrik des mehrjährigen Finanzrahmens	3	Sicherheit und Unionsbürgerschaft

GD Home			Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**Jahr 2028**	**Ins-ges.**
• Operative Mittel													
18 02 01 03 (Intelligente Grenzen)	Verpflichtungen	(1)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Zahlungen	(2)	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300
Mittel administrativer Art, die aus Geldern spezifischer Programme finanziert werden[75]													
Nummer der Haushaltslinie		(3)											
Mittel INSGESAMT für die GD HOME	Verpflichtungen	=1+1a +3)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Zahlungen	=2+2a +3	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300

Diese Ausgaben decken folgende Kosten:

[75] Technische und/oder administrative Unterstützung und Ausgaben zur Unterstützung der Umsetzung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

– Kosten der Anpassung der einheitlichen nationalen Schnittstellen, deren Entwicklung im Rahmen des EES-Vorschlags finanziert wird, veranschlagter Betrag für die aufgrund der Änderungen an den Zentralsystemen erforderlichen Änderungen an den Systemen in den Mitgliedstaaten und veranschlagter Betrag für die Schulung der Endnutzer.

18 02 03 (Europäische Grenz- und Küstenwache)			Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGE-SAMT**
Titel 1: Personalausgaben	Verpflichtungen	(1)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
	Zahlungen	(2)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
Titel 2: Infrastruktur- und Betriebsausgaben	Verpflichtungen	(1a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
	Zahlungen	(2a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
Titel 3: Operative Ausgaben	Verpflichtungen	(3a)	0	0	0	0,183	2,200	0	0	0	0	2,383
	Zahlungen	(3b)	0	0	0	0,183	2,200	0	0	0	0	2,383
Mittel INSGESAMT für Europol	(Verpflichtungen insg. = Zahlungen insg.)	=1+1a +3a	**0**	**0**	**0**	**0,776**	**4,744**	**0,402**	**0**	**0**	**0**	**5,923**

– Die Mittel für die Europäische Grenz- und Küstenwache decken die Ausgaben für ein Team ab, das die vom MID generierten Verknüpfungen zum Datenbestand (ca. 14 Mio. Datensätze) validieren soll. Insgesamt müssen schätzungsweise 550 000 Verknüpfungen validiert werden. Das für diesen Zweck eingesetzte Team wird in das bestehende Team der Europäischen Grenz- und Küstenwache integriert, das für das ETIAS eingerichtet wurde, da beide Teams ähnliche Aufgaben haben und so die Kosten für die Einrichtung eines neuen Teams gespart werden. Das Team wird voraussichtlich im Jahr 2023 seine Tätigkeit aufnehmen. Die betreffenden Vertragsbediensteten werden bis zu drei Monate vorher eingestellt werden. Ihre Verträge werden spätestens zwei Monate nach Ende der Migrationstätigkeiten beendet werden. Ein Teil des Personalbedarfs wird voraussichtlich nicht durch Vertragsbedienstete, sondern durch Berater gedeckt werden. Dies erklärt die unter Titel 3 aufgeführten Kosten für 2023. Die Berater werden voraussichtlich einen Monat im Voraus eingestellt werden. Weitere Einzelheiten der Personalzusammensetzung werden zu einem späteren Zeitpunkt bekannt gegeben.

– Titel 1 umfasst mithin die Kosten für 20 interne Bedienstete sowie für die Aufstockung des Führungs- und des Unterstützungspersonals.

– Titel 2 umfasst die zusätzlichen Kosten für die Unterbringung der 10 zusätzlichen Mitarbeiter des Auftragnehmers.

– Titel 3 umfasst die Vergütungen für die 10 zusätzlichen Mitarbeiter des Auftragnehmers. Sonstige Kosten sind nicht berücksichtigt.

18 02 04 (Europol)			Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGE-SAMT**
Titel 1: Personalausgaben	Verpflichtungen	(1)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
	Zahlungen	(2)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
Titel 2: Infrastruktur- und Betriebsausgaben	Verpflichtungen	(1a)	0	0	0	0	0	0	0	0	0	0
	Zahlungen	(2a)	0	0	0	0	0	0	0	0	0	0
Titel 3: Operative Ausgaben	Verpflichtungen	(3a)	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
	Zahlungen	(3b)	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
Mittel INSGESAMT für Europol	(Verpflichtungen insg. = Zahlungen insg.)	=1+1a +3a	0,690	8,382	8,382	3,589	3,589	3,382	8,732	8,732	3,382	48,860

Die Ausgaben von Europol decken die Modernisierung der IT-Systeme von Europol zur Bewältigung der Menge der zu verarbeitenden Mitteilungen und zur Erreichung des erforderlichen höheren Leistungsniveaus (kürzere Reaktionszeiten) ab.

Die Personalausgaben unter Titel 1 decken die Kosten für zusätzliches IKT-Personal ab, das eingestellt werden soll, um die Kapazitäten der Informationssysteme von Europol aus den obigen Gründen zu verstärken. Nähere Einzelheiten der Stellenaufteilung nach Zeitbediensteten und Vertragsbediensteten sowie der nötigen Fachkenntnisse dieser Bediensteten siehe unten.

Titel 3 umfasst die Kosten der für den Ausbau der Informationssysteme von Europol benötigten Hard- und Software. Zurzeit stehen die IT-Systeme von Europol nur einem begrenzten Kreis von Europol-Mitarbeitern, Europol-Verbindungsbeamten und mitgliedstaatlichen Ermittlern zur Verfügung, die diese Systeme für Analyse- und Ermittlungszwecke nutzen. Durch die Implementierung von QUEST (Systemschnittstelle, über die das ESP künftig Europol-Daten abfragen können soll) mit Basisschutzniveau (gegenwärtig sind die Informationssysteme von Europol maximal für die Geheimhaltungsgrade „EU restricted“ und „EU confidential“ zugelassen) werden die Informationssysteme von Europol einem weit größeren Kreis ermächtigter Strafverfolgungsbeamter zur Verfügung gestellt werden. Außerdem wird das ESP auch vom ETIAS für die automatische Abfrage von Europol-Daten im Zuge der Bearbeitung von Anträgen auf Reisegenehmigungen verwendet werden. Dadurch wird

sich die Zahl der Abfragen von Europol-Daten von aktuell schätzungsweise 107 000 pro Monat auf über 100 000 pro Tag erhöhen, und um den Anforderungen der ETIAS-Verordnung gerecht zu werden, wird es erforderlich sein, das Informationssystem rund um die Uhr verfügbar zu halten und für sehr kurze Reaktionszeiten zu sorgen. Der Großteil der Kosten ist auf den Zeitraum bis zur Erreichung der Betriebsbereitschaft der Interoperabilitätskomponenten beschränkt, doch um eine fortwährend hohe Einsatzbereitschaft der Informationssysteme von Europol sicherzustellen, müssen auch in gewissem Umfang laufend Mittel zur Verfügung gestellt werden. Außerdem sind bestimmte Entwicklungsarbeiten erforderlich, um die Interoperabilitätskomponenten zu implementieren, die Europol in seiner Eigenschaft als Nutzer benötigt.

18 02 05 (CEPOL)			Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGE-SAMT**
Titel 1: Personalausgaben	Verpflichtungen	(1)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
	Zahlungen	(2)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
Titel 2: Infrastruktur- und Betriebsausgaben	Verpflichtungen	(1a)	0	0	0	0	0	0	0	0	0	0
	Zahlungen	(2a)	0	0	0	0	0	0	0	0	0	0
Titel 3: Operative Ausgaben	Verpflichtungen	(3a)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
	Zahlungen	(3b)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Mittel INSGESAMT für CEPOL	(Verpflichtungen insg. = Zahlungen insg.)	=1+1a +3a	0	0,144	0,384	0,482	0,208	0,208	0,208	0,208	0,208	2,050

Die zentrale Koordinierung von Schulungsmaßnahmen auf EU-Ebene ist einer kohärenten Durchführung von Schulungsmaßnahmen auf nationaler Ebene förderlich und trägt auf diese Weise zu einer korrekten und erfolgreichen Umsetzung und Nutzung der Interoperabilitätskomponenten bei. Die Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL) ist perfekt aufgestellt, um zentrale Schulungen auf EU-Ebene durchzuführen. Diese Ausgaben decken die vorbereitenden Arbeiten für die „Ausbildung von Schulungspersonal der Mitgliedstaaten“ ab, das die Zentralsysteme nutzen soll, sobald diese miteinander verbunden sind. Die Kosten umfassen die Kosten für eine geringfügige Personalaufstockung bei CEPOL zwecks Koordinierung, Leitung, Organisation und Aktualisierung der Kurse sowie die Kosten für die Durchführung einer bestimmten Anzahl von Schulungen pro Jahr und für die Ausarbeitung von Onlinekursen. Nähere Einzelheiten dieser Kosten siehe unten. Die Schulungen werden sich jeweils auf den Zeitraum unmittelbar vor der

Inbetriebnahme konzentrieren. Darüber hinaus wird nach der Inbetriebnahme ein kontinuierlicher Schulungsbedarf bestehen, da die Interoperabilitätskomponenten gewartet werden müssen und – wie die Erfahrung beim bestehenden Schengener Informationssystem gezeigt hat – die Ausbilder möglicherweise wechseln werden.

18 02 07 (eu-LISA)			Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGE-SAMT**
Titel 1: Personalausgaben	Verpflichtungen	(1)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
	Zahlungen	(2)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
Titel 2: Infrastruktur- und Betriebsausgaben	Verpflichtungen	(1a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
	Zahlungen	(2a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
Titel 3: Operative Ausgaben	Verpflichtungen	(3a)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
	Zahlungen	(3b)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Mittel INSGESAMT für eu-LISA	(Verpflichtungen insg. = Zahlungen insg.)	=1+1a +3a	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**

Diese Ausgaben decken Folgendes ab:

– Entwicklung und Wartung der vier Interoperabilitätskomponenten (Europäisches Suchportal - ESP, gemeinsamer Dienst für den Abgleich biometrischer Daten - gemeinsamer BMS, gemeinsamer Speicher für Identitätsdaten - CIR und Detektor für Mehrfachidentitäten - MID), die Gegenstand des vorliegenden Legislativvorschlags sind, sowie des zentralen Speichers für Berichte und Statistiken (CRRS). Die Agentur eu-LISA wird als Vertreterin des Projektträgers agieren und mit ihrem eigenen Personal Spezifikationen erstellen, Auftragnehmer auswählen, die Arbeiten leiten, die Ergebnisse einer Reihe von Tests unterziehen und die Arbeiten abnehmen.

– die Kosten der Migration der Daten von den bestehenden Systemen zu den neuen Komponenten. Allerdings wird eu-LISA keine direkte Rolle beim anfänglichen Hochladen von Daten in den MID (zwecks Validierung von Verknüpfungen) spielen, da dieser Vorgang ausschließlich den

Inhalt der Daten betrifft. Die Migration der biometrischen Daten aus den bestehenden Systemen hingegen berührt nicht den Inhalt der Daten, sondern ihr Format und ihre Kennzeichnung.

– Die Kosten für die Modernisierung und den Betrieb des ECRIS-TCN zwecks Sicherstellung eines hochgradig verfügbaren Systems ab 2022. Das ECRIS-TCN ist das Zentralsystem mit den Strafregisterinformationen über Drittstaatsangehörige. Das System soll spätestens im Jahr 2020 verfügbar sein. Da die Interoperabilitätskomponenten voraussichtlich auch auf das ECRIS-TCN zugreifen sollen, sollte auch dieses System eine hohe Verfügbarkeit besitzen. Die zusätzlichen Kosten für die Herstellung einer hohen Verfügbarkeit sind in den operativen Ausgaben enthalten. Im Jahr 2021 werden erhebliche Entwicklungskosten anfallen, an die sich laufende Wartungs- und Betriebskosten anschließen werden. Diese Kosten sind nicht im Finanzbogen der überarbeiteten Gründungsverordnung für eu-LISA[76] enthalten, da dieser nur die Mittel für den Zeitraum 2018-2020 umfasst und diesen Mittelbedarf mithin nicht erfasst.

– Das Ausgabenmuster ergibt sich aus dem vorgesehenen Projektablauf. Da die einzelnen Komponenten nicht voneinander unabhängig sind, erstreckt sich der Entwicklungszeitraum auf die Jahre 2019 bis 2023. Allerdings werden bereits ab dem Jahr 2020 Wartung und Betrieb der ersten verfügbaren Komponenten aufgenommen werden. Dies erklärt, warum die vorgesehenen Ausgaben zunächst langsam einsetzen, dann zunehmen und dann auf einen konstanten Wert zurückgehen werden.

– Die Ausgaben unter Titel 1 (Personalausgaben) ergeben sich ebenfalls aus dem vorgesehenen Projektablauf: Sobald die Projektdurchführung vonseiten des Auftragsnehmers (dessen Ausgaben unter Titel 3 aufgeführt sind) beginnt, wird mehr Personal benötigt werden. Während der Projektdurchführung werden Teile des Durchführungsteams mit Entwicklungs- und Wartungsarbeiten befasst werden. Gleichzeitig wird das Personal für den Betrieb der neuen Systeme aufgestockt werden.

– Die Ausgaben unter Titel 2 (Infrastruktur- und Betriebsausgaben) decken die zusätzlichen Büroräume für die vorübergehende Unterbringung der vom Auftragnehmer eingesetzten Teams für die Aufgaben im Zusammenhang mit Entwicklung, Wartung und Betrieb ab. Die zeitliche Staffelung der Ausgaben entspricht somit ebenfalls der Entwicklung des Personalbestands. Die Kosten für die Unterbringung zusätzlicher Ausrüstung sind bereits im Haushaltsplan von eu-LISA enthalten. Für die Unterbringung des Personals von eu-LISA entstehen ebenfalls keine zusätzlichen Kosten, da dies durch die herkömmlichen Personalkosten abgedeckt ist.

– Die Ausgaben unter Titel 3 (operative Ausgaben) enthalten die Kosten für die Entwicklung und Wartung des Systems durch den Auftragnehmer sowie für den Erwerb der einschlägigen Hard- und Software.
Die Kosten für den Auftragnehmer beginnen zunächst mit den erforderlichen Studien für die Ermittlung der benötigten Komponenten und betreffen zunächst nur die Entwicklung einer einzigen Komponente (CRRS). Im Zeitraum 2020-2022 werden dann weitere Komponenten parallel zueinander entwickelt werden und die Kosten entsprechend steigen. Da die Aufgaben im Zusammenhang mit der Datenmigration in

[76] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts und zur Änderung der Verordnung (EG) Nr. 1987/2006 und des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EU) Nr. 1077/2011 (COM 2017/0145 (COD)).

diesem Projektteil besonders umfangreich sind, werden die Kosten nach Erreichung ihres Höhepunkts nicht zurückgehen. Die Kosten für den Auftragnehmer werden nach der Fertigstellung der Komponenten abnehmen, aber auch der anschließende Betriebsmodus wird stabile Ressourcenmuster erfordern.
Gleichzeitig zu den Ausgaben unter Titel 3 werden die Ausgaben im Jahr 2020 gegenüber dem Vorjahr stark ansteigen, weil Anfangsinvestitionen in Hard- und Software für die Entwicklungsphase erforderlich sein werden. Die Ausgaben unter Titel 3 (Betriebsausgaben) werden in den Jahren 2021 und 2022 stark ansteigen, weil jeweils im Jahr vor der Inbetriebnahme Hard- und Softwareinvestitionen für die operativen IT-Umgebungen (Produktions- und Vorproduktionsumgebungen für die Zentraleinheit und für die Backup-Zentraleinheit) bzw. für die Interoperabilitätskomponenten (CIR und MID) mit ihren hohen Hard- und Softwareanforderungen erforderlich sein werden. Nach der Inbetriebnahme werden für Hard- und Software im Wesentlichen nur noch Kosten in Form von Wartungskosten anfallen.

– Nähere Einzelheiten siehe unten.

Rubrik des mehrjährigen Finanzrahmens	**5**	Verwaltungsausgaben

in Mio. EUR (3 Dezimalstellen)

		Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGE-SAMT**
GD HOME											
• Personelle Ressourcen Nummer der Haushaltslinie 18 01		0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Sonstige Verwaltungskosten (Sitzungen usw.)		0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
GD HOME INSGESAMT	Mittel	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Mittel INSGESAMT unter RUBRIK 5 des mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

in Mio. EUR (3 Dezimalstellen)

		Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	Jahr 2028	**INSGE-SAMT**
Mittel INSGESAMT unter den RUBRIKEN 1 bis 5 des mehrjährigen Finanzrahmens	Verpflichtungen	**7,533**	**26,569**	**104,672**	**98,591**	**83,363**	**25,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**
	Zahlungen	**7,533**	**26,569**	**96,042**	**97,591**	**83,993**	**34,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**

3.2.2. Geschätzte Auswirkungen auf die operativen Mittel

3.2.2.1. Geschätzte Auswirkungen auf die Mittel der Europäischen Agentur für die Grenz- und Küstenwache

– ☐ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

– ☒ Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

Mittel für Verpflichtungen in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse			Jahr **2019**		Jahr **2020**		Jahr **2021**		Jahr **2022**		Jahr **2023**		Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		**INSGESAMT**	
Europäische Agentur für die Grenz- und Küstenwache ⇩	Art[77]	Durch-schnitts-kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1[78] Validierung von Verknüpfungen																						
für die Verknüpfungsverifizierung eingestellte Sachverständige	Kosten für den Auftragnehmer		0	0	0	0	0	0	0,8	0,183	10	2,200	0	0	0	0	0	0	0	0		2,383
Zwischensumme für Einzelziel Nr. 1			**0**	**0**	**0**	**0**	**0**	**0**	**0,8**	**0,183**	**10**	**2,200**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**2,383**

Diese Ausgaben decken Folgendes ab:

- Einstellung von genügend zusätzlichem Personal (geschätzter Bedarf: 10 Sachverständige) zur Ergänzung des vorhandenen internen Personals (ca. 20 Personen) zwecks Validierung von Verknüpfungen in der Europäischen Agentur für die Grenz- und Küstenwache. Das

[77] Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Zahl der Austauschstudenten, gebaute Straßenkilometer usw.).

[78] Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

Einstellungsverfahren soll binnen nur eines Monats vor dem voraussichtlichen Starttermin, an dem der erforderliche Personalbestand vorhanden sein muss, durchgeführt werden.

- Sonstige Kosten für den Auftragnehmer werden nicht erwartet. Die Kosten für die erforderliche Software sind durch die Lizenzgebühren für den gemeinsamen BMS abgedeckt. Hardwareverarbeitungskapazitäten sind nicht vorgesehen. Die Unterbringung des Personals des Auftragnehmers erfolgt voraussichtlich durch die Europäische Agentur für die Grenz- und Küstenwache. Aus diesem Grund wurden bei den Ausgaben unter Titel 2 die jährlichen Kosten für durchschnittlich 12 m² pro Person hinzugefügt.

3.2.2.2. Geschätzte Auswirkungen auf die Mittel von Europol

– ☐ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

– ☒ Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

Mittel für Verpflichtungen in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse **Europol** ⇩			Jahr **2019**		Jahr **2020**		Jahr **2021**		Jahr **2022**		Jahr **2023**		Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		**INSGESAMT**	
	Art[79]	Durch-schnitts-kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1[80] Entwicklung und Wartung der (Europol-)Systeme																						
IT-Umgebung	Infrastruktur					1,840		1,840		0,736		0,736		0,736		0,736		0,736		0,736		8,096
IT-Umgebung	Hardware					3,510		3,510		1,404		1,404		1,404		5,754		5,754		1,404		26,144
IT-Umgebung	Software					0,670		0,670		0,268		0,268		0,268		0,268		0,268		0,268		2,948

79 Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Zahl der Austauschstudenten, gebaute Straßenkilometer usw.).

80 Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

Entwicklungs-arbeiten	Auftragnehmer				0,360		0,360												0,720
Zwischensumme			**0**		**6,380**		**6,380**		**2,408**		**2,408**		**2,408**		**7,758**		**7,758**		**2,408**		**37,908**

Diese Ausgaben decken den für die Bewältigung der steigenden Anzahl von Abfragen erforderlichen Ausbau der Informationssysteme von Europol und der betreffenden Infrastruktur ab. Sie schließen folgende Kosten ein:

– Kosten für die Modernisierung der Sicherheits- und Netzwerkinfrastruktur sowie der betreffenden Hardware (Server, Speicher) und Software (Lizenzgebühren). Diese Modernisierung muss abgeschlossen werden, bevor im Jahr 2021 die Betriebsbereitschaft des Europäischen Suchportals und des ETIAS hergestellt wird. Die Kosten wurden zu gleichen Teilen auf die Jahre 2020 und 2021 verteilt. Ab dem Jahr 2022 wurde für die Berechnung der Wartungskosten eine jährliche Wartungsquote von 20 % zugrunde gelegt. Außerdem wurde der übliche Fünfjahreszyklus für die Ersetzung veralteter Hardware und Infrastrukturen zugrunde gelegt.

– Kosten für die vom Auftragnehmer durchzuführenden Entwicklungsarbeiten zur Implementierung von QUEST mit Basisschutzniveau.

3.2.2.3. Geschätzte Auswirkungen auf die Mittel der CEPOL

– ☐ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

– ☒ Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

Mittel für Verpflichtungen in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse CEPOL ⇩			Jahr **2019**		Jahr **2020**		Jahr **2021**		Jahr **2022**		Jahr **2023**		Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		**INSGESAMT**	
	Art[81]	Durch-schnitts-kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1[82] Ausarbeitung und Durchführung von Schulungen																						
Zahl der aufenthaltsge-bundenen Schulungen	0,34 je Schulung		0		1	0,040	4	0,136	8	0,272	2	0,068	2	0,068	2	0,068	2	0,068	2	0,068		0,788
Online-Schulungen	0,02			0				0,040		0,002		0,002		0,002		0,002		0,002		0,002		0,052
Zwischensumme				**0**		**0,040**		**0,176**		**0,274**		**0,070**		**0,070**		**0,070**		**0,070**		**0,070**		**0,840**

[81] Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Zahl der Austauschstudenten, gebaute Straßenkilometer usw.).

[82] Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

Um eine einheitliche Implementierung und Nutzung der Interoperabilitätslösungen sicherzustellen, werden sämtliche Schulungsmaßnahmen von der CEPOL und den Mitgliedstaaten zentral auf EU-Ebene organisiert. Die Ausgaben für Schulungsmaßnahmen auf EU-Ebene schließen Folgendes ein:

– Ausarbeitung eines einheitlichen Lehrplans für die nationalen Schulungsmaßnahmen der Mitgliedstaaten;

– aufenthaltsgebundene Maßnahmen zur Schulung der Ausbilder. Es wird davon ausgegangen, dass in den beiden Jahren unmittelbar nach der Herstellung der Betriebsbereitschaft der Interoperabilitätslösungen Schulungen in größerem Umfang durchgeführt werden und danach jährlich zwei aufenthaltsgebundene Schulungen stattfinden werden.

– Online-Schulungskurs zur Ergänzung der aufenthaltsgebundenen Schulungsmaßnahmen auf EU-Ebene und in den Mitgliedstaaten.

3.2.2.4. Geschätzte Auswirkungen auf die Mittel von eu-LISA

– ☐ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

– ☒ Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

Mittel für Verpflichtungen in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse eu-LISA ⇩			Jahr **2019**		Jahr **2020**		Jahr **2021**		Jahr **2022**		Jahr **2023**		Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		**INSGE-SAMT**	
	Art[83]	Durch-schnitts-kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Gesamtzahl	Gesamt-kosten
EINZELZIEL Nr. 1[84] Entwicklung der Interoperabilitätskomponenten																						
erstellte Systeme	Auftrag-nehmer			1,800		4,930		8,324		4,340		1,073		1,000		0,100		0,020		0,020		21,607
Software-produkte	Software			0,320		3,868		15,029		8,857		3,068		0,265		0,265		0,265		0,265		32,202
Hardware-produkte	Hardware			0,250		2,324		5,496		2,904		2,660		0,500		0		0		0		14,133
IT-Schulungen	Schulungen und sonstige Maßnahmen			0,020		0,030		0,030		0,030		0,030		0,050		0,050		0,050		0,050		0,340

83 Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Zahl der Austauschstudenten, gebaute Straßenkilometer usw.).

84 Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

Zwischensumme für Einzelziel Nr. 1		**2,390**		**11,151**		**28,879**		**16,131**		**6,830**		**1,815**		**0,415**		**0,335**		**0,335**		**68,281**

– Dieses Ziel schließt nur die Kosten für die Erstellung der vier Interoperabilitätskomponenten und des CRRS ein.

– Bei der Kostenschätzung für den gemeinsamen BMS wurde vorausgesetzt, dass das noch zu entwickelnde EES als Kernsystem für die Entwicklung dienen wird. So ist geplant, die Lizenzen der biometrischen Software für das EES (Kosten: 36 Mio. EUR) für die anderen Komponenten wiederzuverwenden.

– In haushaltstechnischer Hinsicht wird der gemeinsame BMS in dieser Rubrik als Erweiterung des BMS für das EES behandelt. Aus diesem Grund werden in diesem Finanzbogen lediglich geringfügige Kosten für Softwarelizenzen (6,8 Mio. EUR) veranschlagt, die für die Eingabe der rund 20 Millionen biometrischen Datensätze aus dem SIS AFIS (AFIS ist das System für die automatische Identifizierung von Fingerabdrücken, also quasi der „BMS“ des SIS), aus dem Eurodac AFIS und aus dem künftigen ECRIS-TCN (Europäisches Strafregisterinformationssystem für Drittstaatsangehörige) in den für das EES einzurichtenden BMS benötigt werden. Die Kosten für den Anschluss der verschiedenen Systeme (SIS, Eurodac und ECRIS-TCN) an den gemeinsamen BMS sind in diesem Finanzbogen enthalten.

– Da die benötigte technische Lösung zum Zeitpunkt der Vorlage des Legislativvorschlags noch nicht genau bestimmt werden kann, wird die Agentur eu-LISA beauftragt werden, im Rahmen der für die Jahre 2019 und 2020 vorgesehenen Arbeiten eine solche Lösung auszuarbeiten und eine Kostenschätzung für die Umsetzung der letztendlich ausgewählten technischen Lösung vorzunehmen. Daher wird es möglicherweise erforderlich werden, die an dieser Stelle vorgenommene Kostenschätzung entsprechend anzupassen.

– Sämtliche Komponenten werden bis Ende 2023 fertiggestellt. Deshalb verringern sich die Ausgaben für den Auftragnehmer bis dahin fast auf Null, und es wird lediglich ein Restkostenbetrag für die regelmäßigen Aktualisierungen des CRRS verbleiben.

– Im Zeitraum 2019 bis 2021 werden die Ausgaben für Software stark ansteigen, da Softwarelizenzgebühren für die benötigten Produktions-, Vorproduktions- und Testumgebungen sowohl am zentralen Standort als auch am Backupstandort anfallen werden. Hinzu kommt, dass sich der Preis bestimmter unbedingt benötigter Softwarekomponenten nach der Zahl der „Referenzobjekte“ (in diesem Fall also sozusagen nach dem Datenvolumen) bemisst. Da die Datenbank jedoch letztendlich immerhin etwa 220 Millionen Identitäten enthalten soll, ist die Software ihren Preis wert.

Ziele und Ergebnisse eu-LISA ⇩			Jahr **2019**		Jahr **2020**		Jahr **2021**		Jahr **2022**		Jahr **2023**		Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		**INSGE-SAMT**	
	Art[85]	Durch-schnitts-kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Gesamtzahl	Gesamt-kosten
EINZELZIEL Nr. 2 Wartung und Betrieb der Interoperabilitätskomponenten																						
Sicherstel-lung der kontinu-ierlichen Betriebsberei	Auftragnehmer			0		0		0		1,430		2,919		2,788		2,788		2,788		2,788		15,501
Software-produkte	Software			0		0,265		0,265		1,541		5,344		5,904		5,904		5,904		5,904		31,032
Hardware-produkte	Hardware			0		0,060		0,060		0,596		1,741		1,741		1,741		1,741		1,741		9,423
IT-	Schulung			0		0		0		0		0,030		0,030		0,030		0,030		0,030		0,150
Zwischensumme für Einzelziel Nr. 2				**0**		**0,325**		**0,325**		**3,567**		**10,034**		**10,464**		**10,464**		**10,464**		**10,464**		**56,105**

– Die Wartung wird aufgenommen werden, sobald bestimmte Komponenten fertiggestellt sind. Aus diesem Grund werden ab dem Zeitpunkt der Fertigstellung des ESP (im Laufe des Jahres 2021) Mittel für einen externen Wartungsdienst veranschlagt. Die für Wartungszwecke vorgesehenen Mittel werden in dem Maße, wie nach und nach weitere Komponenten fertiggestellt werden, zunehmen und danach auf nahezu konstantem Niveau (15 bis 22 % der Anfangsinvestition) bleiben.

[85] Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Zahl der Austauschstudenten, gebaute Straßenkilometer usw.).

– Da die Hardwarewartung und die Softwarepflege jeweils ab dem Jahr der Inbetriebnahme einsetzen werden, ist der diesbezügliche Kostenverlauf ähnlich wie bei der Entwicklung der Kosten für den Auftragnehmer.

Ziele und Ergebnisse eu-LISA ⇩			Jahr **2019**		Jahr **2020**		Jahr **2021**		Jahr **2022**		Jahr **2023**		Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		**INSGESAMT**	
	Art[86]	Durch-schnitts-kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 3[87] Datenmigration																						
Migration bestehender BMS-Daten	zum gemeinsamen BMS			0		0		0		7,000		3,000		0		0		0		0		10,000
Herstellung der Migrations-fähigkeit bestehender	Neukonzipie-rung/Neukon-struktion des EDAC			0		0		7,500		7,500				0		0		0		0		15,000
Zwischensumme für Einzelziel Nr. 3				**0**		**0**		**7,500**		**14,500**		**3,000**										**25,000**

– Es ist erforderlich, aus den anderen biometrischen Maschinen Daten zum gemeinsamen BMS zu migrieren, da dieser gemeinsame Speicher wirksamer betrieben werden kann und auch finanziell günstiger ist als die bisher erfolgende Wartung zahlreicher kleinerer Speicher dieser Art.

[86] Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Zahl der Austauschstudenten, gebaute Straßenkilometer usw.).

[87] Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

– Im Gegensatz zum Zusammenspiel des BMS und des VIS ist Eurodac von seiner Geschäftslogik her derzeit nicht eindeutig vom Mechanismus für den Abgleich biometrischer Daten getrennt. Die Funktionsweise von Eurodac und das Verfahren, wie seine Geschäftsdienste auf die systemeigenen Dienste für den Abgleich biometrischer Daten zugreifen, sind für den Außenstehenden nicht nachvollziehbar und gründen sich auf proprietäre Technik. Daher wird es nicht möglich sein, die Daten ohne Weiteres zu einem gemeinsamen BMS zu migrieren und dabei die bestehende Anwendungsschicht beizubehalten. Die Datenmigration wird daher mit erheblichen Kosten für die Anpassung der Mechanismen für den Datenaustausch mit der zentralen Eurodac-Anwendung einhergehen.

Ziele und Ergebnisse eu-LISA ⇩			Jahr **2019**		Jahr **2020**		Jahr **2021**		Jahr **2022**		Jahr **2023**		Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		**INSGESAMT**	
	Art[88]	Durch-schnitts-kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 4[89] Netz																						
Netzverbin-dungen	Netzkonfiguration			0		0		0		0,505										0		0,505
Abwicklung des Netzverkehrs	Netzbetrieb			0		0						0,246		0,246		0,246		0,246		0,246		1,230
Zwischensumme für Einzelziel Nr. 4				**0**		**0**		**0**		**0,505**		**0,246**		**0,246**		**0,246**		**0,246**		**0,246**		**1,735**

– Die Interoperabilitätskomponenten werden sich nur marginal auf den Netzverkehr auswirken. Es werden lediglich Verknüpfungen zwischen bestehenden Daten generiert werden, wodurch nur ein geringer Netzverkehr entstehen wird. Bei den hierfür veranschlagten Kosten handelt es

88 Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Zahl der Austauschstudenten, gebaute Straßenkilometer usw.).

89 Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

sich lediglich um die geringfügigen Kosten, die zusätzlich zu den für die Netzkonfiguration und den Netzverkehr des EES und des ETIAS veranschlagten Kosten anfallen werden.

Ziele und Ergebnisse eu-LISA ⇩			Jahr **2019**		Jahr **2020**		Jahr **2021**		Jahr **2022**		Jahr **2023**		Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		**INSGESAMT**	
	Art[90]	Durch-schnitts-kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 5[91] Aktualisierung der einheitlichen nationalen Schnittstellen																						
aktualisierte einheitliche nationale Schnittstellen	Auftragnehmer			0		0		0		0,505		0,505								0		1,010
Zwischensumme für Einzelziel Nr. 5				**0**		**0**		**0**		**0,505**		**0,505**										**1,010**

– Im Legislativvorschlag zur Errichtung des EES wurde das Konzept der einheitlichen nationalen Schnittstellen eingeführt, die von eu-LISA entwickelt und gewartet werden sollen. Die obige Tabelle enthält die vorgesehenen Mittel für die Aktualisierung dieser Schnittstellen für einen zusätzlichen Informationsaustausch. Für den Betrieb der Schnittstellen entstehen keine zusätzlichen Kosten zu den bereits im EES-Vorschlag veranschlagten Kosten.

90 Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Zahl der Austauschstudenten, gebaute Straßenkilometer usw.).

91 Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

Ziele und Ergebnisse eu-LISA ⇩			Jahr **2019**		Jahr **2020**		Jahr **2021**		Jahr **2022**		Jahr **2023**		Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		**INSGESAMT**	
	Art 92	Durch-schnitts-kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 6: Sitzungen und Schulungsmaßnahmen																						
Monatliche Arbeits-sitzungen (Entwick-lung)	0,021 je Sitzung x 10 pro Jahr		10	*0,210*	10	*0,210*	10	*0,210*	10	*0,210*											40	0,840
vierteljähr-liche Sitzungen (Betrieb)	0,021 je Sitzung x 4 pro Jahr		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Berater-gruppen	0,021 x 4 pro Jahr		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Schulungen in den MS	0,025 je Schulung		2	0,050	4	0,100	4	0,100	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	24	1,150
Zwischensumme für Einzelziel Nr. 6			20	**0,428**	22	**0,478**	22	**0,478**	24	**0,528**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**		**3,502**

92 Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Zahl der Austauschstudenten, gebaute Straßenkilometer usw.).

– In der Zwischensumme für Einzelziel Nr. 6 sind die Kosten für die Organisation von Sitzungen der für die Projektleitung verantwortlichen Verwaltungsbehörde (in diesem Fall eu-LISA) enthalten. Dabei handelt es sich um zusätzliche Sitzungen im Zusammenhang mit der Erstellung der Interoperabilitätskomponenten.

– In der Zwischensumme für Einzelziel Nr. 6 sind zudem die Kosten für Zusammenkünfte von eu-LISA mit Bediensteten der Mitgliedstaaten zu Fragen im Zusammenhang mit der Entwicklung, der Wartung und dem Betrieb der Interoperabilitätskomponenten sowie mit der Organisation und Durchführung von Schulungen für IT-Bedienstete der Mitgliedstaaten enthalten.

– In der Entwicklungsphase sind jährlich 10 Projektsitzungen veranschlagt. Während der (im Jahr 2019 beginnenden) Vorbereitungen für die Inbetriebnahme sollen vier Sitzungen pro Jahr stattfinden. Von Beginn an wird auf höherer Ebene eine Beratergruppe eingerichtet, die sich mit der Implementierung der von der Kommission erlassenen Durchführungsbeschlüsse befassen soll. Für diese Beratergruppe sind – wie für die bereits bestehenden Beratergruppen – vier Sitzungen pro Jahr vorgesehen. Außerdem soll die Agentur eu-LISA Schulungen für IT-Bedienstete der Mitgliedstaaten konzipieren und abhalten. Dabei wird es sich um Schulungen über technische Aspekte der Interoperabilitätskomponenten handeln.

Ziele und Ergebnisse eu-LISA ⇩			Jahr **2019**		Jahr **2020**		Jahr **2021**		Jahr **2022**		Jahr **2023**		Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		**INSGESAMT**	
	Art[93]	Durch-schnitts-kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 7[94] hohe Verfügbarkeit des ECRIS-TCN																						
Hochverfüg-bares System	Systemkonfigu-ration			0		0		8,067												0		8,067

93 Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Zahl der Austauschstudenten, gebaute Straßenkilometer usw.).

94 Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

Hochverfüg-barer Betrieb	Systemwartung und -betrieb		0		0		0		1,768		1,768		1,768		1,768		1,768		1,768		10,608
Zwischensumme für Einzelziel Nr. 7			**0**		**0**		**8,067**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**18,675**

– Das Einzelziel Nr. 7 besteht darin, das ECRIS-TCN von einem System mit „standardmäßiger“ Verfügbarkeit zu einem System mit hoher Verfügbarkeit zu machen. Für den diesbezüglichen, für 2021 vorgesehenen Ausbau des ECRIS-TCN wird im Wesentlichen zusätzliche Hardware angeschafft werden müssen. Da die Modernisierung des ECRIS-TCN bereits für das Jahr 2020 vorgesehen ist, könnte auf den ersten Blick einiges dafür sprechen, das System bereits von Beginn an hochverfügbar zu gestalten und in die anderen Interoperabilitätskomponenten zu integrieren. Angesichts der Tatsache, dass zahlreiche Abhängigkeiten zwischen der Vielzahl von Projekten bestehen werden, ist es jedoch angebracht, vorsichtshalber von derartigen Überlegungen abzusehen und die einzelnen Maßnahmen separat zu veranschlagen. Bei diesen Mitteln handelt es sich um zusätzliche Mittel zur Deckung der Entwicklungs-, Wartungs- und Betriebskosten für das ECRIS-TCN in den Jahren 2019 und 2020.

3.2.2.5. Geschätzte Auswirkungen auf die Mittel der GD HOME

– ☐ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

– ☒ Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

Mittel für Verpflichtungen in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse GD Home ⇩			Jahr **2019**		Jahr **2020**		Jahr **2021**		Jahr **2022**		Jahr **2023**		Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		**INSGESAMT**	
	Art[95]	Durch-schnitts-kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Zahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1: Integration der nationalen Systeme (der Mitgliedstaaten)																						
betriebsbereite einheitliche nationale Schnittstellen	Anpassung der einheitlichen nationalen Schnittstellen - Entwicklungs-arbeiten						30	3,150	30	3,150											30	6,300
Anpassung der mitgliedstaat-lichen Systeme zwecks Herstellung	Integrationskosten						30	40,000	30	40,000	30	40,000									30	120,000

[95] Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Zahl der Austauschstudenten, gebaute Straßenkilometer usw.).

geschulte Endnutzer	insges. 10 000 Endnutzer-sitzungen zu je 1 000 EUR							5,000	5,000	5,000	5,000							10,000	10,000
Zwischensumme für Einzelziel Nr. 1							**43,150**		**48,150**		**45,000**								**136,300**

– Das Einzelziel Nr. 1 steht im Zusammenhang mit den Mitteln, die den Mitgliedstaaten zur Verfügung gestellt werden, damit diese die interoperablen Zentralsysteme nutzen können. Die einheitlichen nationalen Schnittstellen werden nach der Fertigstellung des ESP und bei Erreichung der Betriebsbereitschaft des MID angepasst werden. In beiden Fällen werden die einzelnen Mitgliedstaaten moderate Modifizierungen (Aufwand: ca. 150 Manntage) vornehmen müssen, um den Nachrichtenaustausch mit den Zentralsystemen anzupassen. Deutlich umfangreicher werden die Anpassungen des Dateninhalts sein, die zur Herstellung der Interoperabilität vorgenommen werden müssen und deren Kosten unter den „Integrationskosten“ zusammengefasst sind. Diese Mittel betreffen die notwendigen Änderungen an der Art der an das Zentralsystem übermittelten Mitteilungen und bei der Behandlung der betreffenden Antworten. Zur Deckung der voraussichtlichen Kosten dieser Anpassungen werden 4 Mio. EUR je Mitgliedstaat veranschlagt. Dies ist der gleiche Betrag wie beim EES, da für die Anpassungen zur Integration der nationalen Systeme mit einer einheitlichen nationalen Schnittstelle ein vergleichbarer Arbeitsaufwand entstehen wird.

– Es wird erforderlich sein, die Endnutzer der Systeme entsprechend zu schulen. Für diese Schulung einer sehr großen Zahl von Endnutzern (schätzungsweise 10 000 Schulungen, die von den Mitgliedstaaten in eigenen Schulungseinrichtungen abgehalten werden müssen) werden Kosten in Höhe von 1 000 EUR je Schulung (mit jeweils 10 bis 20 Endnutzern) veranschlagt.

3.2.3. Geschätzte Auswirkungen auf die Humanressourcen

3.2.3.1. Zusammenfassung für die Europäische Agentur für die Grenz- und Küstenwache

☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt

☒ Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

	Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGESAMT**
Beamte (AD)										
Beamte (AST)	0									
Vertragsbe-dienstete	0	0	0	0,350	1,400	0,233	0	0	0	1,983
Zeitbedienstete	0	0	0	0	0	0	0	0	0	0
Abgeordnete nationale Sachverständige										
INSGESAMT	**0,0**	**0,0**	**0,0**	**0,350**	**1,400**	**0,233**	**0,0**	**0,0**	**0,0**	**1,983**

Die von diesen zusätzlichen Mitarbeitern der Europäischen Agentur für die Grenz- und Küstenwache voraussichtlich zu erfüllenden Aufgaben sind zeitlich begrenzt (2023) und beginnen 24 Monate nach dem Zeitpunkt der Verfügbarkeit der biometrischen Suchmaschine für das EES. Allerdings müssen Mitarbeiter bereits vorher eingestellt werden (für die Berechnung wird von durchschnittlich drei Monaten ausgegangen), was den Betrag im Jahr 2022 erklärt. Auf die erledigten Arbeiten folgen abschließende Aufgaben, die zwei Monate in Anspruch nehmen werden, was den Personalbedarf für 2024 erklärt.

Beim Personalbedarf selbst wird von 20 Personen ausgegangen, die für die auszuführenden Arbeiten erforderlich sind (+ 10 Personen von einem Auftragnehmer wie unter Titel 3 angegeben). Die Erfüllung der Aufgaben wird voraussichtlich verlängerte Arbeitszeiten erfordern und nicht auf die üblichen Dienstzeiten beschränkt sein. Bei Unterstützungs- und Führungspersonal wird voraussichtlich auf die Ressourcen der Agentur zurückgegriffen werden.

Die Zahl der Mitarbeiter basiert auf der Annahme, dass etwa 550 000 Fingerabdrücke geprüft werden müssen, was pro Fall durchschnittlich 5 bis 10 Minuten dauert (17 000 geprüfte Fingerabdrücke pro Jahr pro Mitarbeiter).[96]

[96] Die Personalangaben für das Jahr 2020 und die folgenden Jahre sind Richtwerte, und es wird zu prüfen sein, ob die betreffenden Mitarbeiter zusätzlich zu den Vorausberechnungen für das Personal der

Zahl der Mitarbeiter	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total
Mitarbeiter für die manuelle Bearbeitung von Verknüpfungen und Entscheidungen	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Insgesamt Titel 1 - VB	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Insgesamt Titel 1 - ZB	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Insgesamt Titel 1	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3

.

3.2.3.2. Zusammenfassung für Europol

☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt

☒ Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

	Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGESAMT**
Beamte (AD)										
Beamte (AST)	0									
Vertragsbe-dienstete	0,000	0,070	0,070	0,560	0,560	0,560	0,560	0,560	0,560	3,500
Zeitbedienstete	0,690	1,932	1,932	0,621	0,621	0,414	0,414	0,414	0,414	7,452
Abgeordnete nationale Sachverständige										
INSGESAMT	**0,690**	**2,002**	**2,002**	**1,181**	**1,181**	**0,974**	**0,974**	**0,974**	**0,974**	**10,952**

Diese Kosten werden auf der Grundlage des folgenden Personalbestands geschätzt:

Zahl der VZÄ für IKT	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Insge-samt**
Vertrags-bedienstete	0,0	1,0	1,0	8,0	8,0	8,0	8,0	8,0	8,0	50,0
Zeitbedienstete	5,0	14,0	14,0	4,5	4,5	3,0	3,0	3,0	3,0	54,0
Personal insgesamt (VZÄ)	**5,0**	**15,0**	**15,0**	**12,5**	**12,5**	**11,0**	**11,0**	**11,0**	**11,0**	**104,0**

Europäischen Agentur für die Grenz- oder Dokument im Dokument COM(2015) 671 erforderlich sein werden oder nicht.

Für Europol ist zusätzliches IKT-Personal vorgesehen, das die Kapazitäten der Informationssysteme von Europol ausbauen soll, damit die steigende Zahl von Abfragen im ESP und im ETIAS bewältigt werden kann, und das die Systeme später rund um die Uhr warten soll.

– Für die Implementierungsphase des ESP (2020 und 2021) besteht zusätzlicher Bedarf an technischen Experten (Architekten, Ingenieure, Entwickler, Tester). Ab dem Jahr 2022 werden weniger technische Experten benötigt werden; ihre Aufgabe wird die Implementierung der übrigen Interoperabilitätskomponenten und die Wartung der Systeme sein.

– Ab dem zweiten Halbjahr 2021 muss eine permanente Überwachung der IKT-Systeme eingeführt werden, um die erforderlichen Leistungsniveaus des ESP und des ETIAS sicherzustellen. Hierfür sollen zwei Vertragsbedienstete sorgen, die in vier Schichten rund um die Uhr arbeiten.

– Soweit möglich wurden die Profile zu gleichen Teilen zwischen Zeitbediensteten und Vertragsbediensteten aufgeteilt. Aufgrund der hohen Sicherheitsanforderungen können für bestimmte Stellen allerdings nur Zeitbedienstete eingesetzt werden. Die Ergebnisse der Konzertierung über das Haushaltsverfahren 2018 werden bei der Beantragung von Zeitbediensteten berücksichtigt werden.

3.2.3.3. Zusammenfassung für die CEPOL

☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt

☒ Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

	Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGESAMT**
Beamte (AD)										
Beamte (AST)										
Vertragsbe-dienstete			0,070	0,070						**0,140**
Zeitbedienstete		0,104	0,138	0,138	0,138	0,138	0,138	0,138	0,138	1,070
Abgeordnete nationale Sachverständige										
INSGESAMT		**0,104**	**0,208**	**0,208**	**0,138**	**0,138**	**0,138**	**0,138**	**0,138**	**1,210**

Es ist zusätzliches Personal erforderlich, da Ausbildungsmaßnahmen für Schulungspersonal der Mitgliedstaaten im Hinblick auf die Nutzung der Interoperabilitätskomponenten unter operativen Gegebenheiten ausgearbeitet werden müssen.

- Die Ausarbeitung von Lehrplänen und Schulungsmodulen sollte mindestens 8 Monate vor der Inbetriebnahme des Systems beginnen. In den ersten beiden Jahren nach der Inbetriebnahme wird die Schulungstätigkeit am intensivsten sein. Allerdings müssen die Schulungen über einen längeren Zeitraum durchgeführt werden, um angesichts der Erfahrungen mit dem Schengener Informationssystem für eine kohärente Umsetzung zu sorgen.

- Das zusätzliche Personal wird für die Ausarbeitung, Koordinierung und Umsetzung des Lehrplans, der aufenthaltsgebundenen Lehrgänge und der Online-Kurse benötigt. Diese Schulungen können nur zusätzlich zum bestehenden Schulungskatalog der CEPOL durchgeführt werden, weshalb zusätzliches Personal erforderlich ist.

- Geplant ist der Einsatz eines Zeitbediensteten als Schulungsmanager während der gesamten Entwicklungs- und Wartungsphase, der in der intensivsten Phase der Organisation von Schulungen von einem Vertragsbediensteten unterstützt werden soll.

3.2.3.4. Zusammenfassung für eu-LISA

☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt

☒ Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

	Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGESAMT**
Beamte (AD)										
Beamte (AST)										
Vertragsbe-dienstete	0,875	1,400	1,855	2,555	2,415	2,170	2,100	2,100	2,100	17,570
Zeitbedienstete	2,001	3,450	4,347	4,347	4,209	3,312	3,036	3,036	3,036	30,774
Abgeordnete nationale Sachverständige										
INSGESAMT	**2,876**	**4,850**	**6,202**	**6,902**	**6,624**	**5,482**	**5,136**	**5,136**	**5,136**	**48,344**

– Der Personalbedarf trägt der Tatsache Rechnung, dass die vier Komponenten und der CRRS ein Portfolio voneinander abhängiger Projekte (d. h. ein Programm) darstellen. Zur Bewältigung der Abhängigkeiten zwischen den Projekten wird ein Programmmanagementteam eingesetzt, das aus den Programm- und Projektmanagern und

den Profilen, die die Gemeinsamkeiten zwischen diesen festlegen müssen (häufig als Architekten bezeichnet), besteht. Für die Durchführung des Programms bzw. Projekts sind auch Profile für die Unterstützung von Programmen und Projekten erforderlich.

– Der Personalbedarf je Projekt wurde analog zu früheren Projekten (Visa-Informationssystem) geschätzt, wobei zwischen der Projektabschlussphase und der Betriebsphase unterschieden wird.

– Die Profile, die auch während der Betriebsphase weiter benötigt werden, werden als Zeitbedienstete eingestellt. Die während der Durchführung des Programms bzw. Projekts erforderlichen Profile werden als Vertragsbedienstete eingestellt. Zur Gewährleistung der erwarteten Kontinuität der Arbeiten und zur Sicherung des Wissensbestands innerhalb der Agentur wird die Zahl der Stellen im Verhältnis von fast 50:50 auf Zeitbedienstete und Vertragsbedienstete verteilt.

– Es wird davon ausgegangen, dass für das Projekt des ECRIS-TCN im Hochverfügbarkeitsmodus kein zusätzliches Personal erforderlich wäre und dass die Personalausstattung für eu-LISA für das Projekt durch den Einsatz vorhandener Mitarbeiter aus Projekten, die in diesem Zeitraum abgeschlossen werden, erfolgt.

Diese Schätzungen basieren auf folgender Personalausstattung:

Vertragsbedienstete:

3.2.1. Übersicht EU-LISA (entspricht T1) Zahl der Mitarbeiter	2019	2020	2021	2022	2023	2024	2025	2026	2027	Insges. (Formel)
Vertragsbedienstete										-
Programm-/Projektmanagement	4,0	5,0	5,5	5,5	4,5	3,0	3,0	3,0	3,0	36,5
CRRS PM	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*1,5*
MID	*0,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*2,0*
Programm-/Projektbüro	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*14,0*
Qualitätssicherung	*1,0*	*2,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*19,0*
Mittelverwaltung und Auftragsvergabe	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Mittelverwaltung										*0,0*
Planung und Kontrolle der Haushaltsmittel										*0,0*
Auftragsvergabe/-verwaltung	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Technische Experten	7,0	7,0	7,0	7,0	6,0	5,0	5,0	5,0	5,0	54,0
CRRS	*3,0*	*3,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*22,0*
ESP	*4,0*	*4,0*	*4,0*	*4,0*	*4,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Gemeinsamer BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Erprobung	1,5	3,0	4,0	4,0	4,0	3,0	2,0	2,0	2,0	25,5
CRRS	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*6,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Gemeinsamer BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,5*	*1,0*	*2,0*	*2,5*	*2,5*	*1,5*	*1,0*	*1,0*	*1,0*	*13,0*
MID	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*6,5*
Systemüberwachung	0,0	5,0	10,0	20,0	20,0	20,0	20,0	20,0	20,0	135,0
Gemeinsam (24:7)	0,0	*5,0*	*10,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*135,0*
Gesamtkoordinierung	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Humanressourcen	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
HR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Zwischensumme Vertragsbedienstete	**12,5**	**20,0**	**26,5**	**36,5**	**34,5**	**31,0**	**30,0**	**30,0**	**30,0**	**251,0**

Zeitbedienstete:

Zeitbedienstete										
Programm-/Projektmanagement	3,0	4,0	5,5	5,5	5,5	4,5	4,0	4,0	4,0	40,0
Programmmanager	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Projektmanagement	*0,0*	*0,0*	*1,0*	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*12,0*
Programm-/Projektbüro	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
ESP	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
Gemeinsamer BMS	*0,5*	*0,5*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*4,0*
CIR	*0,0*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Mittelverwaltung und Auftragsvergabe	3,0	3,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	34,0
Mittelverwaltung	*0,0*	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*7,0*
Planung und Kontrolle der Haushaltsmittel	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Auftragsvergabe/-verwaltung	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*18,0*
Technische Experten	6,0	14,0	17,0	17,0	15,0	11,0	10,0	10,0	10,0	110,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Gemeinsamer BMS	*2,0*	*3,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
CIR	*2,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Sicherheit	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*17,0*
MID	*0,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*12,0*
Architekten	*1,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,0*	*1,0*	*1,0*	*17,0*
Erprobung	2,5	3,0	4,0	4,0	4,0	2,5	2,0	2,0	2,0	26,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,5*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*6,5*
Gemeinsamer BMS	*2,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,5*	*1,5*	*1,5*	*19,5*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Systemüberwachung	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Gemeinsamer BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Schulungen	0,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	8,0
Schulungen	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*8,0*
Humanressourcen	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
HR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Sonstige	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	5,0
Datenschutzexperte	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	*5,0*
Zwischensumme Zeitbedienstete	**14,5**	**25,0**	**31,5**	**31,5**	**30,5**	**24,0**	**22,0**	**22,0**	**22,0**	**223,0**
Insgesamt	**27,0**	**45,0**	**58,0**	**68,0**	**65,0**	**55,0**	**52,0**	**52,0**	**52,0**	**474,0**

3.2.4. Geschätzte Auswirkungen auf die Verwaltungsmittel

3.2.4.1. Zusammenfassung für die GD HOME

– ☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt

– ☒ Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

	Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGESAMT**
RUBRIK 5 des mehrjährigen Finanzrahmens										
Personalausgaben GD HOME	0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Sonstige Verwaltungsausgaben	0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
Zwischensumme RUBRIK 5 des mehrjährigen Finanzrahmens	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Außerhalb der RUBRIK 5[97] des mehrjährigen Finanzrahmens	(Nicht verwendet)									
Personalausgaben										
Sonstige Verwaltungsausgaben										
Zwischensumme außerhalb der RUBRIK 5 des mehrjährigen Finanzrahmens										

INSGESAMT	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

.

97 Technische und/oder administrative Unterstützung und Ausgaben zur Unterstützung der Umsetzung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

3.2.4.2. Geschätzter Personalbedarf

– ☐ Für den Vorschlag/die Initiative wird kein Personal benötigt.

– ☒ Für den Vorschlag/die Initiative wird das folgende Personal benötigt:

Schätzung in Vollzeitäquivalenten

	Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGE-SAMT**
• Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit)										
18 01 01 01 (am Sitz und in den Vertretungen der Kommission) – GD HOME	5,0	5,0	5,0	5,0	5,0	5,0	2,0	2,0	2,0	36,0
XX 01 01 02 (in den Delegationen)										
XX 01 05 01 (indirekte Forschung)										
10 01 05 01 (direkte Forschung)										
• Externes Personal (in Vollzeitäquivalenten: VZÄ)[98]										
XX 01 02 02 (VB, ÖB, ANS, LAK und JSD in den Delegationen)										
XX 01 04 **yy** 99 - am Sitz										
XX 01 04 **yy** 99 - in den Delegationen										
XX 01 05 02 (VB, ANS und LAK der indirekten Forschung)										
10 01 05 02 (VB, ANS und LAK der direkten Forschung)										
Sonstige Haushaltslinien (bitte angeben)										
INSGESAMT	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**2,0**	**2,0**	**2,0**	**36,0**

18 steht für den jeweiligen Haushaltstitel bzw. Politikbereich.

Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD oder GD-interne Personalumsetzung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

Beschreibung der auszuführenden Aufgaben:

Projektüberwachung und Folgemaßnahmen. Drei Beamte für die Folgemaßnahmen. Die Mitarbeiter übernehmen die Aufgaben der Kommission bei der Durchführung des Programms: die Überprüfung der Übereinstimmung mit dem Legislativvorschlag, die Lösung diesbezüglicher Probleme, die Erstellung von Berichten an das Europäische Parlament und den Rat und die Bewertung der Fortschritte der Mitgliedstaaten. Da es sich bei dem Programm um eine zusätzliche Maßnahme zur bestehenden Arbeitsbelastung handelt, ist zusätzliches Personal erforderlich. Diese Personalaufstockung ist zeitlich begrenzt und lediglich für die Entwicklungsphase vorgesehen.

Verwaltung des UMF

Die Kommission übernimmt die tägliche Verwaltung des UMF-Standards. Hierfür sind zwei Beamte erforderlich: ein Experte im Bereich der Strafverfolgung und eine weitere Person mit soliden Kenntnissen in Geschäftsprozessmodellierung und IKT-Kenntnissen.

Mit dem universellen Nachrichtenformat (Universal Message Format – UMF) wird ein Standard für den strukturierten grenzübergreifenden Informationsaustausch zwischen Informationssystemen, Behörden und/oder

98 VB = Vertragsbedienstete, ÖB = örtliche Bedienstete, ANS = abgeordnete nationale Sachverständige, LAK = Leiharbeitskräfte, JSD = junge Sachverständige in Delegationen.

99 Teilobergrenze für aus operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

Organisationen im Bereich Justiz und Inneres festgelegt. Durch das UMF werden ein gemeinsames Vokabular und logische Strukturen für üblicherweise ausgetauschte Informationen vorgegeben, damit die ausgetauschten Inhalte einheitlich und semantisch gleichwertig erstellt und gelesen werden können und somit die Interoperabilität verbessert wird.

Zur Gewährleistung einheitlicher Bedingungen für die Implementierung des universellen Nachrichtenformats wird vorgeschlagen, der Kommission Durchführungsbefugnisse zu übertragen. Es wird vorgeschlagen, dass diese Befugnisse im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren, ausgeübt werden.

3.2.5. Vereinbarkeit mit dem mehrjährigen Finanzrahmen

– ☐ Der Vorschlag/Die Initiative ist mit dem mehrjährigen Finanzrahmen vereinbar.

– ☒ Der Vorschlag/Die Initiative erfordert eine Anpassung der betreffenden Rubrik des mehrjährigen Finanzrahmens.

Bitte erläutern Sie die erforderliche Anpassung unter Angabe der betreffenden Haushaltslinien und der entsprechenden Beträge.

Die Verordnung über den Fonds für die innere Sicherheit (ISF) – Grenzen ist das Finanzierungsinstrument, das die Mittel für die Umsetzung der Interoperabilitätsinitiative enthält.

Artikel 5 Buchstabe b dieser Verordnung sieht vor, dass 791 Mio. EUR im Wege eines Programms für die Entwicklung von auf bestehenden und/oder neuen IT-Systemen basierenden IT-Systemen zur Unterstützung der Steuerung von Migrationsströmen über die Außengrenzen verwendet werden, sofern die entsprechenden Rechtsakte der Union angenommen werden und die in Artikel 15 festgelegten Bedingungen erfüllt sind. Von diesen 791 Mio. EUR sind 480,2 Mio. EUR für die Entwicklung des EES, 210 Mio. EUR für das ETIAS und 67,9 Mio. EUR für die Überarbeitung des SIS II vorgesehen. Der Restbetrag (32,9 Mio. EUR) ist nach dem Verfahren des ISF – Grenzen neu zuzuweisen. **Gemäß dem vorliegenden Vorschlag ist für den Zeitraum des derzeitigen mehrjährigen Finanzrahmens ein Betrag von 32,1 Mio. EUR erforderlich, der aus den restlichen Haushaltsmitteln gedeckt werden kann**.

Der im vorstehenden Feld genannte erforderliche Betrag von 32,1 Mio. EUR ist das Ergebnis der folgenden Berechnung:

VERPFLICHTUNGEN										
3.2. Geschätzte Auswirkungen auf die Ausgaben GD HOME										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Insges. (horiz.)**
18 02 01 03 - Intelligente Grenzen (einschl. Unterstützung für die MS)	0	0	43,150	48,150	45,000	0	0	0	0	136,300
Insgesamt (1)	**0**	**0**	**43,150**	**48,150**	**45,000**	**0**	**0**	**0**	**0**	**136,300**
18 02 07 -3.2. eu-LISA										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Insges. (Formel)**
T1: Personalausgaben	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
T2: Infrastruktur- und Betriebsausgaben	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
T3: Operative Ausgaben	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Insgesamt (2)	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**
		22,861							**202,181**	**225,041**
18 02 04 -3.2. Europol										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Insges. (Formel)**
T1: Personalausgaben	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
T2: Infrastruktur- und Betriebsausgaben	0	0	0	0	0	0	0	0	0	0
T3: Operative Ausgaben	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
Insgesamt (3)	**0,690**	**8,382**	**8,382**	**3,589**	**3,589**	**3,382**	**8,732**	**8,732**	**3,382**	**48,860**
		9,072							39,788	48,860
18 02 05 -3.2. CEPOL										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Insges. (Formel)**
T1: Personalausgaben	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
T2: Infrastruktur- und Betriebsausgaben	0	0	0	0	0	0	0	0	0	0
T3: Operative Ausgaben	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Insgesamt (4)	**0**	**0,144**	**0,384**	**0,482**	**0,208**	**0,208**	**0,208**	**0,208**	**0,208**	**2,050**
		0,144							**1,906**	**2,050**
18 02 03 -3.2. Frontex - Europäische Grenz- und Küstenwache										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Insges. (Formel)**
T1: Personalausgaben	0	0	0	0,350	1,400	0,233	0	0	0	1,983
T2: Infrastruktur- und Betriebsausgaben	0	0	0	0,075	0,300	0,050	0	0	0	0,425
T3: Operative Ausgaben	0	0	0	0,183	2,200	0	0	0	0	2,383
Insgesamt (5)	**0**	**0**	**0**	**0,608**	**3,900**	**0,283**	**0**	**0**	**0**	**4,792**
		0							**4,792**	**4,792**
INSGESAMT (1)+(2)+(3)+(4)+(5)	6,520	25,556	103,659	97,578	82,350	24,243	27,549	27,469	22,119	417,043
		32,076							384,966	
3.2. GD HOME Rubrik 5 "Verwaltungsausgaben"										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Insgesamt**
Insgesamt (6)	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695
INSGESAMT (1)+(2)+(3)+(4)+(5)+(6)	7,533	26,569	104,672	98,591	83,363	25,256	28,088	28,008	22,658	424,738

– ☐ Der Vorschlag/Die Initiative erfordert eine Inanspruchnahme des Flexibilitätsinstruments oder eine Änderung des mehrjährigen Finanzrahmens.

3.2.6. Finanzierungsbeteiligung Dritter

– Der Vorschlag/Die Initiative **sieht keine** Kofinanzierung durch Dritte vor.

3.3. Geschätzte Auswirkungen auf die Einnahmen

– ☐ Der Vorschlag/Die Initiative wirkt sich nicht auf die Einnahmen aus.

– ☒ Der Vorschlag/Die Initiative wirkt sich auf die Einnahmen aus, und zwar:

– ☐ auf die Eigenmittel

– ☒ auf die sonstigen Einnahmen

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Für das laufende Haushaltsjahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative[100]								
		Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**
Artikel 6313 - Beitrag Schengen-assoziierter Staaten (CH, NO, LI, IS)		pm	pm	pm	pm	pm	pm	pm	pm	pm

Bitte geben Sie für die sonstigen zweckgebundenen Einnahmen die betreffende(n) Ausgabenlinie(n) an.

18 02 07

Bitte geben Sie an, wie die Auswirkungen auf die Einnahmen berechnet werden.

Die Mittel enthalten einen Beitrag der Länder, die durch entsprechende Abkommen bei der Umsetzung, Anwendung und Weiterentwicklung des Schengen-Besitzstands und Eurodac-bezogener Maßnahmen assoziiert sind.

[100] Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d. h. abzüglich 25 % für Erhebungskosten, anzugeben.