



Brüssel, den 20.6.2022  
COM(2021) 784 final/2

2021/0410 (COD)

## CORRIGENDUM

This document corrects document COM(2021) 784 final of 8.12.2021

Concerns all language versions

Deletion of Article 58 (on the Burden of proof) and replacement of Article 61 (on Communication of personal data to third countries and international organisations)

The text shall read as follows:

Vorschlag für eine

## **VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES**

**über den automatisierten Datenaustausch für die polizeiliche Zusammenarbeit („Prüm II“) und zur Änderung der Beschlüsse 2008/615/JI und 2008/616/JI des Rates sowie der Verordnungen (EU) 2018/1726, 2019/817 und 2019/818 des Europäischen Parlaments und des Rates**

{SEC(2021) 421 final} - {SWD(2021) 378 final} - {SWD(2021) 379 final}

## BEGRÜNDUNG

### KONTEXT DES VORSCHLAGS

#### • Gründe für den Vorschlag

Die Kriminalität in ganz Europa untergräbt die Sicherheit und das Wohlergehen der EU-Bürgerinnen und -Bürger. Für eine wirksame Bekämpfung der Kriminalität benötigen die Strafverfolgungsbehörden robuste und leistungsfähige Instrumente. Zusammenarbeit und Informationsaustausch sind die wirksamsten Mittel zur Bekämpfung der Kriminalität und zur Durchsetzung von Recht und Gesetz.<sup>1</sup> Im Jahr 2021 waren mehr als 70 % der organisierten kriminellen Gruppen in mehr als drei Mitgliedstaaten aktiv.<sup>2</sup> Selbst ein scheinbar rein lokales Verbrechen kann einen Bezug zu anderen Orten in Europa haben, an denen derselbe Täter seine Straftaten verübt hat. Ebenso sind die Verbindungen der vermutlich lokalen Kriminalität zu den Strukturen und Operationen der organisierten Kriminalität oft nicht offensichtlich. Daher müssen die Strafverfolgungsbehörden in der Lage sein, Daten zeitnah auszutauschen, um die Kriminalität wirksam bekämpfen zu können. Die EU hat den Strafverfolgungsbehörden bereits eine Reihe von Instrumenten zur Erleichterung des Informationsaustauschs zur Verfügung gestellt, die sich bei der Aufdeckung von kriminellen Tätigkeiten und Netzen als maßgeblich erwiesen haben,<sup>3</sup> aber es gibt immer noch Informationslücken, die geschlossen werden müssen. Da die Daten in verschiedenen nationalen IT-Systemen und in großen IT-Systemen auf EU-Ebene getrennt gespeichert werden, muss sichergestellt werden, dass die Systeme miteinander kompatibel sind.

In einem Raum ohne Kontrollen an den Binnengrenzen (Schengen-Raum) gibt es immer noch Grenzen und Hindernisse für den Datenaustausch zwischen den Strafverfolgungsbehörden,<sup>4</sup> was zu blinden Flecken und Schlupflöchern für zahlreiche Kriminelle und Terroristen führt, die in mehr als einem Mitgliedstaat agieren. Diese Initiative und der gleichzeitig angenommene Vorschlag für eine Richtlinie über den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten<sup>5</sup> zielen darauf ab, den Informationsaustausch zwischen den Mitgliedstaaten zu verstärken und somit den Strafverfolgungsbehörden der EU bessere Instrumente zur Bekämpfung von Kriminalität und Terrorismus an die Hand zu geben.<sup>6</sup>

Seit mehr als zehn Jahren ermöglicht der Prüm-Rahmen den Strafverfolgungsbehörden in der EU den Austausch von Informationen. In den Prüm-Beschlüssen<sup>7</sup>, die im Jahr 2008 mit dem Ziel verabschiedet wurden, die grenzüberschreitende polizeiliche und justizielle Zusammenarbeit in Strafsachen zu unterstützen, ist der automatische Austausch bestimmter Daten (DNA-Profile, Fingerabdrücke und Fahrzeugregisterdaten) zwischen den für die Verhütung, Aufdeckung und Untersuchung von Straftaten zuständigen Behörden vorgesehen. Der Prüm-Rahmen trägt erfolgreich zur Bekämpfung von Kriminalität und Terrorismus in der EU bei, aber es gibt immer noch Lücken im Bereich des Informationsaustauschs und somit gibt es Raum für weitere Verbesserungen.

---

<sup>1</sup> Siehe die EU-Strategie für eine Sicherheitsunion 2020 (COM(2020) 605 final vom 24.7.2020).

<sup>2</sup> Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität in der EU 2021.

<sup>3</sup> EU-Strategie zur Bekämpfung der organisierten Kriminalität 2021-2025 (COM(2021) 170 final vom 14.4.2021).

<sup>4</sup> Dies betrifft etwa die Art und Weise, wie bestimmte Datenkategorien ausgetauscht werden, den dafür verwendeten Kanal, die geltenden Fristen usw.

<sup>5</sup> [Verweis].

<sup>6</sup> Mitteilung über eine Strategie für einen reibungslos funktionierenden und resilienten Schengen-Raum (COM(2021) 277 final vom 2.6.2021).

<sup>7</sup> Beschluss 2008/615/JI des Rates zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität und Beschluss 2008/616/JI des Rates zur Durchführung des Beschlusses 2008/615/JI. Die Beschlüsse des Rates stützen sich auf den Prüm-Vertrag von 2005.

In den Schlussfolgerungen des Rates zur Umsetzung der Prüm-Beschlüsse zehn Jahre nach ihrer Annahme wurde die Bedeutung des automatisierten Abrufs und Abgleichs von DNA-Profilen, daktyloskopischen Daten und Fahrzeugregisterdaten für die Bekämpfung von Terrorismus und grenzüberschreitender Kriminalität hervorgehoben. Der Rat forderte die Kommission ferner auf, eine Überarbeitung der Prüm-Beschlüsse in Erwägung zu ziehen, um deren Anwendungsbereich auszuweiten und zu diesem Zweck die nötigen technischen und rechtlichen Anforderungen zu aktualisieren.<sup>8</sup>

Prüm II baut auf dem bestehenden Prüm-Rahmen auf, stärkt und modernisiert ihn und ermöglicht die Interoperabilität mit anderen EU-Informationssystemen. Dadurch wird sichergestellt, dass alle relevanten Daten, die den Strafverfolgungsbehörden in einem Mitgliedstaat zur Verfügung stehen, von den Strafverfolgungsbehörden in anderen Mitgliedstaaten genutzt werden können. Dadurch wird zudem sichergestellt, dass Europol die Mitgliedstaaten im Zusammenhang mit dem Prüm-Rahmen unterstützen kann. Diese Initiative sieht die Schaffung einer neuen Infrastruktur vor, die einen einfacheren und schnelleren Datenaustausch zwischen den Mitgliedstaaten ermöglicht und ein hohes Maß an Schutz der Grundrechte gewährleistet.

- **Ziele des Vorschlags**

Das allgemeine Ziel dieses Vorschlags resultiert aus dem im Vertrag verankerten Ziel eines Beitrags zur inneren Sicherheit der Europäischen Union. Zu den Maßnahmen, die zu diesem Zweck ergriffen werden, gehören die Erhebung, Speicherung, Verarbeitung, Analyse und der Austausch relevanter Informationen.<sup>9</sup> Das allgemeine Ziel dieses Instruments besteht somit darin, den Informationsaustausch zum Zwecke der Verhütung, Aufdeckung und Untersuchung von Straftaten und terroristischen Straftaten zwischen den Strafverfolgungsbehörden der Mitgliedstaaten, aber auch mit Europol als EU-Drehscheibe für strafrechtliche Informationen zu verbessern, zu straffen und zu erleichtern.

Die spezifischen politischen Ziele dieses Vorschlags lauten:

- a) Bereitstellung einer technischen Lösung für einen effizienten automatisierten Datenaustausch zwischen den Strafverfolgungsbehörden, um sie auf einschlägige Daten hinzuweisen, die in der nationalen Datenbank eines anderen Mitgliedstaats verfügbar sind,
- b) Sicherstellung, dass allen zuständigen Strafverfolgungsbehörden mehr einschlägige Daten (in Bezug auf die Datenkategorien) aus nationalen Datenbanken in anderen Mitgliedstaaten zur Verfügung stehen,
- c) Sicherstellung, dass den Strafverfolgungsbehörden einschlägige Daten (in Bezug auf die Datenquellen) aus den Europol-Datenbanken zur Verfügung stehen,
- d) Gewährleistung eines effizienten Zugriffs der Strafverfolgungsbehörden auf die tatsächlichen Daten, die einem „Treffer“ entsprechen und in der nationalen Datenbank eines anderen Mitgliedstaats abrufbar sind.

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

In der jüngsten Schengen-Strategie<sup>10</sup> wurden mehrere Maßnahmen zur Intensivierung der polizeilichen Zusammenarbeit und des Informationsaustauschs zwischen den Strafverfolgungsbehörden angekündigt, um die Sicherheit in einem von Natur aus interdependenten Raum ohne Binnengrenzen zu erhöhen. Zusammen mit dem Vorschlag für eine Richtlinie über den

---

<sup>8</sup> Schlussfolgerungen des Rates zur Umsetzung der „PRÜMER BESCHLÜSSE“ zehn Jahre nach ihrer Annahme (Dokument 11227/18), <https://data.consilium.europa.eu/doc/document/ST-11227-2018-INIT/de/pdf>.

<sup>9</sup> Artikel 87 Absatz 2 Buchstabe a AEUV.

<sup>10</sup> Mitteilung der Kommission an das Europäische Parlament und den Rat „Strategie für einen reibungslos funktionierenden und resilienten Schengen-Raum“ (COM(2021) 277 final vom 2.6.2021).

Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten trägt dieser Vorschlag zu den Zielen dieser Strategie bei, indem sichergestellt wird, dass die Strafverfolgungsbehörden eines Mitgliedstaats Zugriff auf dieselben Informationen haben, die ihren Kollegen in einem anderen Mitgliedstaat zur Verfügung stehen.

Der Vorschlag fügt sich in den größeren Rahmen der groß angelegten EU-Informationssysteme ein, die sich seit der Annahme des Prüm-Rahmens erheblich weiterentwickelt haben. Dazu gehören auch die drei zentralen Informationssysteme der EU, die bereits in Betrieb sind: das Schengener Informationssystem (SIS), das Visa-Informationssystem (VIS) und das Eurodac-System.<sup>11</sup> Derzeit sind drei neue Systeme in der Entwicklungsphase: das Einreise-/Ausreisensystem (Entry/Exit System, EES), das Europäische Reiseinformations- und -genehmigungssystem (European Travel Information and Authorisation System, ETIAS) und das zentralisierte System für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen vorliegen (ECRIS-TCN-System).<sup>12</sup> Alle diese derzeitigen und künftigen Systeme sind durch den Interoperabilitätsrahmen für die EU-Informationssysteme<sup>13</sup> für das Sicherheits-, Grenz- und Migrationsmanagement miteinander verbunden, der im Jahr 2019 angenommen wurde und derzeit in Betrieb genommen wird. Die in diesem Vorschlag enthaltenen Änderungen zielen darauf ab, den Prüm-Rahmen an den Interoperabilitätsrahmen anzugleichen, insbesondere in Bezug auf den Datenaustausch und die Gesamtarchitektur, die durch die Interoperabilität der EU-Informationssysteme geschaffen wird. Dies würde einen schnellen und kontrollierten Zugriff auf die Informationen ermöglichen, die die Strafverfolgungsbehörden zur Erfüllung ihrer Aufgaben benötigen und für die sie Zugriffsrechte haben.

Das SIS enthält bereits Ausschreibungen von Vermissten und ermöglicht die Suche anhand von Fingerabdrücken. Das SIS ist ein verwertbares, zentralisiertes Informationssystem mit Treffer-/Kein-Treffer-Verfahren, auf das eine große Zahl von Endnutzern direkten Zugriff hat und das Ausschreibungen enthält, die eine sofortige Reaktion vor Ort ermöglichen, wobei Maßnahmen in Bezug auf den Gegenstand der Ausschreibung ergriffen werden können. Das SIS wird hauptsächlich bei Polizei-, Grenz- und Zollkontrollen sowie von Visum- und Einwanderungsbehörden bei ihren Routineverfahren und -kontrollen eingesetzt.

Im Gegensatz dazu gibt es im Prüm-Rahmen keine zentrale Komponente/Datenbank auf EU-Ebene, und er wird nur bei strafrechtlichen Ermittlungen verwendet. Er ermöglicht anderen Mitgliedstaaten den Zugriff auf die entpersonalisierten Teilsätze der nationalen DNA- und Fingerabdruckdatenbanken aller angeschlossenen Mitgliedstaaten. Dieser Zugriff wird nur den nationalen Kontaktstellen gewährt. Zwar wird die Antwort „Treffer/Kein-Treffer“ innerhalb von Sekunden oder Minuten gegeben, doch kann es Wochen oder sogar Monate dauern, bis die entsprechenden personenbezogenen Daten zu dem Treffer vorliegen.

---

<sup>11</sup> Das SIS unterstützt die zuständigen Behörden in der EU bei der Erhaltung der inneren Sicherheit angesichts der fehlenden Kontrollen an den Binnengrenzen, und das VIS ermöglicht den Schengen-Staaten den Austausch von Visadaten. Mit dem Eurodac-System wird eine EU-Datenbank für Fingerabdrücke von Asylbewerbern eingerichtet, die es den Mitgliedstaaten ermöglicht, die Fingerabdrücke von Asylbewerbern zu vergleichen, um festzustellen, ob sie zuvor einen Asylantrag gestellt haben oder über einen anderen Mitgliedstaat irregulär in die EU eingereist sind.

<sup>12</sup> Ziel des EES und des ETIAS ist es, die Sicherheitskontrollen von nicht visumpflichtigen Reisenden zu verschärfen, indem ermöglicht wird, vorab Kontrollen zu irregulärer Migration und Sicherheitsüberprüfungen vorzunehmen. Mit dem ECRIS-TCN-System wird die festgestellte Lücke im Informationsaustausch zwischen den Mitgliedstaaten über verurteilte Drittstaatsangehörige geschlossen.

<sup>13</sup> Verordnung (EU) 2019/817 und Verordnung (EU) 2019/818.

## 2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISSMÄSSIGKEIT

### • Rechtsgrundlage

Rechtsgrundlage dieses Vorschlags bilden folgende Artikel des Vertrags über die Arbeitsweise der Europäischen Union (AEUV): Artikel 16 Absatz 2, 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 87 Absatz 2 Buchstabe a ist die Union befugt, Maßnahmen zum Einholen, Speichern, Verarbeiten, Analysieren und Austauschen sachdienlicher Informationen zu erlassen, um die polizeiliche Zusammenarbeit zwischen den zuständigen Behörden der Mitgliedstaaten, einschließlich der Polizei, des Zolls und anderer auf die Verhütung, Aufdeckung oder Untersuchung von Straftaten spezialisierter Strafverfolgungsbehörden zu gewährleisten. Gemäß Artikel 88 Absatz 2 können das Europäische Parlament und der Rat den Aufbau, die Arbeitsweise, den Tätigkeitsbereich und die Aufgaben von Europol festlegen.

### • Subsidiarität

Aufgrund des grenzüberschreitenden Charakters der Bekämpfung der Kriminalität und der Sicherheitsfragen kann der Informationsaustausch zwischen den Polizei- und Strafverfolgungsbehörden innerhalb der Europäischen Union von den Mitgliedstaaten allein nicht ausreichend verbessert werden. In diesem Bereich müssen sich die Mitgliedstaaten gegenseitig unterstützen.

Mit mehreren Durchführungsprojekten auf EU-Ebene<sup>14</sup> haben die Mitgliedstaaten versucht, die Unzulänglichkeiten des derzeitigen Prüm-Rahmens zu beheben.<sup>15</sup> Trotz all dieser Maßnahmen blieben viele der im Bericht zur Durchführung des Prüm-Beschlusses 2012 beschriebenen Unzulänglichkeiten bestehen.<sup>16</sup> Dies verdeutlicht die Notwendigkeit von EU-Maßnahmen, da sich die von den Mitgliedstaaten allein durchgeführten Maßnahmen als unzureichend erwiesen haben, um die Grenzen des derzeitigen Prüm-Rahmens zu überwinden.

Gemeinsame Vorschriften, Normen und Anforderungen auf EU-Ebene erleichtern den Informationsaustausch und sorgen gleichzeitig für Kompatibilität zwischen den verschiedenen nationalen Systemen. Dies wiederum ermöglicht eine gewisse Automatisierung der Arbeitsabläufe beim Informationsaustausch, die die Strafverfolgungsbehörden von arbeitsintensiven manuellen Tätigkeiten entlastet.

---

<sup>14</sup> So wurde beispielsweise das Projekt Mobiles Kompetenzteam (Mobile Competence Team, MCT) (2011-2014) von Deutschland initiiert und durch das Programm der Kommission zur Kriminalprävention und Kriminalitätsbekämpfung (ISEC) finanziert. Ziel des MCT war es, den EU-Mitgliedstaaten, die noch nicht für den Austausch von DNA- und Fingerabdruckdaten bereit waren, Expertenwissen und Unterstützung zu bieten.

<sup>15</sup> Im Rahmen eines von Finnland geleiteten Projekts analysierten die Mitgliedstaaten die nach einem Treffer angewandten nationalen Verfahren. Als Ergebnis dieses Projekts wurden eine Reihe von bewährten und nicht verbindlichen Verfahren empfohlen, um den Informationsaustausch nach einem Treffer EU-weit zu optimieren (siehe Dokument 14310/2/16 REV2, nicht öffentlich).

Darüber hinaus unterstützte Europol im Zeitraum 2012-2013 die Entwicklung standardisierter Formulare, die unabhängig vom verwendeten Kommunikationskanal für den Austausch von Folgeinformationen verwendet werden sollen (siehe Dokument 9383/13 für weitere Informationen). Es ist jedoch nicht bekannt, in welchem Umfang die nationalen Kontaktstellen diese Formulare verwenden.

<sup>16</sup>COM(2012) 732 final.

- **Verhältnismäßigkeit**

Wie in der Folgenabschätzung zu der vorgeschlagenen Verordnung ausführlich erläutert, werden die im Rahmen dieses Vorschlags getroffenen politischen Entscheidungen als verhältnismäßig erachtet. Dies liegt daran, dass sie nicht über das zur Erreichung der festgelegten Ziele erforderliche Maß hinausgehen.

In dem Vorschlag ist die Einrichtung **zentraler Router** (Prüm-II-Router und EPRIS) vorgesehen, die jeweils als Verbindungspunkt zwischen den Mitgliedstaaten fungieren würden. Dabei handelt es sich um einen hybriden Ansatz zwischen einer dezentralen und einer zentralen Lösung, ohne dass die Daten auf zentraler Ebene gespeichert werden. Das bedeutet, dass die nationalen Datenbanken der einzelnen Mitgliedstaaten alle mit dem zentralen Router anstatt untereinander verbunden werden. Diese Router würden als Schnittstellen fungieren, die Suchvorgänge und Antworten an die nationalen Systeme weiterleiten, ohne neue Datenprozesse zu schaffen, die Zugriffsrechte zu erweitern oder nationale Datenbanken zu ersetzen. Auf diese Weise würde sichergestellt, dass die Strafverfolgungsbehörden im Einklang mit ihren Zugriffsrechten einen schnellen und kontrollierten Zugriff auf die Informationen haben, die sie zur Erfüllung ihrer Aufgaben benötigen. Mit dem Router würden die Mitgliedstaaten den bestehenden und künftigen Datenaustausch auf der Grundlage des Prüm-Rahmens leichter durchführen können.

Der **automatisierte Austausch zusätzlicher Datenkategorien**, wie Gesichtsbilder und Kriminalakten, ist für effektive strafrechtliche Ermittlungen und für die Identifizierung von Straftätern von entscheidender Bedeutung. Die Einführung dieser zusätzlichen Datenkategorien würde nicht zur Speicherung neuer Datenkategorien führen, da die Mitgliedstaaten diese Daten bereits nach nationalem Recht erheben und in nationalen Datenbanken speichern. Der Austausch dieser neuen Datenkategorien würde eine neue Verarbeitung von Daten darstellen. Sie wäre jedoch auf das zur Erreichung ihres Zwecks notwendige Maß beschränkt und würde nur in Einzelfällen einen Vergleich der Daten ermöglichen. In dem Vorschlag sind auch eine Reihe von Sicherheitsgarantien vorgesehen (z. B. die Weitergabe vollständiger Daten nur bei einem „Treffer“ nach einer Abfrage).

Mit diesem Vorschlag wird **Europol** integraler Bestandteil des Prüm-Rahmens, indem die Mitgliedstaaten in die Lage versetzt werden, biometrische Daten aus Drittländern, die bei Europol gespeichert sind, automatisch zu überprüfen. Zweitens könnte Europol auch Daten aus Drittländern mit den nationalen Datenbanken der Mitgliedstaaten abgleichen. Diese beiden Aspekte der Beteiligung von Europol am neuen Prüm-Rahmen würden im Einklang mit den in der Verordnung (EU) 2016/794 festgelegten Aufgaben von Europol gewährleisten, dass keine Lücken in Bezug auf die von Drittländern erhaltenen Daten über schwerwiegende Straftaten und Terrorismus entstehen. In einer offenen Gesellschaft in einer globalisierten Welt sind die von Drittländern bereitgestellten Daten über Straftäter und Terroristen von entscheidender Bedeutung. Damit könnten Straftäter, die in Ländern außerhalb der EU bekannt sind, identifiziert werden, während gleichzeitig strenge Garantien in Bezug auf den Schutz der Privatsphäre und der Grundrechte und -freiheiten von Personen gelten, die in den Europol-Kooperationsabkommen mit Drittländern festgelegt sind.

Das überarbeitete **Austauschverfahren im Anschluss an einen Treffer** würde durch die Vereinfachung und Optimierung des Austauschs von Strafverfolgungsinformationen zur inneren Sicherheit der Europäischen Union beitragen. Im Vergleich zur derzeitigen Situation, in der der Informationsaustausch im Anschluss an einen Treffer durch nationales Recht geregelt ist und somit unterschiedlichen Regeln und Verfahren unterliegt, würden gemeinsame Regeln zur Harmonisierung dieses zweiten Schritts des Prüm-Verfahrens allen Nutzern Vorhersehbarkeit bieten, da sie alle wüssten, welche Daten sie in diesem Schritt erhalten würden. Der Datenaustausch würde durch eine teilweise Automatisierung erleichtert, was bedeutet, dass vor einem umfassenden Austausch von Folgedaten immer noch ein menschliches Eingreifen erforderlich wäre. Die

Mitgliedstaaten würden weiterhin Eigentümer ihrer Daten bleiben und die Kontrolle über diese behalten.

- **Wahl des Instruments**

Es wird eine Verordnung des Europäischen Parlaments und des Rates vorgeschlagen. Die vorgeschlagene Rechtsvorschrift stützt sich auf einen bestehenden Rahmen von Beschlüssen des Rates, die zur grenzüberschreitenden Zusammenarbeit zwischen den EU-Mitgliedstaaten in den Bereichen Justiz und Inneres beitragen.<sup>17</sup>

Da die vorgeschlagenen Maßnahmen unmittelbar anwendbar sein und in allen Mitgliedstaaten einheitlich angewandt werden müssen und der Informationsaustausch verbessert werden soll, ist eine Verordnung das geeignete Rechtsinstrument.

### **3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG**

- **Ex-post-Bewertungen geltender Rechtsvorschriften**

Insgesamt hat die Bewertung des Prüm-Rahmens gezeigt,<sup>18</sup> dass der Abruf und der Abgleich von DNA-, Fingerabdruck- und Fahrzeugregisterdaten in den Datenbanken anderer Mitgliedstaaten zur Verhütung und Untersuchung von Straftaten von größter Bedeutung für den Schutz der inneren Sicherheit der EU und die Sicherheit der EU-Bürgerinnen und -Bürger sind. Des Weiteren ergab die Bewertung, dass die Prümer Beschlüsse dazu beigetragen haben, gemeinsame Regeln, Normen und Anforderungen auf EU-Ebene festzulegen, um den Informationsaustausch zu erleichtern und die Kompatibilität zwischen den verschiedenen nationalen Systemen zu gewährleisten.

Seit dem Ablauf der Frist für die Umsetzung des Prüm-Rahmens vor zehn Jahren hat die EU jedoch mehrere andere Maßnahmen zur Erleichterung des Informationsaustauschs zwischen den Strafverfolgungsbehörden angenommen,<sup>19</sup> darunter den Interoperabilitätsrahmen<sup>20</sup>. Außerdem wurden die Bestimmungen über die technischen Spezifikationen der Abfragen, die Sicherheitsmaßnahmen und die Kommunikation seit der Annahme der Prümer Beschlüsse im Jahr 2008 nicht aktualisiert.<sup>21</sup> Einige dieser Vorschriften sind überholt, da sich die forensische Wissenschaft und Technologie in den letzten zehn Jahren erheblich weiterentwickelt haben.

Aus der Bewertung ging auch hervor, dass die Umsetzung der Prümer Beschlüsse in den letzten zehn Jahren nur langsam vorankam und dass nicht alle Mitgliedstaaten die notwendigen Schritte zur

---

<sup>17</sup> Beschluss 2008/615/JI des Rates zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, und Beschluss 2008/616/JI des Rates zur Durchführung des Beschlusses 2008/615/JI.

<sup>18</sup> Anhang 4 der begleitenden Arbeitsunterlage der Kommissionsdienststellen [Verweis auf die Folgenabschätzung von Prüm].

<sup>19</sup> Beispielsweise das Europol-Informationssystem (EIS), die Informationssysteme von Interpol und das Schengener Informationssystem (SIS).

<sup>20</sup> Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates;

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

<sup>21</sup> Im Beschluss 2008/616/JI des Rates enthalten.

Umsetzung der Beschlüsse unternommen haben.<sup>22</sup> Folglich wurde eine Reihe von bilateralen Verbindungen nicht hergestellt, und Abfragen an die Datenbanken einiger Mitgliedstaaten sind nicht möglich. Die Ergebnisse der Bewertung zeigten ferner, dass die Folgemaßnahmen zu Treffern auf der Grundlage des nationalen Rechts erfolgen und daher nicht in den Anwendungsbereich der Prüm-Beschlüsse fallen. Unterschiedliche nationale Vorschriften und Verfahren können in einigen Fällen dazu führen, dass die zuständigen Behörden erst mit erheblicher Verzögerung Informationen im Anschluss an einen Treffer erhalten. Dies beeinträchtigt die Funktionsweise des Prüm-Systems und den wirksamen Informationsaustausch zwischen den Mitgliedstaaten, da die Möglichkeit, Straftäter zu identifizieren und grenzüberschreitende Verbindungen zwischen Straftaten aufzudecken, verringert wird.

Die Ergebnisse der Bewertung dienen der Vorbereitung der Folgenabschätzung und des vorliegenden Vorschlags.

- **Konsultation der Interessenträger**

Die Ausarbeitung dieses Vorschlags umfasste gezielte Konsultationen der betroffenen Interessenträger, einschließlich der Endnutzer des Systems, d. h. der Behörden der Mitgliedstaaten, die das Prüm-System für den automatisierten Datenaustausch nutzen – von Strafverfolgungs- und Justizbehörden über nationale Kfz-Zulassungsbehörden bis hin zu nationalen Datenbankverwaltern und kriminaltechnischen Labors. Auch Europol und eu-LISA wurden im Hinblick auf ihr jeweiliges Fachwissen und ihre mögliche Rolle im neuen Prüm-Rahmen konsultiert.

Die Agentur der Europäischen Union für Grundrechte (FRA) sowie Nichtregierungsorganisationen wie EDRi (European Digital Rights) und zwischenstaatliche Organisationen (Eucaris - Europäisches Informationssystem für Kraftfahrzeuge und Führerscheine) lieferten ebenfalls Beiträge, die auf ihrem Fachwissen basieren.

Im Rahmen der Konsultation zur Vorbereitung der Folgenabschätzung, die diesem Vorschlag zugrunde liegt, wurden in verschiedenen Foren Rückmeldungen von Interessenträgern eingeholt. Dazu gehörten insbesondere eine anfängliche Folgenabschätzung, eine öffentliche Konsultation und mehrere technische Workshops. Eine Durchführbarkeitsanalyse wurde auf der Grundlage von Sekundärforschung, Befragung von Fachleuten, Fragebögen und drei Experten-Workshops durchgeführt; dabei wurde untersucht, ob der Informationsaustausch im Rahmen der Prüm-Beschlüsse verbessert werden kann.

Regelmäßige Diskussionen über den Austausch von Strafverfolgungsinformationen und insbesondere über die Prüm-Beschlüsse in der Arbeitsgruppe DAPIX/IXIM des Rates<sup>23</sup> trugen ebenfalls zur Vorbereitung dieses Vorschlags bei.

Von August bis Oktober 2020 wurde eine **Folgenabschätzung in der Anfangsphase** zur Rückmeldung veröffentlicht, zu der insgesamt sechs Beiträge eingingen.<sup>24</sup>

Eine **öffentliche Konsultation**, die auf der Website der Europäischen Kommission angekündigt wurde, richtete sich an die breite Öffentlichkeit. Die Antworten bestätigten, dass der bestehende Prüm-Rahmen für die Verhütung und Untersuchung von Straftaten relevant ist und den Datenaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten verbessert hat. Der automatisierte Datenaustausch auf der Grundlage des Prüm-Rahmens hat auch Effizienzgewinne

---

<sup>22</sup> Die Kommission hat im Jahr 2016 Vertragsverletzungsverfahren gegen fünf Mitgliedstaaten eingeleitet. Im Oktober 2021 sind zwei dieser Vertragsverletzungsverfahren noch nicht abgeschlossen.

<sup>23</sup> Arbeitsgruppe des Rates für Informationsaustausch und Datenschutz (DAPIX) und ab dem 1. Januar 2020 Arbeitsgruppe für den Informationsaustausch im Bereich Justiz und Inneres (IXIM).

<sup>24</sup> Die Folgenabschätzung in der Anfangsphase und die Beiträge sind [hier](#) abrufbar.

mit sich gebracht, da nicht mehr jeder Mitgliedstaat bilateral abgefragt werden muss. In den Antworten wurde ferner bestätigt, dass der Rahmen mit den Maßnahmen der EU und der internationalen Gemeinschaft in diesem Bereich kohärent ist und im Vergleich zu dem, was die Mitgliedstaaten ohne den Prüm-Rahmen im Bereich des strafverfolungsrelevanten Informationsaustauschs erreichen könnten, einen zusätzlichen Nutzen bietet. In Bezug auf die Verbesserung des derzeitigen Rahmens stimmten die meisten Befragten darin überein, dass die Tatsache, dass einige Datenkategorien nicht durch den Rahmen abgedeckt sind und daher durch manuelle Abfragen ausgetauscht werden, einen Mangel darstellt.

Die Kommissionsdienststellen organisierten auch eine Reihe von gezielten informellen **technischen Workshops** mit Experten aus den Mitgliedstaaten und den assoziierten Schengen-Ländern. Ziel der Workshops war es, einen Meinungsaustausch zwischen den Endnutzern über die Optionen zu ermöglichen, die zur Stärkung des Prüm-Rahmens aus technischer Sicht erwogen und bewertet wurden.

Die beigelegte Folgenabschätzung enthält eine ausführlichere Beschreibung der Konsultation der Interessenträger (Anhang 2).

- **Folgenabschätzung**

Der Vorschlag wird durch eine Folgenabschätzung gestützt, die in der beigelegten Arbeitsunterlage der Kommissionsdienststellen [Verweis auf die Folgenabschätzung von Prüm] dargelegt ist. Der Ausschuss für Regulierungskontrolle prüfte den Entwurf der Folgenabschätzung in seiner Sitzung vom 14. Juli 2021 und gab am 16. Juli 2021 seine befürwortende Stellungnahme ab.

Die Folgenabschätzung ergab Folgendes:

- 1) Um eine technische Lösung für einen effizienten automatisierten Datenaustausch bereitzustellen, sollte eine hybride Lösung zwischen einem dezentralisierten und einem zentralisierten Ansatz ohne Datenspeicherung auf zentraler Ebene angewandt werden.
- 2) Um sicherzustellen, dass den Strafverfolgungsbehörden mehr einschlägige Daten (in Bezug auf die Datenkategorien) zur Verfügung stehen, sollte der Austausch von Gesichtsbildern und Kriminalakten eingeführt werden.
- 3) Um sicherzustellen, dass den Strafverfolgungsbehörden einschlägige Daten aus den Europol-Datenbanken zur Verfügung stehen, sollten die Mitgliedstaaten in der Lage sein, biometrische Daten aus Drittländern als Teil des Prüm-Rahmens automatisch bei Europol zu überprüfen. Europol sollte auch in der Lage sein, Daten aus Drittländern mit den nationalen Datenbanken der Mitgliedstaaten abzugleichen.
- 4) Um einen effizienten Zugriff auf die tatsächlichen Daten zu einem „Treffer“ zu ermöglichen, die in der nationalen Datenbank eines anderen Mitgliedstaats oder bei Europol abrufbar sind, sollte das Folgeverfahren auf EU-Ebene durch einen halbautomatischen Austausch der tatsächlichen Daten zu einem „Treffer“ geregelt werden.

Der Vorschlag wird sich vor allem dadurch positiv auswirken, dass er eine effektive Antwort auf die festgestellten Probleme darstellt und den derzeitigen Prüm-Rahmen durch gezielte und starke zusätzliche Kapazitäten verstärkt, um die Mitgliedstaaten bei der Intensivierung des Informationsaustauschs mit dem Endziel der Verhütung und Untersuchung von terroristischen und anderen Straftaten unter voller Wahrung der Grundrechte stärker zu unterstützen.

Alle bevorzugten Optionen kommen letztlich den Bürgerinnen und Bürgern zugute, die direkt und indirekt von einer besseren Bekämpfung der Kriminalität und niedrigeren Kriminalitätsraten profitieren werden. Im Hinblick auf die Effizienz sind die nationalen Strafverfolgungsbehörden die Hauptnutznießer.

Die unmittelbaren finanziellen und wirtschaftlichen Auswirkungen des Vorschlags erfordern Investitionen sowohl auf EU-Ebene als auch auf Ebene der Mitgliedstaaten. Es wird davon ausgegangen, dass die voraussichtlichen Investitionskosten durch Vorteile und Einsparungen, insbesondere auf Ebene der Mitgliedstaaten, aufgewogen werden. Abgesehen von den anfänglichen Investitionen wird die Einrichtung des zentralen Prüm Routers den Mitgliedstaaten Kosten ersparen, da der Router nicht erfordert, dass jeder Mitgliedstaat so viele Verbindungen einrichtet (und unterhält), wie es Mitgliedstaaten und Datenkategorien gibt.

- **Grundrechte**

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 Umsetzung des EU-Rechts gebunden sind (Artikel 51 Absatz 1 der Charta), und dem Grundsatz der Nichtdiskriminierung müssen die Möglichkeiten, die die vorgestellten Optionen bieten, in einem ausgewogenen Verhältnis zu der Verpflichtung stehen, der zufolge zu gewährleisten ist, dass Eingriffe in die Grundrechte, die sich daraus ergeben können, 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 Lösungen bieten die Möglichkeit, gezielte Präventivmaßnahmen zur Erhöhung der Sicherheit zu beschließen. Damit können sie dazu beitragen, das legitime Ziel der Erleichterung der Bekämpfung der Kriminalität zu verfolgen, 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.<sup>25</sup>

- **Schutz personenbezogener Daten**

Der Informationsaustausch hat Auswirkungen auf das Recht auf den Schutz personenbezogener Daten. 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 Europäischen Union betont hat,<sup>26</sup> kann das Recht auf Schutz der personenbezogenen Daten jedoch keine uneingeschränkte Geltung beanspruchen, sondern muss im Hinblick auf seine gesellschaftliche Funktion gesehen werden. Der Datenschutz und die Achtung des Privat- und Familienlebens, die durch Artikel 7 der Charta geschützt ist, hängen eng zusammen.

Für Prüm gelten die Datenschutzvorschriften der Richtlinie (EU) 2016/680. Im Prüm-Rahmen ist nämlich die Verarbeitung personenbezogener Daten im Rahmen des Informationsaustauschs zwischen den für die Verhütung und Untersuchung von Straftaten zuständigen Strafverfolgungsbehörden vorgesehen.

Der freie Datenverkehr in der EU darf 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:

- 1) Sie muss gesetzlich vorgesehen sein,
- 2) sie muss den Wesensgehalt der Rechte achten,

---

<sup>25</sup>Urteil des Gerichtshofs für Menschenrechte vom 28. Oktober 1998, Osman/Vereinigtes Königreich, Nr. 87/1997/871/1083, Rn. 116.

<sup>26</sup> Urteil des Gerichtshofs der Europäischen Union vom 9. November 2010, Volker und Markus Schecke und Eifert, verbundene Rechtssachen C-92/09 und C-93/09, ECR I-0000.

- 3) sie muss den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen,
- 4) sie muss erforderlich sein und
- 5) sie muss verhältnismäßig sein.

Wie in der Folgenabschätzung zu der vorgeschlagenen Verordnung ausführlich erläutert, trägt der 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. Der Datenzugriff ist ausschließlich den dazu ermächtigten Bediensteten der Behörden der Mitgliedstaaten oder der EU-Stellen vorbehalten, die für die festgelegten Zwecke des überarbeiteten Prüm-Rahmens zuständig sind, soweit die Daten zur Erfüllung ihrer Aufgaben im Einklang mit diesen Zwecken erforderlich sind.

Die Kommission wird zum Zeitpunkt der Veröffentlichung des Berichts zur Bewertung der Umsetzung der [Empfehlung des Rates über die operative polizeiliche Zusammenarbeit] durch die in Punkt 9 Buchstabe d dieser Empfehlung genannten Mitgliedstaaten entscheiden, ob EU-Rechtsvorschriften über die grenzüberschreitende operative polizeiliche Zusammenarbeit erforderlich sind. Sollte ein solcher Rechtsakt erforderlich sein, wird die Kommission einen Legislativvorschlag zur grenzüberschreitenden operativen polizeilichen Zusammenarbeit vorlegen, der auch die Angleichung der Bestimmungen des Beschlusses 2008/615/JI und des Beschlusses 2008/616/JI, die nicht unter diesen Vorschlag fallen, an die Richtlinie 2016/680 im Einklang mit den Ergebnissen der Bewertung nach Artikel 62 Absatz 6 der Richtlinie 2016/680 gewährleisten wird. Sollte kein Bedarf an EU-Rechtsvorschriften über die grenzüberschreitende operative polizeiliche Zusammenarbeit bestehen, wird die Kommission einen Legislativvorschlag vorlegen, um dieselbe Angleichung im Einklang mit den Ergebnissen der Bewertung gemäß Artikel 62 Absatz 6 der Richtlinie 2016/680 sicherzustellen.

#### **4. AUSWIRKUNGEN AUF DEN HAUSHALT**

Diese Gesetzgebungsinitiative würde sich auf den Haushalt und den Personalbedarf von eu-LISA und Europol auswirken.

Für eu-LISA wären für den gesamten Zeitraum des Mehrjährigen Finanzrahmens (MFR) Schätzungen zufolge zusätzliche Haushaltsmittel in Höhe von etwa 16 Mio. EUR und rund 10 zusätzliche Stellen erforderlich, um sicherzustellen, dass eu-LISA über die erforderlichen Ressourcen verfügt, um die der Agentur in diesem Verordnungsvorschlag zugewiesenen Aufgaben zu erfüllen. Die für eu-LISA bereitgestellten Mittel werden mit dem Instrument für Grenzmanagement und Visa (BMVI) verrechnet.

Für Europol wären für den gesamten MFR-Zeitraum Schätzungen zufolge zusätzliche Haushaltsmittel in Höhe von etwa 7 Mio. EUR und rund 5 zusätzliche Stellen erforderlich, um sicherzustellen, dass Europol über die erforderlichen Ressourcen verfügt, um die der Agentur in diesem Verordnungsvorschlag zugewiesenen Aufgaben zu erfüllen. Die für von Europol bereitgestellten Mittel werden mit dem Fonds für die innere Sicherheit (ISF) verrechnet.

## 5. WEITERE ANGABEN

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

Die Kommission wird sicherstellen, dass die notwendigen Vorkehrungen getroffen werden, um das Funktionieren der vorgeschlagenen Maßnahmen zu überwachen und sie anhand der wichtigsten politischen Ziele zu bewerten. Zwei Jahre nachdem die neuen Funktionen eingerichtet und in Betrieb genommen wurden, und danach alle zwei Jahre, sollten die Agenturen der Union dem Europäischen Parlament, dem Rat und der Kommission einen Bericht über die technische Funktionsweise der vorgeschlagenen neuen Maßnahmen vorlegen. Darüber hinaus sollte die Kommission drei Jahre nachdem die neuen Funktionen eingerichtet und in Betrieb genommen wurden, und danach alle vier Jahre eine Gesamtbewertung der Maßnahmen erstellen, die auch die direkten oder indirekten Auswirkungen 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 1 enthält die allgemeinen Bestimmungen für diese Verordnung mit ihrem Gegenstand, Zweck und Anwendungsbereich. Darin wird eine Liste von Definitionen aufgeführt und es wird darauf hingewiesen, dass bei der Verarbeitung personenbezogener Daten für die Zwecke dieser Verordnung der Grundsatz der Nichtdiskriminierung und andere Grundrechte zu beachten sind.

Kapitel 2 enthält die Bestimmungen für den Austausch der in dieser Verordnung vorgesehenen Datenkategorien, nämlich den Austausch von DNA-Profilen, daktyloskopischen Daten, Fahrzeugregisterdaten, Gesichtsbildern und Kriminalakten. Die Grundsätze für den Austausch, die automatisierte Suche nach Daten und die Regeln für Anfragen und Antworten werden in einem eigenen Abschnitt für jede Datenkategorie erläutert. Kapitel 2 enthält auch gemeinsame Bestimmungen für den Datenaustausch, die Einrichtung nationaler Kontaktstellen und Durchführungsmaßnahmen.

In Kapitel 3 werden die Einzelheiten der neuen (technischen) Architektur für den Datenaustausch dargelegt. Der erste Abschnitt dieses Kapitels enthält Bestimmungen, in denen der zentrale Router, die Nutzung des Routers und die Abfrage von Daten beschrieben werden. Zur Festlegung der technischen Verfahren für diese Abfragen sind Durchführungsrechtsakte erforderlich. Dieser Abschnitt enthält auch Bestimmungen über die Interoperabilität zwischen dem Router und dem gemeinsamen Speicher für Identitätsdaten zum Zwecke des Zugriffs durch die Strafverfolgungsbehörden, die Führung von Protokollen über alle Datenverarbeitungsvorgänge im Router, die Qualitätskontrolle und die Meldeverfahren für den Fall, dass die Nutzung des Routers aus technischen Gründen nicht möglich ist. Im zweiten Abschnitt werden Einzelheiten zur Nutzung des Europäischen Kriminalaktennachweissystems (EPRIS) für den Austausch von Kriminalakten erläutert. Dieser Abschnitt enthält auch Bestimmungen über die Führung von Protokollen über alle Datenverarbeitungsvorgänge im EPRIS und über die Meldeverfahren im Falle der technischen Unmöglichkeit, das EPRIS zu nutzen.

In Kapitel 4 werden die Verfahren für den Austausch von Daten im Anschluss an eine Übereinstimmung beschrieben. Es enthält eine Bestimmung über den automatisierten Austausch von Kerndaten, wobei die Daten auf das beschränkt sind, was für die Identifizierung der betreffenden Person erforderlich ist, sowie eine Bestimmung über den Austausch von Daten in jeder Phase des Verfahrens gemäß dieser Verordnung, die in dieser Verordnung nicht ausdrücklich beschrieben sind.

Kapitel 5 enthält Bestimmungen über den Zugriff der Mitgliedstaaten auf die von Europol gespeicherten biometrischen Daten aus Drittländern und über den Zugriff von Europol auf die in den Datenbanken der Mitgliedstaaten gespeicherten Daten.

Kapitel 6 zum Datenschutz enthält Bestimmungen, mit denen sichergestellt wird, dass die Daten im Rahmen dieser Verordnung im Einklang mit den Bestimmungen der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates rechtmäßig und ordnungsgemäß verarbeitet werden.<sup>27</sup> Darin wird erläutert, wer für die Verarbeitung von Daten im Rahmen dieser Verordnung zuständig ist. Es enthält Maßnahmen, die von eu-LISA und den Behörden der Mitgliedstaaten verlangt werden, um die Sicherheit der Datenverarbeitung, den angemessenen Umgang mit Sicherheitsvorfällen und die Überwachung der Einhaltung der in dieser Verordnung vorgesehenen Maßnahmen zu gewährleisten. In diesem Kapitel werden auch die Bestimmungen hinsichtlich Überwachung und Prüfung im Zusammenhang mit dem Datenschutz dargelegt. Darin wird der Grundsatz unterstrichen, dass Daten, die im Rahmen dieser Verordnung verarbeitet werden, nicht automatisiert an ein Drittland oder eine internationale Organisation übermittelt oder ihnen zur Verfügung gestellt werden dürfen.

In Kapitel 7 werden die Zuständigkeiten der Mitgliedstaaten, von Europol bzw. von eu-LISA bei der Durchführung der Maßnahmen dieser Verordnung im Einzelnen dargelegt.

Kapitel 8 betrifft Änderungen an anderen bestehenden Instrumenten, nämlich den Beschlüssen 2008/615/JI und 2008/616/JI, der Verordnung (EU) 2018/1726, der Verordnung (EU) 2019/817 und der Verordnung (EU) 2019/818.

In Kapitel 9 über die Schlussbestimmungen werden die Einzelheiten in Bezug auf Berichterstattung und Statistiken, Kosten, Mitteilungen, Übergangsbestimmungen und Ausnahmeregelungen dargelegt. Außerdem werden darin die Voraussetzungen für die Inbetriebnahme der im Rahmen dieser Verordnung vorgeschlagenen Maßnahmen festgelegt. Das Kapitel sieht auch die Einsetzung eines Ausschusses und die Erstellung eines Leitfadens zur Unterstützung der Durchführung und Verwaltung dieser Verordnung vor. Es enthält auch eine Bestimmung über die Überwachung und Bewertung sowie eine Bestimmung über das Inkrafttreten und die Anwendbarkeit dieser Verordnung. Diese Verordnung ersetzt insbesondere die Artikel 2 bis 6 und die Abschnitte 2 und 3 von Kapitel 2 des Beschlusses 2008/615/JI des Rates sowie die Kapitel 2 bis 5 und die Artikel 18, 20 und 21 des Beschlusses 2008/616/JI des Rates, die folglich ab dem Zeitpunkt der Anwendung dieser Verordnung aus den genannten Beschlüssen des Rates gestrichen werden. Diese Änderungen haben zur Folge, dass die ersetzten und gestrichenen Bestimmungen für keinen Mitgliedstaat mehr gelten.

---

<sup>27</sup> Nach den Feststellungen der Kommission in ihrer Mitteilung vom 24. Juni 2020 über weiteres Vorgehen hinsichtlich der Angleichung des früheren Besitzstands des dritten Pfeilers an die Datenschutzvorschriften (COM(2020) 262 final).

Vorschlag für eine

## VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

### über den automatisierten Datenaustausch für die polizeiliche Zusammenarbeit („Prüm II“) und zur Änderung der Beschlüsse 2008/615/JI und 2008/616/JI des Rates sowie der Verordnungen (EU) 2018/1726, 2019/817 und 2019/818 des Europäischen Parlaments und des Rates

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16 Absatz 2, 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 Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses<sup>28</sup>,

nach Stellungnahme des Ausschusses der Regionen<sup>29</sup>,

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

- (1) Die Union verfolgt das Ziel, ihren Bürgerinnen und Bürgern einen Raum der Freiheit, der Sicherheit und des Rechts ohne Binnengrenzen zu bieten, in dem der freie Personenverkehr gewährleistet ist. Dieses Ziel sollte unter anderem mittels geeigneter Maßnahmen zur Verhütung und Bekämpfung von Kriminalität, einschließlich der organisierten Kriminalität und des Terrorismus, erreicht werden.
- (2) Dieses Ziel setzt voraus, dass die Strafverfolgungsbehörden Daten effizient und zeitnah austauschen, um Kriminalität wirksam zu bekämpfen.
- (3) Ziel dieser Verordnung ist es daher, den Austausch kriminalpolizeilicher Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten, aber auch mit der durch die Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates<sup>30</sup> errichteten Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) als Plattform der Union für kriminalpolizeiliche Informationen zu verbessern, zu straffen und zu erleichtern.
- (4) Die Beschlüsse 2008/615/JI<sup>31</sup> und 2008/616/JI<sup>32</sup> des Rates zur Festlegung von Vorschriften für den Informationsaustausch zwischen den für die Verhütung und Untersuchung von

<sup>28</sup> ABl. C ... vom ..., S. ....

<sup>29</sup> ABl. C ... vom ..., S. ....

<sup>30</sup> 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 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).

<sup>31</sup> Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6.8.2008, S. 1).

Straftaten zuständigen Behörden durch die automatisierte Übermittlung von DNA-Profilen, daktyloskopischen Daten und bestimmten Fahrzeugregisterdaten haben sich für die Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität als wichtig erwiesen.

- (5) In dieser Verordnung sollten die Bedingungen und Verfahren für die automatisierte Übermittlung von DNA-Profilen, daktyloskopischen Daten, Fahrzeugregisterdaten, Gesichtsbildern und Kriminalakten festgelegt werden. Dies sollte die Verarbeitung dieser Daten im Schengener Informationssystem (SIS), den Austausch damit verbundener Zusatzinformationen über die SIRENE-Büros sowie die Rechte von Personen, deren Daten in diesem System verarbeitet werden, unberührt lassen.
- (6) Die Verarbeitung und der Austausch personenbezogener Daten für die Zwecke dieser Verordnung sollten nicht zu einer Diskriminierung von Personen aus egal welchen Gründen führen. Die Menschenwürde und die Integrität sowie andere Grundrechte der Betroffenen, darunter auch das Recht auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten, sollten im Einklang mit der Charta der Grundrechte der Europäischen Union uneingeschränkt gewahrt werden.
- (7) Da diese Verordnung den automatisierten Abruf oder Abgleich von DNA-Profilen, daktyloskopischen Daten, Fahrzeugregisterdaten, Gesichtsbildern und Kriminalakten vorsieht, besteht ihr Zweck auch darin, die Suche nach vermissten Personen und nicht identifizierten menschlichen Überresten zu ermöglichen. Dies sollte die Eingabe von SIS-Ausschreibungen von vermissten Personen und den Austausch von Zusatzinformationen zu solchen Ausschreibungen gemäß der Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates<sup>33</sup> unberührt lassen.
- (8) Die Richtlinie (EU) .../... [*über den Informationsaustausch zwischen Strafverfolgungsbehörden der Mitgliedstaaten*] bietet einen kohärenten Rechtsrahmen der Union, der dafür sorgt, dass die Strafverfolgungsbehörden einen gleichwertigen Zugang zu Informationen anderer Mitgliedstaaten haben, wenn sie diese zur Bekämpfung von Kriminalität und Terrorismus benötigen. Zur Verbesserung des Informationsaustauschs formalisiert und präzisiert die genannte Richtlinie die Verfahren für den Informationsaustausch zwischen den Mitgliedstaaten, insbesondere zu Ermittlungszwecken, einschließlich der Rolle der „zentralen Kontaktstelle“ für diesen Austausch, und für die umfassende Nutzung des Informationsaustauschkanals SIENA von Europol. Jeder über die Bestimmungen dieser Verordnung hinausgehende Informationsaustausch sollte durch die Richtlinie (EU) .../... [*über den Informationsaustausch zwischen Strafverfolgungsbehörden der Mitgliedstaaten*] geregelt werden.
- (9) Für den automatisierten Abruf von Fahrzeugregisterdaten sollten die Mitgliedstaaten das Europäische Fahrzeug- und Führerschein-Informationssystem (EUCARIS) nutzen, das durch den Vertrag über ein Europäisches Fahrzeug- und Führerschein-Informationssystem (EUCARIS) für diesen Zweck eingerichtet wurde. Das EUCARIS sollte alle teilnehmenden Mitgliedstaaten in einem Netz miteinander verbinden. Für die Herstellung der

---

<sup>32</sup> Beschluss 2008/616/JI des Rates vom 23. Juni 2008 zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6.8.2008, S. 12).

<sup>33</sup> Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission (ABl. L 312 vom 7.12.2018, S. 56).

Kommunikation ist keine zentrale Komponente erforderlich, da jeder Mitgliedstaat direkt mit den anderen angeschlossenen Mitgliedstaaten kommuniziert.

- (10) Die Identifizierung von Straftätern ist für eine erfolgreiche strafrechtliche Ermittlung und Strafverfolgung von entscheidender Bedeutung. Der automatisierte Abruf von Gesichtsbildern von Verdächtigen und verurteilten Straftätern sollte zusätzliche Informationen für die erfolgreiche Identifizierung von Straftätern und Bekämpfung von Kriminalität liefern.
- (11) Der automatisierte Abruf oder Abgleich biometrischer Daten (DNA-Profile, daktyloskopische Daten und Gesichtsbilder) zwischen für die Verhütung, Aufdeckung und Untersuchung von Straftaten zuständigen Behörden gemäß dieser Verordnung sollte nur Daten betreffen, die in für die Verhütung, Aufdeckung und Untersuchung von Straftaten eingerichteten Datenbanken enthalten sind.
- (12) Die Beteiligung am Austausch von Kriminalakten sollte freiwillig bleiben. Wenn sich Mitgliedstaaten für eine Teilnahme entscheiden, sollte es ihnen gemäß dem Grundsatz der Gegenseitigkeit nicht möglich sein, die Datenbanken anderer Mitgliedstaaten abzufragen, wenn sie ihre eigenen Daten nicht ebenso für Abfragen anderer Mitgliedstaaten zur Verfügung stellen.
- (13) In den letzten Jahren hat Europol eine große Menge biometrischer Daten von mutmaßlichen und verurteilten Terroristen und anderen Straftätern aus mehreren Drittländern erhalten. Die Aufnahme von bei Europol gespeicherten Daten aus Drittländern in den Prüm-Rahmen und somit die Bereitstellung dieser Daten für Strafverfolgungsbehörden ist für eine bessere Verhütung und Untersuchung von Straftaten erforderlich. Zudem trägt sie dazu bei, Synergien zwischen verschiedenen Strafverfolgungsinstrumenten zu schaffen.
- (14) Europol sollte die Datenbanken der Mitgliedstaaten gemäß dem Prüm-Rahmen anhand von Daten aus Drittländern abfragen können, um grenzüberschreitende Verbindungen zwischen Strafsachen herzustellen. Die Tatsache, dass neben anderen Europol zur Verfügung stehenden Datenbanken auch die Prüm-Daten genutzt werden können, dürfte eine vollständigere und fundiertere Analyse der strafrechtlichen Ermittlungen ermöglichen und Europol in die Lage versetzen, die Strafverfolgungsbehörden der Mitgliedstaaten besser zu unterstützen. Bei Übereinstimmungen zwischen den für die Abfrage verwendeten Daten und in den Datenbanken der Mitgliedstaaten gespeicherten Daten können die Mitgliedstaaten Europol die zur Erfüllung seiner Aufgaben erforderlichen Informationen zur Verfügung stellen.
- (15) Die Beschlüsse 2008/615/JI und 2008/616/JI des Rates sehen ein Netz bilateraler Verbindungen zwischen den nationalen Datenbanken der Mitgliedstaaten vor. Infolge dieser technischen Architektur sollte jeder Mitgliedstaat mindestens 26 Verbindungen, also eine Verbindung zu jedem Mitgliedstaat, je Datenkategorie herstellen. Der Router und das mit dieser Verordnung eingerichtete Europäische Kriminalaktennachweissystem (EPRIS) sollten die technische Architektur des Prüm-Rahmens vereinfachen und als Verbindungspunkte zwischen allen Mitgliedstaaten dienen. Der Router sollte eine einzige Verbindung je Mitgliedstaat in Bezug auf biometrische Daten und das EPRIS eine einzige Verbindung je Mitgliedstaat in Bezug auf Kriminalakten vorschreiben.
- (16) Der Router sollte mit dem durch Artikel 6 der Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates<sup>34</sup> und Artikel 6 der Verordnung (EU) 2019/818 des Europäischen

---

<sup>34</sup> Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726

Parlaments und des Rates<sup>35</sup> eingerichteten Europäischen Suchportal verbunden sein, damit die Behörden der Mitgliedstaaten und Europol zu Gefahrenabwehr- und Strafverfolgungszwecken Abfragen in nationalen Datenbanken gemäß der vorliegenden Verordnung gleichzeitig mit Abfragen in dem mit Artikel 17 der Verordnung (EU) 2019/817 und Artikel 17 der Verordnung (EU) 2019/818 eingerichteten gemeinsamen Speicher für Identitätsdaten durchführen können.

- (17) Bei einer Übereinstimmung zwischen den für die Abfrage oder den Abgleich verwendeten Daten und den in der nationalen Datenbank des ersuchten Mitgliedstaats bzw. der ersuchten Mitgliedstaaten gespeicherten Daten sollte der ersuchte Mitgliedstaat nach Bestätigung dieser Übereinstimmung durch den ersuchenden Mitgliedstaat innerhalb von 24 Stunden einen begrenzten Satz von Kerndaten über den Router übermitteln. Diese Frist würde einen schnellen Informationsaustausch zwischen den Behörden der Mitgliedstaaten gewährleisten. Die Mitgliedstaaten sollten die Kontrolle über die Freigabe dieses begrenzten Satzes von Kerndaten behalten. Bei den wichtigsten Etappen des Prozesses, unter anderem bei der Entscheidung, personenbezogene Daten an den ersuchenden Mitgliedstaat weiterzugeben, sollte ein gewisses Maß an menschlichem Eingreifen beibehalten werden, um sicherzustellen, dass es keinen automatisierten Austausch von Kerndaten gibt.
- (18) Jeder Austausch zwischen den Behörden der Mitgliedstaaten oder mit Europol in allen Phasen der in dieser Verordnung beschriebenen Verfahren, der in dieser Verordnung nicht ausdrücklich beschrieben wird, sollte über SIENA erfolgen, um sicherzustellen, dass alle Mitgliedstaaten einen gemeinsamen, sicheren und zuverlässigen Kommunikationskanal nutzen.
- (19) Bei der Entwicklung des Routers und des EPRIS sollte das universelle Nachrichtenformat (Universal Message Format, im Folgenden „UMF“) verwendet werden. Bei jedem automatisierten Datenaustausch gemäß dieser Verordnung sollte der UMF-Standard verwendet werden. Die Behörden der Mitgliedstaaten und Europol werden dazu angehalten, den UMF-Standard auch für jeden weiteren gegenseitigen Datenaustausch im Zusammenhang mit dem Prüm-II-Rahmen zu verwenden. Der UMF-Standard sollte als Standard für den strukturierten grenzübergreifenden Informationsaustausch zwischen Informationssystemen, Behörden oder Organisationen im Bereich Justiz und Inneres dienen.
- (20) Über den Prüm-II-Rahmen sollten nur nicht als Verschlusssache eingestufte Informationen ausgetauscht werden.
- (21) Bestimmte Aspekte des Prüm-II-Rahmens können aufgrund ihres technischen Charakters, ihrer Detailliertheit und der Tatsache, dass sie häufigen Änderungen unterliegen, durch diese Verordnung nicht erschöpfend geregelt werden. Zu diesen Aspekten gehören beispielsweise technische Vorkehrungen und Spezifikationen für den automatisierten Abruf, die Standards für den Datenaustausch und die auszutauschenden Datenelemente. Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der

---

und (EU) 2018/1861 des Europäischen Parlaments und des Rates und der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27).

<sup>35</sup> Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816 (ABl. L 135 vom 22.5.2019, S. 85).

Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates<sup>36</sup> ausgeübt werden.

- (22) Da diese Verordnung die Festlegung des neuen Prüm-Rahmens vorsieht, sollten die einschlägigen Bestimmungen der Beschlüsse 2008/615/JI und 2008/616/JI des Rates gestrichen werden. Daher sollten diese Beschlüsse entsprechend geändert werden.
- (23) Da der Router von der mit der Verordnung (EU) 2018/1726 des Europäischen Parlaments und des Rates<sup>37</sup> errichteten Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) entwickelt und verwaltet werden sollte, muss die Verordnung (EU) 2018/1726 so geändert werden, dass diese Aufgaben zu den Aufgaben von eu-LISA hinzugefügt werden. Damit der Router an das Europäische Suchportal angeschlossen werden kann, um gleichzeitige Suchabfragen des Routers und des gemeinsamen Speichers für Identitätsdaten zu ermöglichen, muss die Verordnung (EU) 2019/817 geändert werden. Damit der Router an das Europäische Suchportal angeschlossen werden kann, um gleichzeitige Suchabfragen des Routers und des gemeinsamen Speichers für Identitätsdaten zu ermöglichen, und damit Berichte und Statistiken des Routers im zentralen Speicher für Berichte und Statistiken gespeichert werden können, muss die Verordnung (EU) 2019/818 geändert werden. Daher sollten die betreffenden Verordnungen entsprechend geändert werden.
- (24) Nach den Artikeln 1 und 2 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 22 über die Position Dänemarks beteiligt sich Dänemark nicht an der Annahme dieser Verordnung und ist weder durch diese Verordnung gebunden noch zu ihrer Anwendung verpflichtet.
- (25) [Nach Artikel 3 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 hat Irland mitgeteilt, dass es sich an der Annahme und Anwendung dieser Verordnung beteiligen möchte.] ODER [Nach den Artikeln 1 und 2 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 und unbeschadet des Artikels 4 dieses Protokolls beteiligt sich Irland nicht an der Annahme dieser Verordnung und ist weder durch diese Verordnung gebunden noch zu ihrer Anwendung verpflichtet.]
- (26) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates<sup>38</sup> angehört und hat am [XX] eine Stellungnahme abgegeben<sup>39</sup> —

---

<sup>36</sup> 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).

<sup>37</sup> Verordnung (EU) 2018/1726 des Europäischen Parlaments und des Rates vom 14. November 2018 über die Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA), zur Änderung der Verordnung (EG) Nr. 1987/2006 und des Beschlusses 2007/533/JI des Rates sowie zur Aufhebung der Verordnung (EU) Nr. 1077/2011 (ABl. L 295 vom 21.11.2018, S. 99).

<sup>38</sup> Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

<sup>39</sup> [ABl. C ...].

HABEN FOLGENDE VERORDNUNG ERLASSEN:

## KAPITEL 1 ALLGEMEINE BESTIMMUNGEN

### *Artikel 1*

#### **Gegenstand**

Mit dieser Verordnung wird ein Rahmen für den Informationsaustausch zwischen den für die Verhütung, Aufdeckung und Untersuchung von Straftaten zuständigen Behörden geschaffen (Prüm II).

In dieser Verordnung werden die Bedingungen und Verfahren für den automatisierten Abruf von DNA-Profilen, daktyloskopischen Daten, Gesichtsbildern, Kriminalakten und bestimmten Fahrzeugregisterdaten sowie die Vorschriften für den Austausch von Kerndaten nach einer Übereinstimmung festgelegt.

### *Artikel 2*

#### **Ziel**

Das Ziel von Prüm II besteht darin, die grenzüberschreitende Zusammenarbeit in Angelegenheiten, die unter Teil III Titel V Kapitel 5 des Vertrags über die Arbeitsweise der Europäischen Union fallen, zu intensivieren, insbesondere den Informationsaustausch zwischen den für die Verhütung, Aufdeckung und Untersuchung von Straftaten zuständigen Behörden.

Des Weiteren soll Prüm II die Suche nach vermissten Personen und nicht identifizierten menschlichen Überresten durch die für die Verhütung, Aufdeckung und Untersuchung von Straftaten zuständigen Behörden ermöglichen.

### *Artikel 3*

#### **Anwendungsbereich**

Diese Verordnung findet Anwendung auf die nationalen Datenbanken, die für die automatisierte Übermittlung der Kategorien von DNA-Profilen, daktyloskopischen Daten, Gesichtsbildern, Kriminalakten und bestimmten Fahrzeugregisterdaten verwendet werden.

### *Artikel 4*

#### **Begriffsbestimmungen**

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Loci“ die spezielle Molekularstruktur an den verschiedenen DNA-Orten;
2. „DNA-Profil“ einen Buchstaben- beziehungsweise Zahlencode, der eine Reihe von Identifikationsmerkmalen des nicht codierenden Teils einer analysierten menschlichen DNA-Probe, der speziellen Molekularstruktur an den verschiedenen DNA-Orten, abbildet;
3. „nicht codierender Teil der DNA“ die Chromosomenbereiche, die keine genetische Information, d. h. keine Hinweise auf funktionale Eigenschaften eines Organismus, enthalten;
4. „DNA-Fundstellendatensatz“ ein DNA-Profil und die Kennung gemäß Artikel 9;
5. „DNA-Personenprofil“ das DNA-Profil einer identifizierten Person;

6. „nicht identifiziertes DNA-Profil“ ein DNA-Profil einer noch nicht identifizierten Person, das aus Spuren im Zuge der Ermittlung von Straftaten gewonnen wurde (offene Spur);
7. „daktyloskopische Daten“ Fingerabdrücke, Fingerabdruckspuren, Handabdrücke, Handabdruckspuren und Templates derartiger Abdrücke (codierte Minutien), wenn diese in einer automatisierten Datenbank gespeichert und verarbeitet werden;
8. „daktyloskopischer Fundstellendatensatz“ daktyloskopische Daten und die Kennung gemäß Artikel 14;
9. „Einzelfall“ einen einzelnen Ermittlungsakt;
10. „Gesichtsbild“ eine digitale Aufnahme des Gesichts einer Person;
11. „biometrische Daten“ DNA-Profile, daktyloskopische Daten oder Gesichtsbilder;
12. „Übereinstimmung“ eine Übereinstimmung als Ergebnis eines automatischen Abgleichs zwischen zuvor oder zeitgleich in einem Informationssystem oder in einer Datenbank erfassten personenbezogenen Daten;
13. „Kandidat“ Daten, mit denen eine Übereinstimmung festgestellt wurde;
14. „ersuchender Mitgliedstaat“ den Mitgliedstaat, der eine Abfrage über Prüm II durchführt;
15. „ersuchter Mitgliedstaat“ den Mitgliedstaat, in dessen Datenbanken der ersuchende Mitgliedstaat die Abfrage über Prüm II durchführt;
16. „Kriminalakten“ alle Informationen, die im nationalen Register oder nationalen Registern zur Erfassung von Daten der zuständigen Behörden für die Verhütung, Aufdeckung und Untersuchung von Straftaten verfügbar sind;
17. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;
18. „Europol-Daten“ alle personenbezogenen Daten, die von Europol gemäß der Verordnung (EU) 2016/794 verarbeitet werden;
19. „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 41 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates<sup>40</sup> eingerichtete unabhängige staatliche Stelle;
20. „SIENA“ die von Europol verwaltete Netzanwendung für sicheren Datenaustausch, die den Informationsaustausch zwischen den Mitgliedstaaten und Europol erleichtern soll;
21. „erheblicher Vorfall“ jeden Vorfall mit Ausnahme derjenigen, die begrenzte Auswirkungen haben und in Bezug auf die Methode oder Technologie wahrscheinlich bereits wohlbekannt sind;
22. „erhebliche Cyberbedrohung“ eine Cyberbedrohung mit der Absicht, der Möglichkeit und der Fähigkeit, einen erheblichen Vorfall zu verursachen;
23. „erhebliche Schwachstelle“ eine Schwachstelle, die wahrscheinlich zu einem erheblichen Vorfall führen wird, wenn sie genutzt wird;

---

<sup>40</sup> Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

24. „Vorfall“ einen Vorfall im Sinne des Artikels 4 Absatz 5 der Richtlinie (EU) .../... des Europäischen Parlaments und des Rates<sup>41</sup> [*NIS-2-Vorschlag*].

## KAPITEL 2 AUSTAUSCH VON DATEN

### ABSCHNITT 1 DNA-Profile

#### *Artikel 5*

##### **Einrichtung von nationalen DNA-Analyse-Dateien**

(1) Die Mitgliedstaaten errichten und führen nationale DNA-Analyse-Dateien zum Zwecke der Verfolgung von Straftaten.

Die Verarbeitung der in diesen Dateien gespeicherten Daten aufgrund dieser Verordnung erfolgt gemäß dieser Verordnung unter Beachtung des für die Verarbeitung dieser Daten geltenden nationalen Rechts der Mitgliedstaaten.

(2) Die Mitgliedstaaten gewährleisten, dass DNA-Fundstellendatensätze aus dem Bestand der in Absatz 1 genannten nationalen DNA-Analyse-Dateien verfügbar sind.

DNA-Fundstellendatensätze dürfen keine Daten enthalten, aufgrund deren eine Person unmittelbar identifiziert werden kann.

DNA-Fundstellendatensätze, die keiner Person zugeordnet werden können (nicht identifizierte DNA-Profile), müssen als solche erkennbar sein.

#### *Artikel 6*

##### **Automatisierter Abruf von DNA-Profilen**

(1) Die Mitgliedstaaten gestatten den in Artikel 29 genannten nationalen Kontaktstellen und Europol den Zugriff auf die DNA-Fundstellendatensätze in ihren DNA-Analyse-Dateien, um zum Zwecke der Untersuchung von Straftaten automatisierte Abrufe mittels eines Abgleichs von DNA-Profilen durchzuführen.

Die Abrufe dürfen nur im Einzelfall und nur nach Maßgabe des nationalen Rechts des ersuchenden Mitgliedstaats erfolgen.

(2) Wird im Zuge eines automatisierten Abrufs eine Übereinstimmung eines übermittelten DNA-Profiles mit DNA-Profilen festgestellt, die in der Datei des ersuchten Mitgliedstaats gespeichert sind, so erhält die nationale Kontaktstelle des ersuchenden Mitgliedstaats auf automatisierte Weise die DNA-Fundstellendatensätze, mit denen Übereinstimmung festgestellt worden ist.

Liegt keine Übereinstimmung vor, so wird dies dem ersuchenden Mitgliedstaat automatisch mitgeteilt.

(3) Die nationale Kontaktstelle des ersuchenden Mitgliedstaats bestätigt eine Übereinstimmung von DNA-Profildaten mit DNA-Fundstellendatensätzen des ersuchten Mitgliedstaats nach der

---

<sup>41</sup> Richtlinie (EU) .../... des Europäischen Parlaments und des Rates (ABl. ...).

automatisierten Übermittlung der für die Bestätigung einer Übereinstimmung erforderlichen DNA-Fundstellendatensätze.

#### *Artikel 7*

##### **Automatisierter Abgleich von nicht identifizierten DNA-Profilen**

(1) Die Mitgliedstaaten können über ihre nationalen Kontaktstellen die DNA-Profile ihrer nicht identifizierten DNA-Profile zur Untersuchung von Straftaten mit allen DNA-Profilen aus anderen nationalen DNA-Analyse-Dateien abgleichen. Die Übermittlung und der Abgleich der Profile erfolgen automatisiert.

(2) Stellt ein ersuchter Mitgliedstaat in Folge eines Abgleichs gemäß Absatz 1 fest, dass übermittelte DNA-Profile mit denjenigen in seiner DNA-Analyse-Datei übereinstimmen, so übermittelt er der nationalen Kontaktstelle des ersuchenden Mitgliedstaats unverzüglich die DNA-Fundstellendatensätze, mit denen eine Übereinstimmung festgestellt worden ist.

(3) Die Bestätigung einer Übereinstimmung von DNA-Profilen mit DNA-Fundstellendatensätzen des ersuchten Mitgliedstaats erfolgt durch die nationale Kontaktstelle des ersuchenden Mitgliedstaats nach der automatisierten Übermittlung der DNA-Fundstellendatensätze, die für die Bestätigung einer Übereinstimmung erforderlich sind.

#### *Artikel 8*

##### **Berichterstattung über DNA-Analyse-Dateien**

Jeder Mitgliedstaat unterrichtet die Kommission und eu-LISA gemäß Artikel 72 über die nationalen DNA-Analyse-Dateien, auf die die Artikel 5 bis 7 Anwendung finden.

#### *Artikel 9*

##### **Kennungen für DNA-Profile**

Die Kennungen für DNA-Profile bestehen aus einer Kombination folgender Elemente:

- a) einer Kennung, die es den Mitgliedstaaten im Fall einer Übereinstimmung ermöglicht, weitere Daten und sonstige Informationen in ihren Datenbanken gemäß Artikel 5 abzurufen, um sie einem, mehreren oder allen anderen Mitgliedstaaten gemäß den Artikeln 47 und 48 zu übermitteln;
- b) einem Code zur Angabe des Mitgliedstaats, dem das DNA-Profil vorliegt;
- c) einem Code, der den Typ des DNA-Profiles anzeigt (DNA-Personenprofile oder nicht identifizierte DNA-Profile).

#### *Artikel 10*

##### **Grundsätze des Austauschs von DNA-Fundstellendatensätzen**

(1) Es werden geeignete Maßnahmen zur Gewährleistung der Vertraulichkeit und Integrität der an andere Mitgliedstaaten weitergeleiteten DNA-Fundstellendatensätze, einschließlich ihrer Verschlüsselung, getroffen.

(2) Die Mitgliedstaaten treffen die notwendigen Maßnahmen, um die Integrität der den anderen Mitgliedstaaten zur Verfügung gestellten oder zum Abgleich übermittelten DNA-Profile zu garantieren und um zu gewährleisten, dass diese Maßnahmen den einschlägigen internationalen Standards für den Austausch von DNA-Daten entsprechen.

(3) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der einschlägigen internationalen Standards, die die Mitgliedstaaten für den Austausch von DNA-

Fundstellendatensätzen verwenden müssen. Diese Durchführungsrechtsakte werden nach dem in Artikel 75 Absatz 2 genannten Verfahren erlassen.

### *Artikel 11*

#### **Regeln für Ersuchen und Rückmeldungen in Bezug auf DNA-Profile**

(1) Ein Ersuchen um einen automatisierten Abruf oder Abgleich enthält ausschließlich die folgenden Informationen:

- a) Code des ersuchenden Mitgliedstaats;
- b) Datum, Zeitpunkt und Referenznummer des Ersuchens;
- c) DNA-Profile und ihre Kennungen gemäß Artikel 9;
- d) die Typen der übermittelten DNA-Profile (nicht identifizierte DNA-Profile oder DNA-Personenprofile).

(2) Die Rückmeldung auf das Ersuchen gemäß Absatz 1 enthält ausschließlich folgende Informationen:

- a) Angabe, ob eine oder mehrere Übereinstimmungen oder keine Übereinstimmungen vorliegen;
- b) Datum, Zeitpunkt und Referenznummer des Ersuchens;
- c) Datum, Zeitpunkt und Referenznummer der Rückmeldung;
- d) Codes des ersuchenden und des ersuchten Mitgliedstaats;
- e) Kennungen der DNA-Profile des ersuchenden und des ersuchten Mitgliedstaats;
- f) den Typ der übermittelten DNA-Profile (nicht identifizierte DNA-Profile oder DNA-Personenprofile);
- g) die übereinstimmenden DNA-Profile.

(3) Die automatisierte Information über das Vorliegen einer Übereinstimmung erfolgt nur, wenn der automatisierte Abruf oder Abgleich eine Übereinstimmung eines Minimums an Loci ergeben hat. Zur Festlegung dieses Minimums an Loci erlässt die Kommission Durchführungsrechtsakte nach dem in Artikel 75 Absatz 2 genannten Verfahren.

(4) Ergibt ein Abruf oder Abgleich mit nicht identifizierten DNA-Profilen eine Übereinstimmung, so kann jeder ersuchte Mitgliedstaat mit übereinstimmenden Daten eine Markierung in seine nationale Datenbank eingeben, aus der hervorgeht, dass nach dem Abruf oder Abgleich eines anderen Mitgliedstaats eine Übereinstimmung für das betreffende DNA-Profil vorliegt.

(5) Die Mitgliedstaaten stellen sicher, dass die Ersuchen mit den gemäß Artikel 8 abgegebenen Erklärungen übereinstimmen. Diese Erklärungen sind in dem Handbuch gemäß Artikel 77 wiederzugeben.

## **ABSCHNITT 2**

### **Daktyloskopische Daten**

#### *Artikel 12*

#### **Daktyloskopische Fundstellendatensätze**

(1) Die Mitgliedstaaten gewährleisten, dass daktyloskopische Fundstellendatensätze aus dem Bestand der nationalen automatisierten daktyloskopischen Identifizierungssysteme, die zur Verhütung, Aufdeckung und Untersuchung von Straftaten errichtet wurden, verfügbar sind.

(2) Daktyloskopische Fundstellendatensätze dürfen keine Daten enthalten, aufgrund deren eine Person unmittelbar identifiziert werden kann.

(3) Daktyloskopische Fundstellendatensätze, die keiner Person zugeordnet werden können (nicht identifizierte daktyloskopische Daten), müssen als solche erkennbar sein.

### *Artikel 13*

#### **Automatisierter Abruf daktyloskopischer Daten**

(1) Die Mitgliedstaaten gestatten den nationalen Kontaktstellen der anderen Mitgliedstaaten und Europol zur Verhütung, Aufdeckung und Untersuchung von Straftaten den Zugriff auf die daktyloskopischen Fundstellendatensätze ihrer zu diesen Zwecken eingerichteten automatisierten daktyloskopischen Identifizierungssysteme, um automatisierte Abrufe mittels eines Abgleichs von daktyloskopischen Fundstellendatensätzen durchzuführen.

Die Abrufe dürfen nur im Einzelfall und nur nach Maßgabe des nationalen Rechts des ersuchenden Mitgliedstaats erfolgen.

(2) Die nationale Kontaktstelle des ersuchenden Mitgliedstaats bestätigt die Übereinstimmung von daktyloskopischen Daten mit daktyloskopischen Fundstellendatensätzen des ersuchten Mitgliedstaats nach der automatisierten Übermittlung der für die Bestätigung einer Übereinstimmung erforderlichen daktyloskopischen Fundstellendatensätze.

### *Artikel 14*

#### **Kennungen für daktyloskopische Daten**

Die Kennungen für daktyloskopische Daten bestehen aus einer Kombination folgender Elemente:

- a) einer Kennung, die es den Mitgliedstaaten im Fall einer Übereinstimmung ermöglicht, weitere Daten und sonstige Informationen in ihren Datenbanken gemäß Artikel 12 abzurufen, um sie einem, mehreren oder allen anderen Mitgliedstaaten gemäß den Artikeln 47 und 48 zu übermitteln;
- b) einem Code zur Angabe des Mitgliedstaats, dem die daktyloskopischen Daten vorliegen.

### *Artikel 15*

#### **Grundsätze des Austauschs daktyloskopischer Daten**

(1) Die Digitalisierung der daktyloskopischen Daten und ihre Übermittlung an die anderen Mitgliedstaaten erfolgen in einem einheitlichen Datenformat. Zur Festlegung des einheitlichen Datenformats erlässt die Kommission Durchführungsrechtsakte nach dem in Artikel 75 Absatz 2 genannten Verfahren.

(2) Jeder Mitgliedstaat stellt sicher, dass die von ihm übermittelten daktyloskopischen Daten für einen Abgleich anhand der automatisierten Fingerabdruck-Identifizierungssysteme von ausreichender Qualität sind.

(3) Die Mitgliedstaaten treffen geeignete Maßnahmen zur Gewährleistung der Vertraulichkeit und Integrität der an andere Mitgliedstaaten übermittelten daktyloskopischen Daten, einschließlich ihrer Verschlüsselung.

(4) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der einschlägigen bestehenden Standards, die die Mitgliedstaaten für den Austausch von daktyloskopischen Daten verwenden müssen. Diese Durchführungsrechtsakte werden nach dem in Artikel 75 Absatz 2 genannten Verfahren erlassen.

## Artikel 16

### **Abrufkapazitäten für daktyloskopische Daten**

(1) Jeder Mitgliedstaat gewährleistet, dass seine Abrufersuchen nicht die Abrufkapazitäten überschreiten, die der jeweilige ersuchte Mitgliedstaat angegeben hat.

Die Mitgliedstaaten unterrichten die Kommission und eu-LISA gemäß Artikel 78 Absätze 8 und 10 über ihre maximalen täglichen Abrufkapazitäten für daktyloskopische Daten identifizierter Personen und für daktyloskopische Daten von noch nicht identifizierten Personen.

(2) Zur Festlegung der Höchstzahl der pro Übermittlung für einen Abgleich akzeptierten Kandidaten erlässt die Kommission Durchführungsrechtsakte nach dem in Artikel 75 Absatz 2 genannten Verfahren.

## Artikel 17

### **Regeln für Ersuchen und Rückmeldungen in Bezug auf daktyloskopische Daten**

(1) Ein Ersuchen um einen automatisierten Abruf enthält ausschließlich die folgenden Informationen:

- a) Code des ersuchenden Mitgliedstaats;
- b) Datum, Zeitpunkt und Referenznummer des Ersuchens;
- c) die daktyloskopischen Daten und ihre Kennungen gemäß Artikel 14.

(2) Die Rückmeldung auf das Ersuchen gemäß Absatz 1 enthält ausschließlich folgende Informationen:

- a) Angabe, ob eine oder mehrere Übereinstimmungen oder keine Übereinstimmungen vorliegen;
- b) Datum, Zeitpunkt und Referenznummer des Ersuchens;
- c) Datum, Zeitpunkt und Referenznummer der Rückmeldung;
- d) Codes des ersuchenden und des ersuchten Mitgliedstaats;
- e) Kennungen der daktyloskopischen Daten des ersuchenden und des ersuchten Mitgliedstaats;
- f) die übereinstimmenden daktyloskopischen Daten.

## ABSCHNITT 3

### **Daten aus Fahrzeugregistern**

## Artikel 18

### **Automatisierter Abruf von Daten aus den Fahrzeugregistern**

(1) Die Mitgliedstaaten gestatten den nationalen Kontaktstellen anderer Mitgliedstaaten und Europol zur Verhütung, Aufdeckung und Untersuchung von Straftaten den Zugriff auf folgende Daten aus den nationalen Fahrzeugregistern, um in Einzelfällen automatisierte Abrufe durchzuführen:

- a) Eigentümer- oder Halterdaten;
- b) Fahrzeugdaten.

(2) Abrufe dürfen nur anhand einer vollständigen Fahrgestellnummer oder eines vollständigen Kennzeichens erfolgen.

(3) Die Abrufe dürfen nur nach Maßgabe des nationalen Rechts des ersuchenden Mitgliedstaats erfolgen.

#### *Artikel 19*

### **Grundsätze des automatisierten Abrufs von Fahrzeugregisterdaten**

(1) Für den automatisierten Abruf von Fahrzeugregisterdaten verwenden die Mitgliedstaaten das Europäische Fahrzeug- und Führerschein-Informationssystem (EUCARIS).

(2) Die über das EUCARIS ausgetauschten Nachrichten werden verschlüsselt übertragen.

(3) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der Datenelemente der auszutauschenden Fahrzeugregisterdaten. Diese Durchführungsrechtsakte werden nach dem in Artikel 75 Absatz 2 genannten Verfahren erlassen.

#### *Artikel 20*

### **Protokollierung**

(1) Jeder Mitgliedstaat protokolliert die Abfragen, die die zum Austausch von Fahrzeugregisterdaten ordnungsgemäß ermächtigten Bediensteten seiner Behörden durchführen, sowie die Abfrageersuchen von anderen Mitgliedstaaten. Europol protokolliert die Abfragen seiner ordnungsgemäß ermächtigten Bediensteten.

Jeder Mitgliedstaat und Europol protokollieren alle Datenverarbeitungsvorgänge im Zusammenhang mit Fahrzeugregisterdaten. Diese Protokolle enthalten folgende Angaben:

- a) Mitgliedstaat oder Agentur der Union, der bzw. die um die Abfrage ersucht hat;
- b) Datum und Uhrzeit des Ersuchens;
- c) Datum und Uhrzeit der Rückmeldung;
- d) nationale Datenbanken, an die ein Abfrageersuchen gerichtet wurde;
- e) nationale Datenbanken, die eine positive Rückmeldung übermittelt haben.

(2) Die gemäß Absatz 1 erstellten Protokolle dürfen nur zur Erhebung von Statistiken und zur datenschutzrechtlichen Kontrolle einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Gewährleistung der Datensicherheit und -integrität verwendet werden.

Diese Protokolle sind durch geeignete Maßnahmen gegen unbefugten Zugriff zu schützen und ein Jahr nach ihrer Erstellung zu löschen. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, werden sie gelöscht, sobald sie nicht mehr für das Kontrollverfahren benötigt werden.

(3) Zum Zwecke der datenschutzrechtlichen Kontrolle einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung haben die für die Verarbeitung Verantwortlichen Zugang zu den Protokollen für die Eigenkontrolle gemäß Artikel 56.

## **ABSCHNITT 4**

### **Gesichtsbilder**

#### *Artikel 21*

### **Gesichtsbilder**

(1) Die Mitgliedstaaten gewährleisten, dass Gesichtsbilder aus ihren zur Verhütung, Aufdeckung und Untersuchung von Straftaten errichteten nationalen Datenbanken verfügbar sind. Diese Daten umfassen nur Gesichtsbilder und die Kennung gemäß Artikel 23 sowie die Angabe, ob die Gesichtsbilder einer Person zugeordnet werden oder nicht.

Die Mitgliedstaaten dürfen in diesem Zusammenhang keine Daten zur Verfügung stellen, aufgrund deren eine Person unmittelbar identifiziert werden kann.

(2) Gesichtsbilder, die keiner Person zugeordnet werden können (nicht identifizierte Gesichtsbilder), müssen als solche erkennbar sein.

#### *Artikel 22*

##### **Automatisierter Abruf von Gesichtsbildern**

(1) Die Mitgliedstaaten gestatten den nationalen Kontaktstellen anderer Mitgliedstaaten und Europol zur Verhütung, Aufdeckung und Untersuchung von Straftaten den Zugriff auf in ihren nationalen Datenbanken gespeicherte Gesichtsbilder, um automatisierte Abrufe durchzuführen.

Die Abrufe dürfen nur im Einzelfall und nur nach Maßgabe des nationalen Rechts des ersuchenden Mitgliedstaats erfolgen.

(2) Der ersuchende Mitgliedstaat erhält eine Liste mit Übereinstimmungen in Bezug auf wahrscheinliche Kandidaten. Der betreffende Mitgliedstaat überprüft die Liste, um festzustellen, ob eine bestätigte Übereinstimmung vorliegt.

(3) Es wird ein Mindestqualitätsstandard festgelegt, um den Abruf und Abgleich von Gesichtsbildern zu ermöglichen. Die Kommission erlässt Durchführungsrechtsakte zur Festlegung dieses Mindestqualitätsstandards. Diese Durchführungsrechtsakte werden nach dem in Artikel 75 Absatz 2 genannten Verfahren erlassen.

#### *Artikel 23*

##### **Kennungen für Gesichtsbilder**

Die Kennungen für Gesichtsbilder bestehen aus einer Kombination folgender Elemente:

- a) einer Kennung, die es den Mitgliedstaaten im Fall einer Übereinstimmung ermöglicht, weitere Daten und sonstige Informationen in ihren Datenbanken gemäß Artikel 21 abzurufen, um sie einem, mehreren oder allen anderen Mitgliedstaaten gemäß den Artikeln 47 und 48 zu übermitteln;
- b) einem Code zur Angabe des Mitgliedstaats, dem die Gesichtsbilder vorliegen.

#### *Artikel 24*

##### **Regeln für Ersuchen und Rückmeldungen in Bezug auf Gesichtsbilder**

(1) Ein Ersuchen um einen automatisierten Abruf enthält ausschließlich die folgenden Informationen:

- a) Code des ersuchenden Mitgliedstaats;
- b) Datum, Zeitpunkt und Referenznummer des Ersuchens;
- c) die Gesichtsbilder und ihre Kennungen gemäß Artikel 23.

(2) Die Rückmeldung auf das Ersuchen gemäß Absatz 1 enthält ausschließlich folgende Informationen:

- a) Angabe, ob eine oder mehrere Übereinstimmungen oder keine Übereinstimmungen vorliegen;

- b) Datum, Zeitpunkt und Referenznummer des Ersuchens;
- c) Datum, Zeitpunkt und Referenznummer der Rückmeldung;
- d) Codes des ersuchenden und des ersuchten Mitgliedstaats;
- e) Kennungen der Gesichtsbilder des ersuchenden und des ersuchten Mitgliedstaats;
- f) die übereinstimmenden Gesichtsbilder.

## ABSCHNITT 5

### Kriminalakten

#### *Artikel 25*

### Kriminalakten

(1) Die Mitgliedstaaten können beschließen, sich am automatisierten Austausch von Kriminalakten zu beteiligen. Die Mitgliedstaaten, die sich am automatisierten Austausch von Kriminalakten beteiligen, gewährleisten, dass biografische Daten von Verdächtigen und Straftätern aus ihren nationalen Kriminalaktennachweisen, die für die Untersuchung von Straftaten errichtet wurden, verfügbar sind. Der betreffende Datensatz enthält, sofern verfügbar, die folgenden Daten:

- a) Vorname(n);
- b) Familienname(n);
- c) Aliasname(n);
- d) Geburtsdatum;
- e) Staatsangehörigkeit(en);
- f) Geburtsort und -land;
- g) Geschlecht.

(2) Die in Absatz 1 Buchstaben a, b, c, e und f genannten Daten werden pseudonymisiert.

#### *Artikel 26*

### Automatisierter Abruf von Kriminalakten

(1) Die Mitgliedstaaten gestatten den nationalen Kontaktstellen anderer Mitgliedstaaten und Europol zur Untersuchung von Straftaten den Zugriff auf Daten aus ihren nationalen Kriminalaktennachweisen, um automatisierte Abrufe durchzuführen.

Die Abrufe dürfen nur im Einzelfall und nur nach Maßgabe des nationalen Rechts des ersuchenden Mitgliedstaats erfolgen.

(2) Der ersuchende Mitgliedstaat erhält die Liste der Übereinstimmungen mit einer Angabe der Qualität der Übereinstimmungen.

Ferner wird dem ersuchenden Mitgliedstaat der Mitgliedstaat mitgeteilt, dessen Datenbank Daten enthält, die die Übereinstimmung ergeben haben.

#### *Artikel 27*

### Kennungen für Kriminalakten

Die Kennungen für Kriminalakten bestehen aus einer Kombination folgender Elemente:

- a) einer Kennung, die es den Mitgliedstaaten im Fall einer Übereinstimmung ermöglicht, personenbezogene Daten und sonstige Informationen in ihren Nachweisen gemäß

Artikel 25 abzurufen, um sie einem, mehreren oder allen anderen Mitgliedstaaten gemäß den Artikeln 47 und 48 zu übermitteln;

- b) einem Code zur Angabe des Mitgliedstaats, der im Besitz der Kriminalakten ist.

#### *Artikel 28*

##### **Regeln für Ersuchen und Rückmeldungen in Bezug auf Kriminalakten**

(1) Ein Ersuchen um einen automatisierten Abruf enthält ausschließlich die folgenden Informationen:

- a) Code des ersuchenden Mitgliedstaats;
- b) Datum, Zeitpunkt und Referenznummer des Ersuchens;
- c) die Kriminalakten und ihre Kennungen gemäß Artikel 27.

(2) Die Rückmeldung auf das Ersuchen gemäß Absatz 1 enthält ausschließlich folgende Informationen:

- a) Angabe, ob eine oder mehrere Übereinstimmungen oder keine Übereinstimmungen vorliegen;
- b) Datum, Zeitpunkt und Referenznummer des Ersuchens;
- c) Datum, Zeitpunkt und Referenznummer der Rückmeldung;
- d) Codes des ersuchenden und des ersuchten Mitgliedstaats;
- e) Kennungen der Kriminalakten des ersuchenden und des ersuchten Mitgliedstaats.

#### **ABSCHNITT 6**

##### **Gemeinsame Bestimmungen**

#### *Artikel 29*

##### **Nationale Kontaktstellen**

Jeder Mitgliedstaat benennt eine nationale Kontaktstelle.

Die nationalen Kontaktstellen sind für die Übermittlung der in den Artikeln 6, 7, 13, 18, 22 und 26 genannten Daten zuständig.

#### *Artikel 30*

##### **Durchführungsmaßnahmen**

Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der technischen Ausgestaltung der Verfahren gemäß den Artikeln 6, 7, 13, 18, 22 und 26. Diese Durchführungsrechtsakte werden nach dem in Artikel 75 Absatz 2 genannten Verfahren erlassen.

#### *Artikel 31*

##### **Technische Spezifikationen**

Die Mitgliedstaaten und Europol beachten bei allen Ersuchen und Rückmeldungen im Zusammenhang mit Abrufen und Abgleichen von DNA-Profilen, daktyloskopischen Daten, Fahrzeugregisterdaten, Gesichtsbildern und Kriminalakten gemeinsame technische Spezifikationen. Zur Festlegung dieser technischen Spezifikationen erlässt die Kommission Durchführungsrechtsakte nach dem in Artikel 75 Absatz 2 genannten Verfahren.

## Artikel 32

### **Verfügbarkeit des automatisierten Datenaustauschs auf nationaler Ebene**

(1) Die Mitgliedstaaten treffen alle notwendigen Vorkehrungen, damit der automatisierte Abruf oder Abgleich von DNA-Profilen, daktyloskopischen Daten, Fahrzeugregisterdaten, Gesichtsbildern und Kriminalakten 24 Stunden täglich und sieben Tage pro Woche möglich ist.

(2) Die nationalen Kontaktstellen informieren einander, die Kommission, Europol und eu-LISA unverzüglich über etwaige technische Störungen, die eine Nichtverfügbarkeit des automatisierten Datenaustauschs verursacht haben.

Die nationalen Kontaktstellen vereinbaren für die Zwischenzeit einen alternativen Informationsaustausch gemäß dem geltenden Unionsrecht und den geltenden nationalen Rechtsvorschriften.

(3) Die nationalen Kontaktstellen stellen den automatisierten Datenaustausch unverzüglich wieder her.

## Artikel 33

### **Begründung für die Datenverarbeitung**

(1) Jeder Mitgliedstaat bewahrt eine Begründung der von seinen zuständigen Behörden durchgeführten Abfragen auf.

Europol bewahrt eine Begründung seiner Abfragen auf.

(2) Die in Absatz 1 genannte Begründung enthält folgende Angaben:

- a) Zweck der Abfrage, einschließlich einer Bezugnahme auf den konkreten Fall oder die konkrete Untersuchung;
- b) Angabe, ob die Abfrage einen Verdächtigen oder einen Straftäter betrifft;
- c) Angabe, ob die Abfrage darauf abzielt, eine unbekannt Person zu identifizieren oder mehr Daten zu einer bekannten Person zu erhalten.

(3) Die in Absatz 2 genannten Begründungen dürfen nur zur datenschutzrechtlichen Kontrolle, einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit und -integrität verwendet werden.

Die Begründungen sind durch geeignete Maßnahmen gegen unbefugten Zugriff zu schützen und ein Jahr nach ihrer Erstellung zu löschen. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, werden sie gelöscht, sobald sie nicht mehr für das Kontrollverfahren benötigt werden.

(4) Zum Zwecke der datenschutzrechtlichen Kontrolle einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung haben die für die Verarbeitung Verantwortlichen Zugang zu diesen Begründungen für die Eigenkontrolle gemäß Artikel 56.

## Artikel 34

### **Verwendung des universellen Nachrichtenformats**

(1) Bei der Entwicklung des in Artikel 35 genannten Routers und des EPRIS wird das universelle Nachrichtenformat (Universal Message Format, UMF) verwendet.

(2) Für den gesamten automatisierten Datenaustausch gemäß dieser Verordnung wird der UMF-Standard verwendet.

## KAPITEL 3 ARCHITEKTUR

### ABSCHNITT 1

#### **Router**

##### *Artikel 35*

#### **Der Router**

(1) Es wird ein Router eingerichtet, um die Herstellung von Verbindungen zwischen den Mitgliedstaaten und zu Europol zum Zwecke der Abfrage mit, des Abrufs von und der Bewertung (Scoring) von biometrischen Daten gemäß dieser Verordnung zu erleichtern.

(2) Der Router besteht aus:

- a) einer zentralen Infrastruktur, einschließlich einer Suchfunktion, die die gleichzeitige Abfrage der in den Artikeln 5, 12 und 21 genannten Datenbanken der Mitgliedstaaten sowie der Europol-Daten ermöglicht;
- b) einem sicheren Kommunikationskanal zwischen der zentralen Infrastruktur und denjenigen Mitgliedstaaten und Agenturen der Union, die berechtigt sind, den Router zu nutzen;
- c) einer sicheren Kommunikationsinfrastruktur zwischen der zentralen Infrastruktur und dem Europäischen Suchportal für die Zwecke des Artikels 39.

##### *Artikel 36*

#### **Nutzung des Routers**

Die Nutzung des Routers ist den Behörden der Mitgliedstaaten, die Zugang zum Austausch von DNA-Profilen, daktyloskopischen Daten und Gesichtsbildern haben, und Europol gemäß der vorliegenden Verordnung und der Verordnung (EU) 2016/794 vorbehalten.

##### *Artikel 37*

#### **Abfragen**

(1) Die Nutzer des Routers gemäß Artikel 36 ersuchen um eine Abfrage, indem sie dem Router biometrische Daten übermitteln. Der Router versendet das Abfrageersuchen an die Datenbanken der Mitgliedstaaten und die Europol-Daten gleichzeitig mit den vom Nutzer übermittelten Daten und nach Maßgabe der jeweiligen Zugriffsrechte.

(2) Nach Eingang des vom Router übermittelten Abfrageersuchens leiten jeder ersuchte Mitgliedstaat und Europol unverzüglich eine automatisierte Abfrage ihrer Datenbanken ein.

(3) Sämtliche Übereinstimmungen infolge der Abfrage der Datenbanken des jeweiligen Mitgliedstaats und der Europol-Daten werden automatisch an den Router zurückgesendet.

(4) Der Router bringt die Antworten in eine Rangfolge entsprechend der Bewertung (Score) der Übereinstimmung zwischen den für die Abfrage verwendeten biometrischen Daten und den in den Datenbanken der Mitgliedstaaten und den Europol-Daten gespeicherten biometrischen Daten.

(5) Die Liste der übereinstimmenden biometrischen Daten und ihrer Bewertungen (Scores) werden vom Router an den Nutzer des Routers zurückgesandt.

(6) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung des technischen Verfahrens für die Abfrage der Datenbanken der Mitgliedstaaten und der Europol-Daten durch den Router, des Formats der Antworten des Routers und der technischen Vorschriften für die Bewertung der

Übereinstimmung zwischen biometrischen Daten. Diese Durchführungsrechtsakte werden nach dem in Artikel 75 Absatz 2 genannten Verfahren erlassen.

#### *Artikel 38*

### **Qualitätsprüfung**

Der ersuchte Mitgliedstaat prüft die Qualität der übermittelten Daten mittels eines vollständig automatisierten Verfahrens.

Sind die Daten für einen automatisierten Abgleich ungeeignet, informiert der ersuchte Mitgliedstaat den ersuchenden Mitgliedstaat über den Router unverzüglich hierüber.

#### *Artikel 39*

### **Interoperabilität zwischen dem Router und dem gemeinsamen Speicher für Identitätsdaten für die Zwecke des Zugangs der Strafverfolgungsbehörden**

(1) Die Nutzer des Routers gemäß Artikel 36 können nach Maßgabe ihrer Zugangsrechte eine Abfrage der Datenbanken der Mitgliedstaaten und der Europol-Daten gleichzeitig mit einer Abfrage des gemeinsamen Speichers für Identitätsdaten durchführen, wenn die einschlägigen Bedingungen des Unionsrechts erfüllt sind. Zu diesem Zweck führt der Router eine Abfrage des gemeinsamen Speichers für Identitätsdaten über das Europäische Suchportal durch.

(2) Abfragen des gemeinsamen Speichers für Identitätsdaten zu Strafverfolgungszwecken erfolgen gemäß Artikel 22 der Verordnung (EU) 2019/817 und Artikel 22 der Verordnung (EU) 2019/818. Die Ergebnisse der Abfragen werden über das Europäische Suchportal übermittelt.

Nur benannte Behörden im Sinne des Artikels 4 Nummer 20 der Verordnung (EU) 2019/817 und des Artikels 4 Nummer 20 der Verordnung (EU) 2019/818 können diese gleichzeitigen Abfragen vornehmen.

Gleichzeitige Abfragen der Datenbanken der Mitgliedstaaten, der Europol-Daten und des gemeinsamen Speichers für Identitätsdaten dürfen nur in Fällen vorgenommen werden, in denen wahrscheinlich Daten über einen Verdächtigen, einen Täter oder ein Opfer einer terroristischen oder sonstigen schweren Straftat im Sinne des Artikels 4 Nummern 21 und 22 der Verordnung (EU) 2019/817 bzw. des Artikels 4 Nummern 21 und 22 der Verordnung (EU) 2019/818 im gemeinsamen Speicher für Identitätsdaten gespeichert sind.

#### *Artikel 40*

### **Protokollierung**

(1) eu-LISA protokolliert alle Datenverarbeitungsvorgänge im Router. Diese Protokolle enthalten folgende Angaben:

- a) Mitgliedstaat oder Agentur der Union, der bzw. die um die Abfrage ersucht hat;
- b) Datum und Uhrzeit des Ersuchens;
- c) Datum und Uhrzeit der Rückmeldung;
- d) nationale Datenbanken oder Europol-Daten, an die ein Abfrageersuchen gerichtet wurde;
- e) nationale Datenbanken oder Europol-Daten, die eine Antwort übermittelt haben;
- f) gegebenenfalls die Tatsache, dass eine gleichzeitige Abfrage des gemeinsamen Speichers für Identitätsdaten vorgenommen wurde.

(2) Jeder Mitgliedstaat protokolliert die Abfragen, die seine zuständigen Behörden und die zur Nutzung des Routers ordnungsgemäß ermächtigten Bediensteten dieser Behörden durchführen, sowie die Abfrageersuchen von anderen Mitgliedstaaten.

Europol protokolliert die Abfragen seiner ordnungsgemäß ermächtigten Bediensteten.

(3) Die gemäß den Absätzen 1 und 2 erstellten Protokolle dürfen nur zur Erhebung von Statistiken und zur datenschutzrechtlichen Kontrolle einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Gewährleistung der Datensicherheit und -integrität verwendet werden.

Diese Protokolle sind durch geeignete Maßnahmen gegen unbefugten Zugriff zu schützen und ein Jahr nach ihrer Erstellung zu löschen. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, werden sie gelöscht, sobald sie nicht mehr für das Kontrollverfahren benötigt werden.

(4) Zum Zwecke der datenschutzrechtlichen Kontrolle einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung haben die für die Verarbeitung Verantwortlichen Zugang zu den Protokollen für die Eigenkontrolle gemäß Artikel 56.

#### *Artikel 41*

##### **Meldeverfahren für den Fall, dass die Nutzung des Routers technisch nicht möglich ist**

(1) Wenn es wegen eines Ausfalls des Routers technisch nicht möglich ist, den Router für die Abfrage einer oder mehrerer nationaler Datenbanken oder der Europol-Daten zu nutzen, werden die Nutzer des Routers von eu-LISA automatisch entsprechend benachrichtigt. eu-LISA ergreift unverzüglich Maßnahmen zur Behebung der technischen Unmöglichkeit der Nutzung des Routers.

(2) Wenn es wegen eines Ausfalls der nationalen Infrastruktur eines Mitgliedstaats technisch nicht möglich ist, den Router für die Abfrage einer oder mehrerer nationaler Datenbanken oder der Europol-Daten zu nutzen, benachrichtigt der betroffene Mitgliedstaat die anderen Mitgliedstaaten, eu-LISA und die Kommission automatisch. Die Mitgliedstaaten ergreifen unverzüglich Maßnahmen zur Behebung der technischen Unmöglichkeit der Nutzung des Routers.

(3) Wenn es wegen eines Ausfalls der Infrastruktur von Europol technisch nicht möglich ist, den Router für die Abfrage einer oder mehrerer nationaler Datenbanken oder der Europol-Daten zu nutzen, benachrichtigt Europol die Mitgliedstaaten, eu-LISA und die Kommission automatisch. Europol ergreift unverzüglich Maßnahmen zur Behebung der technischen Unmöglichkeit der Nutzung des Routers.

## ABSCHNITT 2

### **EPRIS**

#### *Artikel 42*

### **EPRIS**

(1) Für den automatisierten Abruf von Kriminalakten nach Artikel 26 verwenden die Mitgliedstaaten und Europol das Europäische Kriminalaktennachweissystem (EPRIS).

(2) Das EPRIS setzt sich zusammen aus

- a) einer zentralen Infrastruktur einschließlich einer Suchfunktion, die die gleichzeitige Abfrage der Datenbanken der Mitgliedstaaten ermöglicht;
- b) einem sicheren Kommunikationskanal zwischen der zentralen Infrastruktur des EPRIS, den Mitgliedstaaten und Europol.

### Verwendung des EPRIS

(1) Für den über das EPRIS erfolgenden Abruf von Kriminalakten werden die folgenden Datensätze verwendet:

- a) Vorname(n);
- b) Familienname(n);
- c) Geburtsdatum.

(2) Sofern verfügbar, können auch die folgenden Datensätze verwendet werden:

- a) Aliasname(n);
- b) Staatsangehörigkeit(en);
- c) Geburtsort und -land;
- d) Geschlecht.

(3) Die in Absatz 1 Buchstaben a und b sowie in Absatz 2 Buchstaben a, b und c genannten Daten, die für Abfragen verwendet werden, werden pseudonymisiert.

### Artikel 44

#### Abfragen

(1) Die Mitgliedstaaten und Europol ersuchen um eine Abfrage durch Übermittlung der in Artikel 43 genannten Daten.

Das EPRIS versendet das Abfrageersuchen an die Datenbanken der Mitgliedstaaten mit den vom ersuchenden Mitgliedstaat übermittelten Daten und gemäß dieser Verordnung.

(2) Nach Eingang des vom EPRIS übermittelten Abfrageersuchens leitet jeder ersuchte Mitgliedstaat unverzüglich eine automatisierte Abfrage seines nationalen Kriminalaktennachweises ein.

(3) Sämtliche bei einer Abfrage in der Datenbank des jeweiligen Mitgliedstaats erzielte Übereinstimmungen werden automatisch an das EPRIS zurückgesendet.

(4) Die Liste der Übereinstimmungen wird vom EPRIS an den ersuchenden Mitgliedstaat zurückgesandt. In der Liste der Übereinstimmungen werden die Qualität der Übereinstimmung sowie der Mitgliedstaat angegeben, dessen Datenbank Daten enthält, die zu der Übereinstimmung geführt haben.

(5) Nach Eingang der Liste der Übereinstimmungen entscheidet der ersuchende Mitgliedstaat, welche Übereinstimmungen weiterverfolgt werden müssen, und übermittelt dem/den ersuchten Mitgliedstaat(en) über SIENA einen mit einer Begründung und etwaigen weiteren sachdienlichen Informationen versehenen Antrag auf Weiterverfolgung.

(6) Alle ersuchten Mitgliedstaaten bearbeiten derartige Ersuchen unverzüglich, um zu entscheiden, ob die in ihrer Datenbank gespeicherten Daten weitergegeben werden.

Nach der Bestätigung übermitteln die ersuchten Mitgliedstaaten die in Artikel 43 genannten Daten, sofern diese verfügbar sind. Dieser Informationsaustausch erfolgt über SIENA.

(7) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung des technischen Verfahrens für die vom EPRIS durchgeführte Abfrage der Datenbanken der Mitgliedstaaten und des Formats der Antworten. Diese Durchführungsrechtsakte werden nach dem in Artikel 75 Absatz 2 genannten Verfahren erlassen.

## Artikel 45

### Protokollierung

(1) Europol führt Protokolle über alle im EPRIS durchgeführten Datenverarbeitungsvorgänge. Diese Protokolle enthalten folgende Angaben:

- a) Mitgliedstaat oder Agentur der Union, der bzw. die um die Abfrage ersucht hat;
- b) Datum und Uhrzeit des Ersuchens;
- c) Datum und Uhrzeit der Rückmeldung;
- d) nationale Datenbanken, an die ein Abfrageersuchen gerichtet wurde;
- e) nationale Datenbanken, die eine Rückmeldung übermittelt haben.

(2) Jeder Mitgliedstaat protokolliert die Abfrageersuchen seiner zuständigen Behörden und der ordnungsgemäß zur Nutzung des EPRIS ermächtigten Bediensteten dieser Behörden. Europol protokolliert die Abfrageersuchen seiner ordnungsgemäß ermächtigten Bediensteten.

(3) Die gemäß den Absätzen 1 und 2 erstellten Protokolle dürfen nur zur datenschutzrechtlichen Kontrolle einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Gewährleistung der Datensicherheit und -integrität verwendet werden.

Diese Protokolle sind durch geeignete Maßnahmen gegen unbefugten Zugriff zu schützen und ein Jahr nach ihrer Erstellung zu löschen.

Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, werden sie gelöscht, sobald sie nicht mehr für das Kontrollverfahren benötigt werden.

(4) Zum Zwecke der datenschutzrechtlichen Kontrolle einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung haben die für die Verarbeitung Verantwortlichen Zugang zu den Protokollen für die Eigenkontrolle gemäß Artikel 56.

## Artikel 46

### Meldeverfahren für den Fall, dass die Verwendung des EPRIS technisch nicht möglich ist

(1) Ist die Verwendung des EPRIS zur Abfrage einer oder mehrerer nationaler Datenbanken aufgrund eines Ausfalls der Infrastruktur von Europol technisch nicht möglich, so werden die Mitgliedstaaten von Europol automatisch benachrichtigt. Europol ergreift unverzüglich Maßnahmen zur Behebung der technischen Unmöglichkeit der Verwendung des EPRIS.

(2) Wenn es wegen eines Ausfalls der nationalen Infrastruktur eines Mitgliedstaats technisch nicht möglich ist, das EPRIS für die Abfrage einer oder mehrerer nationaler Datenbanken zu nutzen, benachrichtigt der betroffene Mitgliedstaat automatisch Europol und die Kommission. Die Mitgliedstaaten ergreifen unverzüglich Maßnahmen zur Behebung der technischen Unmöglichkeit der Verwendung des EPRIS.

## KAPITEL 4

### DATENAUSTAUSCH NACH EINER ÜBEREINSTIMMUNG

## Artikel 47

### Austausch von Kerndaten

Ergibt sich bei den Verfahren nach den Artikeln 6, 7, 13 oder 22 eine Übereinstimmung zwischen den für die Abfrage oder den Abgleich verwendeten Daten und den in der Datenbank des ersuchten Mitgliedstaats bzw. der ersuchten Mitgliedstaaten gespeicherten Daten, so übermittelt der ersuchte Mitgliedstaat nach Bestätigung dieser Übereinstimmung durch den ersuchenden Mitgliedstaat

innerhalb von 24 Stunden einen Satz von Kerndaten über den Router. Dieser Kerndatensatz enthält, sofern verfügbar, die folgenden Daten:

- a) Vorname(n);
- b) Familienname(n);
- c) Geburtsdatum;
- d) Staatsangehörigkeit(en);
- e) Geburtsort und -land;
- f) Geschlecht.

#### *Artikel 48*

### **Verwendung von SIENA**

Jeder in dieser Verordnung nicht ausdrücklich vorgesehene Austausch zwischen den zuständigen Behörden der Mitgliedstaaten oder mit Europol hat in allen Phasen eines der in dieser Verordnung vorgesehenen Verfahren über SIENA zu erfolgen.

## **KAPITEL 5**

### **EUROPOL**

#### *Artikel 49*

### **Zugang der Mitgliedstaaten zu von Europol gespeicherten biometrischen Daten aus Drittländern**

- (1) Die Mitgliedstaaten haben nach Maßgabe der Verordnung (EU) 2016/794 Zugang zu biometrischen Daten, die von Drittländern für die Zwecke von Artikel 18 Absatz 2 Buchstaben a, b und c der Verordnung (EU) 2016/794 an Europol übermittelt wurden, und können diese über den Router abfragen.
- (2) Führt dieses Verfahren zu einer Übereinstimmung zwischen den für die Abfrage verwendeten Daten und den Europol-Daten, erfolgt die Weiterverfolgung gemäß der Verordnung (EU) 2016/794.

#### *Artikel 50*

### **Zugang von Europol zu in den Datenbanken der Mitgliedstaaten gespeicherten Daten**

- (1) Europol hat nach Maßgabe der Verordnung (EU) 2016/794 Zugang zu Daten, die von den Mitgliedstaaten in ihren nationalen Datenbanken nach Maßgabe dieser Verordnung gespeichert werden.
- (2) Von Europol vorgenommene Abfragen, bei denen biometrische Daten als Suchkriterium verwendet werden, werden über den Router durchgeführt.
- (3) Von Europol vorgenommene Abfragen, bei denen Fahrzeugregisterdaten als Suchkriterium verwendet werden, werden mittels Eucaris durchgeführt.
- (4) Von Europol vorgenommene Abfragen, bei denen Kriminalakten als Suchkriterium verwendet werden, werden über das EPRIS durchgeführt.
- (5) Europol führt die Abfragen nach Absatz 1 nur durch, wenn es seine Aufgaben nach der Verordnung (EU) 2016/794 wahrnimmt.
- (6) Ergibt sich bei den Verfahren nach den Artikeln 6, 7, 13 oder 22 eine Übereinstimmung zwischen den für die Abfrage oder den Abgleich verwendeten Daten und den in der nationalen

Datenbank des/der ersuchten Mitgliedstaats/Mitgliedstaaten gespeicherten Daten, so entscheidet der ersuchte Mitgliedstaat nach Bestätigung dieser Übereinstimmung durch Europol, ob er innerhalb von 24 Stunden einen Satz von Kerndaten über den Router übermittelt. Dieser Kerndatensatz enthält, sofern verfügbar, die folgenden Daten:

- a) Vorname(n);
- b) Familienname(n);
- c) Geburtsdatum;
- d) Staatsangehörigkeit(en);
- e) Geburtsort und -land;
- f) Geschlecht.

(7) Die Verwendung der Informationen, die Europol bei einer Abfrage nach Absatz 1 und durch den Austausch von Kerndaten nach Absatz 6 erhält, unterliegt der Zustimmung des Mitgliedstaats, in dessen Datenbank die Übereinstimmung gefunden wurde. Gestattet der Mitgliedstaat die Verwendung solcher Informationen, so unterliegt deren Handhabung durch Europol den Bestimmungen der Verordnung (EU) 2016/794.

## KAPITEL 6 DATENSCHUTZ

### *Artikel 51*

#### **Zweck der Daten**

(1) Die Verarbeitung personenbezogener Daten durch den ersuchenden Mitgliedstaat oder Europol ist nur für die Zwecke zulässig, für die die Daten von dem ersuchten Mitgliedstaat nach Maßgabe dieser Verordnung übermittelt wurden. Eine Verarbeitung zu anderen Zwecken ist nur mit vorheriger Genehmigung vonseiten des ersuchten Mitgliedstaats zulässig.

(2) Die Verarbeitung von Daten, die gemäß den Artikeln 6, 7, 13, 18 oder 22 durch den die Abfrage bzw. den Abgleich durchführenden Mitgliedstaat übermittelt wurden, ist ausschließlich zu folgenden Zwecken zulässig:

- a) Prüfung der dem Abgleich unterzogenen DNA-Profile, daktyloskopischen Daten, Fahrzeugregisterdaten, Gesichtsbilder und Kriminalakten auf Übereinstimmungen;
- b) Vorbereitung und Einreichung eines polizeilichen Rechtshilfeersuchens im Fall der Übereinstimmung;
- c) Protokollierung im Sinne der Artikel 40 und 45.

(3) Der ersuchende Mitgliedstaat darf die ihm gemäß den Artikeln 6, 7, 13 oder 22 übermittelten Daten nur verarbeiten, wenn dies für die Zwecke dieser Verordnung erforderlich ist. Die übermittelten Daten werden nach dem Datenabgleich oder der automatisierten Beantwortung von Abfragen unverzüglich gelöscht, sofern sie nicht von dem ersuchenden Mitgliedstaat für die Zwecke der Verhütung, Aufdeckung und Untersuchung von Straftaten weiterverarbeitet werden müssen.

(4) Die gemäß Artikel 18 übermittelten Daten dürfen von dem ersuchenden Mitgliedstaat nur verwendet werden, wenn dies für die Zwecke dieser Verordnung erforderlich ist. Die übermittelten Daten werden nach der automatisierten Beantwortung von Abfragen unverzüglich gelöscht, sofern keine Weiterverarbeitung für die Protokollierung gemäß Artikel 20 erforderlich ist. Der ersuchende Mitgliedstaat darf die ihm in einer Antwort übermittelten Daten ausschließlich für das Verfahren verwenden, für das die Abfrage durchgeführt wurde.

### **Genauigkeit, Relevanz und Datenspeicherung**

(1) Die Mitgliedstaaten gewährleisten die Genauigkeit und die aktuelle Relevanz der personenbezogenen Daten. Stellt ein ersuchter Mitgliedstaat fest, dass unrichtige Daten oder Daten, die nicht hätten übermittelt werden dürfen, übermittelt worden sind, so teilt er dies unverzüglich allen ersuchenden Mitgliedstaaten mit. Alle betroffenen ersuchenden Mitgliedstaaten sind verpflichtet, die Daten entsprechend zu berichtigen oder zu löschen. Darüber hinaus sind übermittelte personenbezogene Daten zu berichtigen, wenn sich herausstellt, dass sie unrichtig sind. Hat der ersuchende Mitgliedstaat Grund zu der Annahme, dass die übermittelten Daten unrichtig sind oder gelöscht werden sollten, so wird der ersuchte Mitgliedstaat davon unterrichtet.

(2) Bestreitet eine betroffene Person die Genauigkeit von Daten, die sich im Besitz eines Mitgliedstaats befinden, und kann die Genauigkeit von dem betreffenden Mitgliedstaat nicht zuverlässig festgestellt werden und wird dies von der betroffenen Person beantragt, so werden die betreffenden Daten mit einer Kennzeichnung versehen. Ist eine solche Kennzeichnung vorhanden, dürfen die Mitgliedstaaten diese nur mit Zustimmung der betroffenen Person oder aufgrund einer Entscheidung des zuständigen Gerichts oder der unabhängigen Datenschutzbehörde entfernen.

(3) Übermittelte Daten, die nicht hätten übermittelt oder empfangen werden dürfen, werden gelöscht. Rechtmäßig übermittelte und empfangene Daten werden gelöscht,

- a) wenn sie für den Zweck, für den sie übermittelt wurden, nicht oder nicht mehr erforderlich sind;
- b) wenn der ersuchte Mitgliedstaat nach Ablauf der in seinem innerstaatlichen Recht vorgesehenen Höchstfrist für die Aufbewahrung der Daten den ersuchenden Mitgliedstaat zum Zeitpunkt der Übermittlung der Daten über diese Höchstfrist informiert hat.

Besteht Grund zu der Annahme, dass die Löschung von Daten die Interessen der betroffenen Person beeinträchtigen würde, so werden die Daten nicht gelöscht, sondern gesperrt. Gesperrte Daten dürfen nur für den Zweck, für den ihre Löschung unterblieben ist, übermittelt oder verwendet werden.

### **Auftragsverarbeiter**

(1) eu-LISA ist der Auftragsverarbeiter im Sinne von Artikel 3 Nummer 12 der Verordnung (EU) 2018/1725 für die Verarbeitung personenbezogener Daten über den Router.

(2) Europol ist der Auftragsverarbeiter für die Verarbeitung von personenbezogenen Daten über das EPRIS.

### **Sicherheit der Verarbeitung**

(1) Europol, eu-LISA und die Behörden der Mitgliedstaaten gewährleisten die Sicherheit der Verarbeitung personenbezogener Daten gemäß dieser Verordnung. Europol, eu-LISA und die Behörden der Mitgliedstaaten arbeiten bei sicherheitsrelevanten Aufgaben zusammen.

(2) Unbeschadet des Artikels 33 der Verordnung (EU) 2018/1725 und des Artikels 32 der Verordnung (EU) 2016/794 ergreifen eu-LISA und Europol die erforderlichen Maßnahmen, um die Sicherheit des Routers bzw. des EPRIS sowie der zugehörigen Kommunikationsinfrastruktur zu gewährleisten.

(3) Insbesondere ergreifen eu-LISA und Europol in Bezug auf den Router bzw. das EPRIS die erforderlichen Maßnahmen einschließlich eines Sicherheitsplans, eines Plans zur Aufrechterhaltung des Geschäftsbetriebs und eines Plans zur Wiederherstellung im Notfall, um

- a) die Daten physisch zu schützen, unter anderem durch Aufstellung von Notfallplänen für den Schutz kritischer Infrastrukturen;
- b) Unbefugten den Zugang zu Datenverarbeitungsgeräten und -anlagen zu verwehren;
- c) das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verhindern;
- d) die unbefugte Eingabe von Daten und die unbefugte Kenntnisnahme, Änderung oder Löschung von gespeicherten personenbezogenen Daten zu verhindern;
- e) die unbefugte Verarbeitung von Daten sowie das unbefugte Kopieren, Ändern oder Löschen von Daten zu verhindern;
- f) zu verhindern, dass Unbefugte mit Hilfe von Datenübertragungsgeräten automatisierte Datenverarbeitungssysteme benutzen;
- g) sicherzustellen, dass die zum Zugriff auf den Router und das EPRIS befugten Personen nur über individuelle Benutzeridentitäten und vertrauliche Zugriffsverfahren ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können;
- h) sicherzustellen, dass überprüft und festgestellt werden kann, welchen Stellen personenbezogene Daten mit Hilfe von Datenübertragungsgeräten übermittelt werden dürfen;
- i) sicherzustellen, dass überprüft und festgestellt werden kann, welche Daten wann, von wem und zu welchem Zweck im Router und im EPRIS verarbeitet wurden;
- j) das unbefugte Lesen, Kopieren, Ändern oder Löschen personenbezogener Daten während der Übermittlung personenbezogener Daten zum oder vom Router und EPRIS oder während des Transports von Datenträgern zu verhindern, insbesondere durch geeignete Verschlüsselungstechniken;
- k) sicherzustellen, dass eingesetzte Systeme im Störfall für den Normalbetrieb wiederhergestellt werden können;
- l) die Zuverlässigkeit sicherzustellen, indem dafür Sorge getragen wird, dass etwaige Funktionsstörungen des Routers und des EPRIS ordnungsgemäß gemeldet werden;
- m) die Wirksamkeit der in diesem Absatz genannten Sicherheitsmaßnahmen zu überwachen, die erforderlichen organisatorischen Maßnahmen für die interne Überwachung zu treffen, um die Einhaltung dieser Verordnung sicherzustellen, und diese Sicherheitsmaßnahmen vor dem Hintergrund neuer technologischer Entwicklungen zu bewerten.

#### *Artikel 55*

#### **Sicherheitsvorfälle**

(1) Jedes Ereignis, das sich auf die Sicherheit des Routers oder des EPRIS auswirkt oder auswirken kann und zu einer Beschädigung oder einem Verlust der dort gespeicherten Daten führen kann, gilt als Sicherheitsvorfall, insbesondere wenn möglicherweise ein unbefugter Zugriff auf Daten erfolgt ist oder die Verfügbarkeit, Integrität oder Vertraulichkeit von Daten tatsächlich oder möglicherweise beeinträchtigt wurde.

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

(3) Die Mitgliedstaaten melden ihren zuständigen Aufsichtsbehörden unverzüglich alle Sicherheitsvorfälle.

Unbeschadet des Artikels 34 der Verordnung (EU) 2016/794 meldet Europol dem CERT-EU erhebliche Cyberbedrohungen, erhebliche Schwachstellen und erhebliche Vorfälle unverzüglich, spätestens jedoch 24 Stunden nach Bekanntwerden. Verwertbare und sachdienliche technische Einzelheiten von Cyberbedrohungen, Schwachstellen und Vorfällen, die eine proaktive Erkennung, eine geeignete Reaktion oder geeignete Abhilfemaßnahmen ermöglichen, werden dem CERT-EU unverzüglich mitgeteilt.

Im Falle eines Sicherheitsvorfalls in Bezug auf die zentrale Infrastruktur des Routers meldet eu-LISA dem CERT-EU erhebliche Cyber-Bedrohungen, erhebliche Schwachstellen und erhebliche Vorfälle unverzüglich, spätestens jedoch 24 Stunden nach Bekanntwerden. Verwertbare und sachdienliche technische Einzelheiten von Cyberbedrohungen, Schwachstellen und Vorfällen, die eine proaktive Erkennung, eine geeignete Reaktion oder geeignete Abhilfemaßnahmen ermöglichen, werden dem CERT-EU unverzüglich mitgeteilt.

(4) Informationen über einen Sicherheitsvorfall, der sich auf den Betrieb des Routers oder auf die Verfügbarkeit, die Integrität oder die Vertraulichkeit der Daten auswirkt oder auswirken könnte, werden von den betroffenen Mitgliedstaaten und Agenturen der Union unverzüglich an die Mitgliedstaaten und an Europol weitergeleitet und gemäß dem von eu-LISA vorzulegenden Plan für die Bewältigung von Sicherheitsvorfällen gemeldet.

(5) Informationen über einen Sicherheitsvorfall, der sich auf den Betrieb des EPRIS oder auf die Verfügbarkeit, die Integrität oder die Vertraulichkeit der Daten auswirkt oder auswirken könnte, werden von den betroffenen Mitgliedstaaten und Agenturen der Union unverzüglich an die Mitgliedstaaten weitergeleitet und gemäß dem von Europol vorzulegenden Plan für die Bewältigung von Sicherheitsvorfällen gemeldet.

#### *Artikel 56*

### **Eigenkontrolle**

(1) Die Mitgliedstaaten und die zuständigen Agenturen der Union stellen sicher, dass jede zur Anwendung von Prüm II befugte Behörde die erforderlichen Maßnahmen zur Einhaltung dieser Verordnung trifft und erforderlichenfalls mit der Aufsichtsbehörde zusammenarbeitet.

(2) Die für die Datenverarbeitung Verantwortlichen treffen die erforderlichen Maßnahmen, um die Ordnungsgemäßheit der Datenverarbeitung gemäß dieser Verordnung zu überwachen, unter anderem durch häufige Überprüfung der gemäß den Artikeln 40 und 45 zu erstellenden Protokolle, und arbeiten erforderlichenfalls mit den Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten zusammen.

#### *Artikel 57*

### **Sanktionen**

Die Mitgliedstaaten stellen sicher, dass jeder Missbrauch von Daten sowie jede Verarbeitung von Daten oder jeder Austausch von Daten, der bzw. die dieser Verordnung zuwiderläuft, gemäß nationalem Recht geahndet werden können. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

#### *Artikel 58*

### **Haftung**

Verursacht ein Verstoß eines Mitgliedstaats gegen seine aus dieser Verordnung erwachsenden Pflichten einen Schaden am Router oder am EPRIS, so haftet dieser Mitgliedstaat für diesen

Schaden, sofern und soweit es eu-LISA, Europol oder ein anderer durch diese Verordnung gebundener Mitgliedstaat nicht versäumt haben, angemessene Maßnahmen zu ergreifen, um den Schaden zu verhindern oder seine Auswirkungen zu minimieren.

#### *Artikel 59*

### **Prüfungen durch den Europäischen Datenschutzbeauftragten**

(1) Der Europäische Datenschutzbeauftragte trägt dafür Sorge, dass die durch eu-LISA und Europol für die Zwecke dieser Verordnung erfolgenden Verarbeitungsvorgänge von personenbezogenen Daten mindestens alle vier Jahre nach den einschlägigen internationalen Prüfungsstandards überprüft werden. Der Prüfbericht wird dem Europäischen Parlament, dem Rat, der Kommission, den Mitgliedstaaten und der betreffenden Agentur der Union übermittelt. Europol und eu-LISA erhalten vor der Annahme des Berichts Gelegenheit zur Stellungnahme.

(2) eu-LISA und Europol erteilen dem Europäischen Datenschutzbeauftragten die von ihm angeforderten Auskünfte, gewähren ihm Zugang zu allen von ihm angeforderten Dokumenten und zu ihren gemäß den Artikeln 40 und 45 erstellten Protokollen und gewähren ihm jederzeit Zugang zu allen ihren Räumlichkeiten.

#### *Artikel 60*

### **Zusammenarbeit zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten**

(1) Die Aufsichtsbehörden und der Europäische Datenschutzbeauftragte arbeiten im Rahmen ihrer jeweiligen Zuständigkeiten aktiv zusammen und sorgen für eine koordinierte Überwachung der Anwendung dieser Verordnung, insbesondere wenn der Europäische Datenschutzbeauftragte oder eine Aufsichtsbehörde größere Abweichungen zwischen den Praktiken der Mitgliedstaaten feststellt oder potenziell unrechtmäßige Übermittlungen über die Prüm-II-Kommunikationskanäle feststellt.

(2) In den in Absatz 1 genannten Fällen wird eine koordinierte Aufsicht gemäß Artikel 62 der Verordnung (EU) 2018/1725 sichergestellt.

(3) Der Europäische Datenschutzausschuss übermittelt dem Europäischen Parlament, dem Rat, der Kommission, Europol und eu-LISA bis zum [*zwei Jahre nach Inbetriebnahme des Routers und des EPRIS*] und danach alle zwei Jahre einen gemeinsamen Bericht über seine Tätigkeiten im Rahmen dieses Artikels. Dieser Bericht enthält für jeden Mitgliedstaat ein Kapitel, das von dessen Aufsichtsbehörde erstellt wird.

#### *Artikel 61*

### **Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen**

Jegliche Übermittlung von Daten, die ein ersuchender Mitgliedstaat gemäß dieser Verordnung erhalten hat, an ein Drittland oder eine internationale Organisation bedarf der Zustimmung des ersuchten Mitgliedstaats.

## KAPITEL 7

### **VERANTWORTLICHKEITEN**

#### *Artikel 62*

### **Verantwortlichkeiten der Mitgliedstaaten**

(1) Jeder Mitgliedstaat ist verantwortlich für

- a) seine Anbindung an die Infrastruktur des Routers;
- b) die Integration der bestehenden nationalen Systeme und Infrastrukturen mit dem Router;
- c) die Organisation, die Verwaltung, den Betrieb und die Instandhaltung seiner bestehenden nationalen Infrastruktur und ihrer Anbindung an den Router;
- d) seine Anbindung an die Infrastruktur des EPRIS;
- e) die Integration der bestehenden nationalen Systeme und Infrastrukturen mit dem EPRIS;
- f) die Organisation, die Verwaltung, den Betrieb und die Instandhaltung seiner bestehenden nationalen Infrastruktur und ihrer Anbindung an das EPRIS;
- g) die Verwaltung und Regelung des Zugangs der ordnungsgemäß ermächtigten Bediensteten der zuständigen nationalen Behörden zum Router gemäß dieser Verordnung sowie die Erstellung und regelmäßige Aktualisierung einer Liste dieser Bediensteten und ihrer Profile;
- h) die Verwaltung und Regelung des Zugangs der ordnungsgemäß ermächtigten Bediensteten der zuständigen nationalen Behörden zum EPRIS gemäß dieser Verordnung sowie die Erstellung und regelmäßige Aktualisierung einer Liste dieser Bediensteten und ihrer Profile;
- i) die Verwaltung und Regelung des Zugangs der ordnungsgemäß ermächtigten Bediensteten der zuständigen nationalen Behörden zum EUCARIS gemäß dieser Verordnung sowie die Erstellung und regelmäßige Aktualisierung einer Liste dieser Bediensteten und ihrer Profile;
- j) die manuelle Bestätigung einer Übereinstimmung gemäß Artikel 6 Absatz 3, Artikel 7 Absatz 3, Artikel 13 Absatz 2, Artikel 22 Absatz 2 und Artikel 26 Absatz 2;
- k) die Sicherstellung der Verfügbarkeit der für den Datenaustausch erforderlichen Daten gemäß den Artikeln 6, 7, 13, 18, 22 und 26;
- l) den Austausch von Informationen gemäß den Artikeln 6, 7, 13, 18, 22 und 26;
- m) die Löschung aller von einem ersuchten Mitgliedstaat eingegangenen Daten innerhalb von 48 Stunden nach der Mitteilung des ersuchten Mitgliedstaats, dass die übermittelten personenbezogenen Daten unrichtig oder nicht mehr aktuell sind oder unrechtmäßig übermittelt wurden;
- n) die Einhaltung der in dieser Verordnung festgelegten Datenqualitätsanforderungen.

(2) Jeder Mitgliedstaat ist für die Anbindung seiner zuständigen nationalen Behörden an den Router, an das EPRIS und an das EUCARIS verantwortlich.

### *Artikel 63*

#### **Verantwortlichkeiten von Europol**

(1) Europol ist für die Verwaltung des Routers, des EPRIS und des EUCARIS sowie für die Regelung des Zugangs seiner ordnungsgemäß ermächtigten Bediensteten zu diesen Systemen nach Maßgabe dieser Verordnung verantwortlich.

(2) Europol ist zudem für die Verarbeitung der Abfragen von Europol-Daten durch den Router verantwortlich. Europol passt seine Informationssysteme entsprechend an.

(3) Europol ist für alle technischen Anpassungen der Europol-Infrastruktur verantwortlich, die für deren Anbindung an den Router und an das EUCARIS erforderlich sind.

(4) Europol ist für die Entwicklung des EPRIS in Zusammenarbeit mit den Mitgliedstaaten verantwortlich. Das EPRIS stellt die in den Artikeln 42 bis 46 festgelegten Funktionen bereit.

Europol übernimmt die technische Verwaltung des EPRIS. Die technische Verwaltung des EPRIS umfasst alle Aufgaben und technischen Lösungen, die erforderlich sind, um den Betrieb der zentralen Infrastruktur des EPRIS aufrechtzuerhalten und den Mitgliedstaaten im Einklang mit dieser Verordnung 24 Stunden am Tag und 7 Tage in der Woche ununterbrochene Dienste zu bieten. Dazu gehören die Wartungsarbeiten und technischen Entwicklungen, die erforderlich sind, um sicherzustellen, dass die Funktionen des EPRIS gemäß den technischen Spezifikationen, insbesondere in Bezug auf die Reaktionszeit für Abfragen der nationalen Datenbanken, mit zufriedenstellender technischer Qualität arbeiten.

(5) Europol führt Schulungen über die technische Nutzung des EPRIS durch.

(6) Europol ist für die in den Artikeln 49 und 50 genannten Verfahren verantwortlich.

#### *Artikel 64*

#### **Verantwortlichkeiten von eu-LISA während der Konzept- und Entwicklungsphase des Routers**

(1) eu-LISA stellt sicher, dass die zentrale Infrastruktur des Routers im Einklang mit dieser Verordnung betrieben wird.

(2) Der Router wird von eu-LISA an deren technischen Standorten betrieben und stellt die in dieser Verordnung vorgesehenen Funktionen gemäß den in Artikel 65 Absatz 1 festgelegten Bedingungen für die Sicherheit, Verfügbarkeit, Qualität und Leistung bereit.

(3) eu-LISA ist für die Entwicklung des Routers und für alle technischen Anpassungen, die für den Betrieb des Routers erforderlich sind, verantwortlich.

eu-LISA hat keinen Zugang zu den über den Router verarbeiteten personenbezogenen Daten.

eu-LISA legt den Entwurf der physischen Architektur des Routers einschließlich seiner Kommunikationsinfrastrukturen sowie die technischen Spezifikationen und seine Weiterentwicklung in Bezug auf die zentrale Infrastruktur und die sichere Kommunikationsinfrastruktur fest. Dieser Entwurf wird vom Verwaltungsrat vorbehaltlich einer befürwortenden Stellungnahme der Kommission angenommen. eu-LISA nimmt ferner alle erforderlichen Anpassungen der Interoperabilitätskomponenten vor, die sich aus der Einrichtung des Routers gemäß dieser Verordnung ergeben.

eu-LISA entwickelt und implementiert den Router so bald wie möglich nach der Annahme der in Artikel 37 Absatz 6 vorgesehenen Maßnahmen durch die Kommission.

Die Entwicklung umfasst die Ausarbeitung und Umsetzung der technischen Spezifikationen, die Erprobung und die Gesamtprojektleitung und -koordinierung.

(4) Während der Konzept- und Entwicklungsphase tritt der in Artikel 54 der Verordnung (EU) 2019/817 und in Artikel 54 der Verordnung (EU) 2019/818 genannte Programmverwaltungsrat für Interoperabilität regelmäßig zusammen. Er stellt die angemessene Verwaltung der Konzept- und Entwicklungsphase des Routers sicher.

Der Programmverwaltungsrat für Interoperabilität legt dem Verwaltungsrat von eu-LISA monatlich schriftliche Berichte über den Fortschritt des Projekts vor. Der Programmverwaltungsrat für

Interoperabilität hat keine Entscheidungsbefugnis und kein Mandat zur Vertretung der Mitglieder des Verwaltungsrats von eu-LISA.

Die in Artikel 76 genannte Beratergruppe tritt bis zur Inbetriebnahme des Routers regelmäßig zusammen. Nach jeder Zusammenkunft erstattet sie dem Programmverwaltungsrat für Interoperabilität Bericht. Sie stellt den technischen Sachverstand zur Unterstützung der Aufgaben des Programmverwaltungsrats für Interoperabilität bereit und überwacht den Stand der Vorbereitungen in den Mitgliedstaaten.

#### *Artikel 65*

### **Verantwortlichkeiten von eu-LISA nach der Inbetriebnahme des Routers**

(1) Nach der Inbetriebnahme des Routers ist eu-LISA für die technische Verwaltung der zentralen Infrastruktur des Routers einschließlich ihrer Wartung und technologischen Weiterentwicklung verantwortlich. In Zusammenarbeit mit den Mitgliedstaaten stellt eu-LISA sicher, dass vorbehaltlich einer Kosten-Nutzen-Analyse die beste verfügbare Technologie eingesetzt wird. eu-LISA ist zudem für die technische Verwaltung der erforderlichen Kommunikationsinfrastruktur verantwortlich.

Die technische Verwaltung des Routers umfasst alle Aufgaben und technischen Lösungen, die erforderlich sind, um den Router betriebsbereit zu halten und den Mitgliedstaaten und Europol 24 Stunden am Tag und 7 Tage in der Woche ununterbrochene Dienste im Einklang mit dieser Verordnung zu bieten. Dazu gehören die Wartungsarbeiten und technischen Entwicklungen, die erforderlich sind, um sicherzustellen, dass die Funktionen des Routers gemäß den technischen Spezifikationen, insbesondere in Bezug auf die Verfügbarkeit und auf die Reaktionszeit für Abfragen der nationalen Datenbanken und von Europol-Daten, mit zufriedenstellender technischer Qualität arbeiten.

Der Router wird so entwickelt und verwaltet, dass ein schneller, effizienter und kontrollierter Zugang, eine uneingeschränkte und ununterbrochene Verfügbarkeit des Routers und eine Reaktionszeit gewährleistet sind, die den operativen Erfordernissen der zuständigen Behörden der Mitgliedstaaten und von Europol entsprechen.

(2) Unbeschadet des Artikels 17 des in der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates<sup>42</sup> festgelegten Statuts der Beamten der Europäischen Union wendet eu-LISA geeignete Regeln für die berufliche Schweigepflicht bzw. eine vergleichbare Geheimhaltungspflicht auf ihre 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.

eu-LISA hat keinen Zugang zu den über den Router verarbeiteten personenbezogenen Daten.

(3) eu-LISA nimmt auch Aufgaben im Zusammenhang mit der Schulung in der technischen Nutzung des Routers wahr.

## KAPITEL 8

### **ÄNDERUNGEN ANDERER BESTEHENDER INSTRUMENTE**

#### *Artikel 66*

### **Änderungen der Beschlüsse 2008/615/JI und 2008/616/JI**

---

<sup>42</sup> ABl. L 56 vom 4.3.1968, S. 1.

- (1) In dem Beschluss 2008/615/JI werden die Artikel 2 bis 6 sowie Kapitel 2 Abschnitte 2 und 3 in Bezug auf die durch die vorliegende Verordnung gebundenen Mitgliedstaaten ab dem in Artikel 73 festgelegten Geltungsbeginn der sich auf den Router beziehenden Bestimmungen dieser Verordnung ersetzt.

Daher werden die Artikel 2 bis 6 sowie Kapitel 2 Abschnitte 2 und 3 des Beschlusses 2008/615/JI ab dem in Artikel 73 festgelegten Geltungsbeginn der sich auf den Router beziehenden Bestimmungen dieser Verordnung gestrichen.

- (2) In dem Beschluss 2008/616/JI werden die Kapitel 2 bis 5 sowie die Artikel 18, 20 und 21 in Bezug auf die durch die vorliegende Verordnung gebundenen Mitgliedstaaten ab dem in Artikel 73 festgelegten Geltungsbeginn der sich auf den Router beziehenden Bestimmungen dieser Verordnung ersetzt.

Daher werden die Kapitel 2 bis 5 und die Artikel 18, 20 und 21 des Beschlusses 2008/616/JI ab dem in Artikel 73 festgelegten Geltungsbeginn der sich auf den Router beziehenden Bestimmungen dieser Verordnung gestrichen.

#### *Artikel 67*

### **Änderungen der Verordnung (EU) 2018/1726**

Die Verordnung (EU) 2018/1726 wird wie folgt geändert:

1. Folgender Artikel 13a wird eingefügt:

„Artikel 13a

#### **Aufgaben im Zusammenhang mit dem Router**

In Bezug auf die Verordnung (EU) .../... des Europäischen Parlaments und des Rates\* [*die vorliegende Verordnung*] nimmt die Agentur die ihr durch die genannte Verordnung übertragenen Aufgaben im Zusammenhang mit dem Router wahr.

\*Verordnung (EU) [Nummer] des Europäischen Parlaments und des Rates vom xy über [amtlich erlassener Titel] (ABl. L ...)

Artikel 17 Absatz 3 erhält folgende Fassung:

„(3) Der Sitz der Agentur ist Tallinn (Estland).

Die Aufgaben im Zusammenhang mit der Entwicklung und dem Betriebsmanagement gemäß Artikel 1 Absätze 4 und 5 sowie den Artikeln 3 bis 8, 9, 11 und 13a werden am technischen Standort in Straßburg (Frankreich) erfüllt.

Ein Back-up-Standort, der bei Ausfall eines IT-Großsystems dessen Betrieb sicherstellen kann, wird in Sankt Johann im Pongau (Österreich) eingerichtet.“

#### *Artikel 68*

### **Änderungen der Verordnung (EU) 2019/817**

In Artikel 6 Absatz 2 der Verordnung (EU) 2019/817 wird folgender Buchstabe d angefügt:

„d) eine sichere Kommunikationsinfrastruktur zwischen dem ESP und dem durch die Verordnung (EU) .../... des Europäischen Parlaments und des Rates\* [*die vorliegende Verordnung*] eingerichteten Router.

---

\*Verordnung (EU) [Nummer] des Europäischen Parlaments und des Rates vom xy über [amtlich erlassener Titel] (ABl. L ...)“

#### Artikel 69

### Änderungen der Verordnung (EU) 2019/818

Die Verordnung (EU) 2019/818 wird wie folgt geändert:

1. In Artikel 6 Absatz 2 wird folgender Buchstabe d angefügt:

„d) eine sichere Kommunikationsinfrastruktur zwischen dem ESP und dem durch die Verordnung (EU) .../... des Europäischen Parlaments und des Rates\* [*die vorliegende Verordnung*] eingerichteten Router.

---

\*Verordnung (EU) [Nummer] des Europäischen Parlaments und des Rates vom xy über [amtlich erlassener Titel] (ABl. L ...)“

2. Artikel 39 Absätze 1 und 2 erhalten folgende Fassung:

„(1) Es wird ein zentraler Speicher für Berichte und Statistiken (CRRS) eingerichtet, um die Ziele von Eurodac, des SIS sowie des ECRIS-TCN gemäß den geltenden Rechtsinstrumenten zu unterstützen und systemübergreifende statistische Daten und analytische Berichte für politische und operative Zwecke sowie für die Zwecke der Datenqualität bereitzustellen. Der CRRS unterstützt auch die Ziele von Prüm II.“

„(2) eu-LISA sorgt an ihren technischen Standorten für die Einrichtung, die Implementierung und das Hosting des CRRS, das logisch nach den EU-Informationssystemen getrennt die Daten und Statistiken nach Artikel 74 der Verordnung (EU) 2018/1862 und Artikel 32 der Verordnung (EU) 2019/816 enthält. eu-LISA erhebt auch die Daten und Statistiken des in Artikel 65 Absatz 1 der Verordnung (EU).../... \* [*die vorliegende Verordnung*] genannten Routers. Der Zugang zum CRRS erfolgt in Form eines kontrollierten, gesicherten Zugangs und mittels spezifischer Nutzerprofile und wird den in Artikel 74 der Verordnung (EU) 2018/1862, Artikel 32 der Verordnung (EU) 2019/816 und Artikel 65 Absatz 1 der Verordnung (EU).../... \* [*die vorliegende Verordnung*] genannten Behörden ausschließlich zu Berichterstattungs- und Statistikzwecken gewährt.“

## KAPITEL 9

### SCHLUSSBESTIMMUNGEN

#### Artikel 70

### Berichte und Statistiken

(1) Die folgenden Daten zum Router dürfen von dazu ordnungsgemäß ermächtigten Bediensteten der zuständigen mitgliedstaatlichen Behörden, der Kommission, von Europol und von eu-LISA ausschließlich zur Erstellung von Berichten und Statistiken abgefragt werden:

- a) Zahl der Abfragen je Mitgliedstaat und von Europol;
- b) Zahl der Abfragen je Datenkategorie;
- c) Zahl der Abfragen in den einzelnen angeschlossenen Datenbanken;
- d) Zahl der Übereinstimmungen mit der Datenbank der einzelnen Mitgliedstaaten je Datenkategorie;
- e) Zahl der Übereinstimmungen mit Europol-Daten je Datenkategorie;
- f) Zahl der bestätigten Übereinstimmungen, bei denen Kerndaten ausgetauscht wurden, und
- g) Zahl der über den Router erfolgten Abfragen im gemeinsamen Speicher für Identitätsdaten.

Die Identifizierung einzelner Personen auf der Grundlage der Daten darf nicht möglich sein.

(2) Die folgenden Daten zum EUCARIS dürfen von dazu ordnungsgemäß ermächtigten Bediensteten der zuständigen mitgliedstaatlichen Behörden, der Kommission und von Europol ausschließlich für die Zwecke der Berichterstattung und für statistische Zwecke abgefragt werden:

- a) Zahl der Abfragen je Mitgliedstaat und von Europol;
- b) Zahl der Abfragen in den einzelnen angeschlossenen Datenbanken; und
- c) Zahl der Übereinstimmungen mit der Datenbank der einzelnen Mitgliedstaaten.

Die Identifizierung einzelner Personen auf der Grundlage der Daten darf nicht möglich sein.

(3) Die folgenden Daten zum EPRIS dürfen von dazu ordnungsgemäß ermächtigten Bediensteten der zuständigen mitgliedstaatlichen Behörden, der Kommission und von Europol ausschließlich zur Erstellung von Berichten und Statistiken abgefragt werden:

- a) Zahl der Abfragen je Mitgliedstaat und von Europol;
- b) Zahl der Abfragen in den einzelnen angeschlossenen Kriminalaktennachweisen; und
- c) Zahl der Übereinstimmungen mit der Datenbank der einzelnen Mitgliedstaaten.

Die Identifizierung einzelner Personen auf der Grundlage der Daten darf nicht möglich sein.

(4) eu-LISA speichert die in diesen Absätzen genannten Daten.

Die Daten müssen es den in Absatz 1 genannten Behörden ermöglichen, anpassbare Berichte und Statistiken einzuholen, um die Effizienz der Zusammenarbeit der Strafverfolgungsbehörden zu verbessern.

## *Artikel 71*

### **Kosten**

(1) Die Kosten im Zusammenhang mit der Einrichtung und dem Betrieb des Routers und des EPRIS gehen zu Lasten des Gesamthaushaltsplans der Europäischen Union.

(2) Die Kosten im Zusammenhang mit der Integration der bestehenden nationalen Infrastrukturen, ihrer Anbindung an den Router und das EPRIS und der Einrichtung nationaler Gesichtsbilddatenbanken und nationaler Kriminalaktennachweise zur Verhütung, Aufdeckung und Untersuchung von Straftaten 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) Jeder Mitgliedstaat trägt die Kosten, die ihm aus der Verwaltung, der Verwendung und der Pflege der in Artikel 19 Absatz 1 genannten EUCARIS-Softwareanwendung entstehen.
- (4) Jeder Mitgliedstaat trägt die Kosten, die ihm aus der Verwaltung, Verwendung und Instandhaltung seiner Verbindungen zum Router und zum EPRIS entstehen.

#### *Artikel 72*

#### **Mitteilungen**

- (1) Die Mitgliedstaaten teilen eu-LISA die Behörden gemäß Artikel 36 mit, die den Router nutzen dürfen oder Zugang zum Router haben.
- (2) eu-LISA teilt der Kommission den erfolgreichen Abschluss der Tests nach Artikel 73 Absatz 1 Buchstabe b mit.
- (3) Die Mitgliedstaaten teilen der Kommission, Europol und eu-LISA die nationalen Kontaktstellen mit.

#### *Artikel 73*

#### **Aufnahme des Betriebs**

- (1) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, ab welchem Zeitpunkt die Mitgliedstaaten und die Agenturen der Union den Router verwenden dürfen, sobald folgende Voraussetzungen erfüllt sind:
- a) Die Maßnahmen nach Artikel 37 Absatz 6 wurden angenommen;
  - b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests des Routers festgestellt, den sie in Zusammenarbeit mit den mitgliedstaatlichen Behörden und Europol durchgeführt hat.

In diesem Durchführungsrechtsakt legt die Kommission auch den Zeitpunkt fest, ab dem die Mitgliedstaaten und die Agenturen der Union mit der Verwendung des Routers beginnen müssen. Dieser Zeitpunkt liegt ein Jahr nach dem gemäß Unterabsatz 1 festgelegten Zeitpunkt.

Die Kommission kann den Zeitpunkt, ab dem die Mitgliedstaaten und die Agenturen der Union mit der Nutzung des Routers beginnen müssen, um höchstens ein Jahr verschieben, falls eine Bewertung der Implementierung des Routers ergeben hat, dass eine solche Verschiebung erforderlich ist. Der betreffende Durchführungsrechtsakt wird nach dem in Artikel 75 Absatz 2 genannten Verfahren erlassen.

- (2) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, ab welchem Zeitpunkt die Mitgliedstaaten und die Agenturen der Union das EPRIS verwenden müssen, sobald folgende Voraussetzungen erfüllt sind:
- a) Die Maßnahmen nach Artikel 44 Absatz 7 wurden angenommen;
  - b) Europol hat den erfolgreichen Abschluss eines umfangreichen Tests des EPRIS festgestellt, den es in Zusammenarbeit mit den mitgliedstaatlichen Behörden durchgeführt hat.

(3) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, ab welchem Zeitpunkt Europol den Mitgliedstaaten biometrische Daten aus Drittländern gemäß Artikel 49 zur Verfügung stellt, sobald folgende Voraussetzungen erfüllt sind:

- a) Der Router ist in Betrieb;
- b) Europol hat den erfolgreichen Abschluss eines umfangreichen Tests der Verbindung festgestellt, den es in Zusammenarbeit mit den mitgliedstaatlichen Behörden und eu-LISA durchgeführt hat.

(4) Die Kommission bestimmt im Wege eines Durchführungsrechtsakts, ab welchem Zeitpunkt Europol Zugang zu den in den Datenbanken der Mitgliedstaaten gespeicherten Daten gemäß Artikel 50 erhält, sobald folgende Voraussetzungen erfüllt sind:

- a) Der Router ist in Betrieb;
- b) Europol hat den erfolgreichen Abschluss eines umfangreichen Tests der Verbindung festgestellt, den es in Zusammenarbeit mit den mitgliedstaatlichen Behörden und eu-LISA durchgeführt hat.

#### *Artikel 74*

### **Übergangsbestimmungen und Ausnahmeregelungen**

(1) Mit Ausnahme der Mitgliedstaaten, die nicht mit der Nutzung des Routers begonnen haben, wenden die Mitgliedstaaten und die Agenturen der Union die Artikel 21 bis 24, Artikel 47 und Artikel 50 Absatz 6 ab dem gemäß Artikel 73 Absatz 1 Unterabsatz 1 festgelegten Zeitpunkt an.

(2) Die Mitgliedstaaten und die Agenturen der Union wenden die Artikel 25 bis 28 und Artikel 50 Absatz 4 ab dem gemäß Artikel 73 Absatz 2 festgelegten Zeitpunkt an.

(3) Die Mitgliedstaaten und die Agenturen der Union wenden den Artikel 49 ab dem gemäß Artikel 73 Absatz 3 festgelegten Zeitpunkt an.

(4) Die Mitgliedstaaten und die Agenturen der Union wenden Artikel 50 Absätze 1, 2, 3, 5 und 7 ab dem gemäß Artikel 73 Absatz 4 festgelegten Zeitpunkt an.

#### *Artikel 75*

### **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. Gibt der Ausschuss keine Stellungnahme ab, so erlässt die Kommission den Durchführungsrechtsakt nicht, und Artikel 5 Absatz 4 Unterabsatz 3 der Verordnung (EU) Nr. 182/2011 findet Anwendung.

#### *Artikel 76*

### **Beratergruppe**

Die Verantwortlichkeiten der Beratergruppe für Interoperabilität von eu-LISA werden auf den Router ausgedehnt. Die Beratergruppe für Interoperabilität stellt eu-LISA insbesondere im Rahmen der Ausarbeitung ihres Jahresarbeitsprogramms und ihres jährlichen Tätigkeitsberichts Fachwissen in Bezug auf den Router zur Verfügung.

#### *Artikel 77*

### **Handbuch**

Die Kommission stellt in enger Zusammenarbeit mit den Mitgliedstaaten, Europol und eu-LISA ein Handbuch für die Umsetzung und die Verwaltung dieser Verordnung zur Verfügung. Das Handbuch enthält technische und operative Leitlinien, Empfehlungen und bewährte Verfahren. Die Kommission nimmt das Handbuch in Form einer Empfehlung an.

## Artikel 78

### Überwachung und Bewertung

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

(2) Bis zum [ein Jahr nach Inkrafttreten der vorliegenden Verordnung] und danach jedes Jahr während der Entwicklungsphase des Routers übermittelt eu-LISA dem Europäischen Parlament und dem Rat jeweils einen Bericht über den Stand der Entwicklung des Routers. Dieser Bericht muss genaue Angaben über die angefallenen Kosten und Informationen über etwaige Risiken enthalten, die sich auf die Gesamtkosten auswirken könnten, welche gemäß Artikel 71 zulasten des Gesamthaushaltsplans der Union gehen.

Sobald die Entwicklung des Routers abgeschlossen ist, übermittelt eu-LISA dem Europäischen Parlament und dem Rat einen Bericht, 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) Bis zum [ein Jahr nach Inkrafttreten der vorliegenden Verordnung] und danach jedes Jahr während der Entwicklungsphase des EPRIS übermittelt Europol dem Europäischen Parlament und dem Rat einen Bericht über den Stand der Vorbereitungen für die Durchführung dieser Verordnung und über den Stand der Entwicklung des EPRIS, der genaue Angaben über die angefallenen Kosten und Informationen über etwaige Risiken enthält, die sich auf die Gesamtkosten auswirken könnten, welche gemäß Artikel 71 zulasten des Gesamthaushaltsplans der Union gehen.

Sobald die Entwicklung des EPRIS abgeschlossen ist, übermittelt Europol dem Europäischen Parlament und dem Rat einen Bericht, 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.

(4) Zum Zwecke der technischen Instandhaltung erhalten eu-LISA und Europol Zugang zu den erforderlichen Informationen über die im Router bzw. im EPRIS durchgeführten Datenverarbeitungsvorgänge.

(5) Zwei Jahre nach Inbetriebnahme des Routers und danach alle zwei Jahre übermittelt eu-LISA dem Europäischen Parlament, dem Rat und der Kommission einen Bericht über die technische Funktionsweise des Routers einschließlich seiner Sicherheit.

(6) Zwei Jahre nach Inbetriebnahme des EPRIS und danach alle zwei Jahre übermittelt Europol dem Europäischen Parlament, dem Rat und der Kommission einen Bericht über die technische Funktionsweise des EPRIS einschließlich seiner Sicherheit.

(7) Drei Jahre nach Inbetriebnahme des Routers und des EPRIS gemäß Artikel 73 und danach alle vier Jahre erstellt die Kommission eine Gesamtbewertung von Prüm II, die Folgendes beinhaltet:

- a) eine Bewertung der Anwendung dieser Verordnung;
- b) eine Analyse der Ergebnisse, gemessen an den Zielen dieser Verordnung, und ihrer Auswirkungen auf die Grundrechte;

- c) die Auswirkungen, die Wirksamkeit und die Effizienz der Leistung von Prüm II und seiner Arbeitspraktiken im Hinblick auf seine Ziele, sein Mandat und seine Aufgaben;
- d) eine Bewertung der Sicherheit von Prüm II.

Die Kommission übermittelt den Bewertungsbericht dem Europäischen Parlament, dem Rat, dem Europäischen Datenschutzbeauftragten und der Europäischen Agentur für Grundrechte.

(8) Die Mitgliedstaaten und Europol stellen eu-LISA und der Kommission die für die Ausarbeitung der Berichte nach den Absätzen 2 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.

(9) Die Mitgliedstaaten stellen Europol und der Kommission die für die Ausarbeitung der Berichte nach den Absätzen 3 und 6 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.

(10) Die Mitgliedstaaten, eu-LISA und Europol stellen der Kommission die für die in Absatz 7 genannten Bewertungen erforderlichen Informationen zur Verfügung. Die Mitgliedstaaten teilen der Kommission zudem die Zahl der bestätigten Übereinstimmungen mit der Datenbank der einzelnen Mitgliedstaaten je Datenkategorie mit.

#### *Artikel 79*

#### **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 Brüssel am

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

## FINANZBOGEN ZU RECHTSAKTEN

### 1 RAHMEN DER GESETZGEBUNGSINITIATIVE

#### 1.1 Bezeichnung der Gesetzgebungsinitiative

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den automatisierten Datenaustausch im Rahmen der polizeilichen Zusammenarbeit („Prüm II“), zur Änderung der Beschlüsse 2008/615/JI und 2008/616/JI des Rates sowie der Verordnungen (EU) 2018/1726, (EU) 2019/817 und (EU) 2019/818 des Europäischen Parlaments und des Rates

#### 1.2 Politikbereich(e)

Politikbereich: Inneres

Tätigkeit: Sicherheit

#### 1.3 Der vorliegende Vorschlag betrifft

eine neue Maßnahme

eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme<sup>43</sup>

die Verlängerung einer bestehenden Maßnahme

die Zusammenführung einer oder mehrerer Maßnahmen unter Neuausrichtung auf eine andere/neue Maßnahme

#### 1.4 Ziel(e)

##### 1.4.1 Allgemeine(s) Ziel(e)

Angesichts dringender operativer Erfordernisse und der Aufforderung des Rates, eine Überarbeitung der Prüm-Beschlüsse<sup>44</sup> in Betracht zu ziehen, um deren Anwendungsbereich zu erweitern und die erforderlichen technischen und rechtlichen Anforderungen zu aktualisieren, soll diese Initiative den automatisierten Datenaustausch auf der Grundlage des Prüm-Rahmens verstärken und den Strafverfolgungsbehörden der Mitgliedstaaten bei der Bekämpfung der Kriminalität behilflich sein.

##### 1.4.2 Einzelziel(e)

Mit der Initiative sollen die folgenden Ziele erreicht werden:

1) **Einzelziel I:** Bereitstellung einer technischen Lösung für einen effizienten automatisierten Datenaustausch zwischen den Strafverfolgungsbehörden der EU, um sie auf einschlägige Daten hinzuweisen, die in der nationalen Datenbank eines anderen Mitgliedstaats verfügbar sind,

2) **Einzelziel II:** Sicherstellung, dass allen zuständigen EU-Strafverfolgungsbehörden mehr einschlägige Daten (insbesondere Gesichtsbilder und Kriminalakten) aus nationalen Datenbanken in anderen Mitgliedstaaten zur Verfügung stehen,

<sup>43</sup> Im Sinne von Artikel 58 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

<sup>44</sup> Beschlüsse 2008/615/JI und 2008/616/JI des Rates.

- 3) **Einzelziel III:** Sicherstellung, dass den nationalen Strafverfolgungsbehörden einschlägige Daten (in Bezug auf die Datenquellen) aus der Europol-Datenbank zur Verfügung stehen und dass Europol seine Daten in vollem Umfang nutzt,
- 4) **Einzelziel IV:** Gewährleistung eines effizienten Zugriffs der Strafverfolgungsbehörden auf die tatsächlichen Daten, die einem „Treffer“ entsprechen und in der nationalen Datenbank eines anderen Mitgliedstaats oder bei Europol abrufbar sind.

### 1.4.3 Erwartete Ergebnisse und Auswirkungen

Bitte geben Sie an, wie sich die Gesetzgebungsinitiative auf die Begünstigten/Zielgruppen auswirken dürfte.

Die Initiative wird eine wirksame Antwort auf die festgestellten Probleme darstellen und den derzeitigen Prüm-Rahmen durch gezielte und starke zusätzliche Kapazitäten ergänzen, um die Mitgliedstaaten bei der Intensivierung des Informationsaustauschs mit dem Endziel der Verhütung und Untersuchung von terroristischen und anderen Straftaten unter voller Wahrung der Grundrechte stärker zu unterstützen.

Alle bevorzugten Optionen kommen letztlich den **Bürgerinnen und Bürgern** zugute, die direkt und indirekt von einer **besseren Bekämpfung der Kriminalität und niedrigeren Kriminalitätsraten** profitieren werden. Im Hinblick auf die Effizienz **sind die nationalen Strafverfolgungsbehörden** die Hauptnutznießer. Die Initiative bietet effiziente Lösungen für Herausforderungen, die andernfalls mit höheren Kosten oder weniger effizient angegangen werden müssten.

### 1.4.4 Leistungsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren sich die Fortschritte und Ergebnisse verfolgen lassen.

Die Entwicklung des Routers und des EPRIS wird beginnen, sobald die Voraussetzungen erfüllt sind, d. h. der Legislativvorschlag von den gesetzgebenden Organen angenommen wurde und die technischen Voraussetzungen erfüllt sind. Während der Router als neues Projekt gestartet wird, sollte die Arbeit am EPRIS auf dem derzeit laufenden Projekt ADEP.EPRIS aufbauen.

Einzelziel: Betriebsbereitschaft zum angestrebten Termin

Bis 2023 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 2024 erfolgen wird.

Aufgrund dieser Annahme wird als Beginn der Entwicklungsphase der Beginn des Jahres 2025 (= 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 Zeitplan entsprechend.

Es wird angenommen, dass die Entwicklung des Routers und des EPRIS in den Jahren 2025 und 2026 erfolgt und die Inbetriebnahme für das Jahr 2027 geplant ist.

Die folgenden Hauptindikatoren ermöglichen die Überwachung der Umsetzung und der Leistung der spezifischen Ziele:

**Einzelziel I:** Bereitstellung einer technischen Lösung für einen effizienten automatisierten Datenaustausch

- Zahl der durchgeführten Vorgänge (Zahl der Anfragen, die vom Router bearbeitet werden können) je Zeitraum,
- Zahl der durchgeführten Vorgänge (Zahl der Anfragen, die vom EPRIS bearbeitet werden können) je Zeitraum.

**Einzelziel II:** Gewährleistung der Verfügbarkeit von mehr einschlägigen Daten

- Anzahl der Abrufanfragen anhand von Gesichtsbildern,
- Anzahl der Abrufanfragen anhand von Kriminalakten,

- Anzahl der Übereinstimmungen nach Abfragen anhand von Gesichtsbildern,
- Anzahl der Übereinstimmungen nach Abfragen anhand von Kriminalakten.

**Einzelziel III:** Sicherstellung, dass den nationalen Strafverfolgungsbehörden einschlägige Daten (in Bezug auf die Datenquellen) aus der Europol-Datenbank zur Verfügung stehen und dass Europol seine Daten in vollem Umfang nutzt

- Anzahl der Abrufanfragen für die aus Drittländern stammenden biometrischen Europol-Daten,
- Anzahl der Treffer bei den aus Drittländern stammenden biometrischen Europol-Daten,
- Anzahl der von Europol gestellten Abrufanfragen,
- Anzahl der Übereinstimmungen nach den von Europol gestellten Anfragen.

**Einzelziel IV:** Gewährleistung eines effizienten Zugriffs der Strafverfolgungsbehörden auf die tatsächlichen Daten, die einem „Treffer“ entsprechen und in der nationalen Datenbank eines anderen Mitgliedstaats oder bei Europol abrufbar sind

- Anzahl der Übereinstimmungen nach Abrufanfragen im Vergleich zur Anzahl der Anfragen für den Austausch von Kerndaten.

## 1.5 Begründung der Gesetzgebungsinitiative

### 1.5.1 Kurz- oder langfristig zu deckender Bedarf, einschließlich eines detaillierten Zeitplans für die Einleitung der Umsetzung der Gesetzgebungsinitiative

Die Einleitung der Umsetzung der Gesetzgebungsinitiative erfordert technische und verfahrenstechnische Maßnahmen auf EU- und nationaler Ebene, die mit dem Inkrafttreten der überarbeiteten Rechtsvorschrift beginnen sollten. Die entsprechenden Ressourcen – insbesondere die personellen Ressourcen – sollten im Laufe der Zeit entsprechend den Maßnahmen aufgestockt werden.

Die wichtigsten Anforderungen nach Inkrafttreten des Vorschlags sind wie folgt:

#### **Erstellen des Prüm Routers:**

Es soll den Prüm-II-Nutzern eine einzige Verbindung zu allen Datenbanken der Mitgliedstaaten und zu Europol-Daten zur Verfügung gestellt werden, um Abrufanfragen anhand biometrischer Daten zu übermitteln.

Ein neues Follow-up-Verfahren auf EU-Ebene mit einem halbautomatischen Austausch von tatsächlichen Daten, die einem „Treffer“ entsprechen, soll eingeführt werden.

#### **Einrichten/Erweitern des EPRIS**

Es soll den Prüm-II-Nutzern eine einzige Verbindung zu allen Datenbanken der teilnehmenden Mitgliedstaaten, die Kriminalakten enthalten, zur Verfügung gestellt werden, damit sie Abrufanfragen anhand von Kriminalakten stellen können.

#### **Ermöglichung des Austauschs neuer Datenkategorien durch die Mitgliedstaaten**

Der Austausch von Gesichtsbildern und Kriminalakten soll mithilfe von Prüm II ermöglicht werden.

**Ermöglichung der automatischen Überprüfung von Daten aus Drittländern durch die Mitgliedstaaten bei Europol als Teil des Prüm-Rahmens:**

Die Mitgliedstaaten sollen die Möglichkeit erhalten, biometrische Daten aus Drittländern über Prüm II zu überprüfen.

**Ermöglichung des Abgleichs von Daten aus Drittländern mit den nationalen Datenbanken der Mitgliedstaaten durch Europol:**

Europol soll in die Lage versetzt werden, Daten aus Drittländern für die Abfrage der Datenbanken der Mitgliedstaaten über Prüm II zu verwenden.

Da jedes Ziel erreicht werden muss, besteht die vollständige Lösung aus einer Kombination der oben genannten Punkte.

- 1.5.2 *Mehrwert aufgrund des Tätigwerdens der Union (kann sich aus unterschiedlichen Faktoren ergeben, z. B. Vorteile durch Koordinierung, Rechtssicherheit, größerer Wirksamkeit oder Komplementarität). Für die Zwecke dieser Nummer bezeichnet der Ausdruck „Mehrwert aufgrund des Tätigwerdens der Union“ den Wert, der sich aus dem Tätigwerden der Union ergibt und den Wert ergänzt, der andernfalls allein von den Mitgliedstaaten geschaffen worden wäre.*

Schwere Kriminalität und Terrorismus sind grenzüberschreitender Natur. Sie lassen sich daher mit Maßnahmen auf nationaler Ebene allein nicht wirksam bekämpfen. Aus diesem Grund haben sich die Mitgliedstaaten dafür entschieden, im Rahmen der EU zusammenzuarbeiten, um auf die Bedrohungen durch schwere Kriminalität und Terrorismus zu reagieren.

Darüber hinaus erfordern sich entwickelnde Sicherheitsbedrohungen, die durch die unterschiedlichen Möglichkeiten der Kriminellen, die Vorteile des digitalen Wandels, der Globalisierung und der Mobilität auszunutzen, auch eine wirksame Unterstützung der Arbeit der nationalen Strafverfolgungsbehörden auf EU-Ebene. EU-Maßnahmen bieten eine wirksame und effiziente Möglichkeit, die Mitgliedstaaten bei der Bekämpfung von schwerer Kriminalität und Terrorismus stärker zu unterstützen, um diesen sich entwickelnden Bedrohungen zu begegnen.

Der Vorschlag wird zu erheblichen Skaleneffekten führen, da er Aufgaben und Dienste, die auf EU-Ebene effizienter erledigt werden können von der nationalen Ebene hin zu Europol verlagert. Der Vorschlag bietet daher effiziente Lösungen für Herausforderungen, die andernfalls durch 27 einzelne nationale Lösungen mit höheren Kosten angegangen werden müssten, oder für Herausforderungen, die aufgrund ihres grenzüberschreitenden Charakters auf nationaler Ebene überhaupt nicht bewältigt werden können.

- 1.5.3 *Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse*

Die Bewertung der Prümer Beschlüsse ergab Folgendes:

- Der Prüm-Rahmen ist im Hinblick auf die aktuellen und künftigen Bedürfnisse und Herausforderungen im Bereich der Sicherheit und insbesondere der strafrechtlichen Ermittlungen von Bedeutung. Die Zusammenarbeit und der Austausch von Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten sowie die Möglichkeit, DNA-, Fingerabdruck- und Fahrzeugregisterdaten in den Datenbanken anderer Mitgliedstaaten zur

Verhütung und Untersuchung von Straftaten abzurufen und abzugleichen, werden als äußerst wichtig für den Schutz der inneren Sicherheit der EU und die Sicherheit der EU-Bürgerinnen und -Bürger erachtet.

- Das Konzept der Prüm-Beschlüsse entspricht den Bedürfnissen der Ermittler, der Opfer von Straftaten, der Forensiker, der Datenbankverwahrer und der Angehörigen der Rechtsberufe im Hinblick auf die in diesem Rahmen verfügbaren Datenkategorien.
- Der automatisierte Datenaustausch im Prüm-Rahmen bringt insofern Effizienzgewinne beim Austausch strafverfolungsrelevanter Informationen mit sich, als er die Geschwindigkeit des Austauschs erhöht und den Verwaltungsaufwand bis zu einem gewissen Grad verringert, da nicht mehr jeder Mitgliedstaat bilateral abgefragt werden muss. Diese Vorteile überwiegen die für die Einführung des Prüm-Rahmens erforderlichen Investitionen. Darüber hinaus ermöglicht das automatisierte Prüm-System erhebliche Einsparungen bei der Arbeitszeit. Allerdings besteht nach wie vor ein gewisser Verwaltungsaufwand im Zusammenhang mit der Überprüfung von Treffern und der Meldung sowie der Entgegennahme bzw. Übermittlung von Informationen der zweiten Stufe.
- Seit der Annahme der Prüm-Beschlüsse im Jahr 2008 haben sich auch im Hinblick auf den EU-Rechtsrahmen, den operativen Bedarf und die technischen und forensischen Möglichkeiten erhebliche Entwicklungen und Veränderungen ergeben. Auf EU- und internationaler Ebene wurden mehrere Initiativen und Systeme entwickelt, die den Informationsaustausch zwischen den Strafverfolgungsbehörden erleichtern sollen. Die Prüm-Beschlüsse und andere einschlägige EU-/internationale Rechtsvorschriften, einschließlich des Interoperabilitätsrahmens, ergänzen sich weitgehend. Außerdem bestehen Komplementaritäten mit einigen zentralen Informationssystemen der EU, die unterschiedlichen Zwecken dienen. Potenzielle Synergien können in Bezug auf Europol und den Interoperabilitätsrahmen ermittelt werden.
- Die Umsetzung der Prüm-Beschlüsse erfolgte jedoch nur langsam. Fast zehn Jahre nach Ablauf der Umsetzungsfrist am 26. August 2011 haben noch nicht alle Mitgliedstaaten das Bewertungsverfahren abgeschlossen, und eine Reihe von bilateralen Verbindungen wurden aufgrund der technischen Komplexität und des hohen finanziellen und personellen Aufwands noch nicht hergestellt. Folglich können Abfragen nicht mit den Daten in einigen Mitgliedstaaten abgeglichen werden, wenn die entsprechende bilaterale Verbindung nicht hergestellt wurde. Dies erschwert die Ermittlung von Straftätern und die Aufdeckung grenzüberschreitender Verbindungen zwischen Straftaten, was den Informationsaustausch und das Funktionieren des Prüm-Systems beeinträchtigt.
- Ein weiteres Problem, das das Funktionieren des Prüm-Systems behindert, ist die Tatsache, dass die Weiterverfolgung von Treffern im Prüm-Rahmen nach nationalem Recht und damit außerhalb des Anwendungsbereichs der Prüm-Beschlüsse erfolgt. Aufgrund der unterschiedlichen nationalen Vorschriften und Verfahren ist der Austausch zusätzlicher Daten nach einem Treffer so uneinheitlich, dass es manchmal Wochen oder sogar Monate dauert, bis die einschlägigen Informationen zu einem Treffer vorliegen.

#### 1.5.4 *Vereinbarkeit mit dem Mehrjährigen Finanzrahmen sowie mögliche Synergieeffekte mit anderen geeigneten Instrumenten*

Die auf EU-Ebene erforderlichen Investitionen sind mit dem Mehrjährigen Finanzrahmen 2021-2027 vereinbar, wobei Mittel aus den Rubriken Sicherheit und Verteidigung sowie Migration und Grenzen bereitgestellt werden.

### *1.5.5 Bewertung der verschiedenen verfügbaren Finanzierungsoptionen, einschließlich der Möglichkeiten für eine Umschichtung*

Die zur Finanzierung der Entwicklung des Prüm-II-Rahmens erforderlichen Mittel wurden nicht im Rahmen der MFR-Zuweisungen für Europol und eu-LISA eingeplant, da es sich um einen neuen Vorschlag handelt, für den die Beträge zum Zeitpunkt des Vorschlags nicht bekannt waren. Es wird vorgeschlagen, die Mittelzuweisungen für Europol und eu-LISA in den Jahren 2024, 2025, 2026 und 2027 durch entsprechende Kürzungen des Fonds für die innere Sicherheit (ISF) bzw. des Instruments für Grenzmanagement und Visa (BMVI) zu erhöhen.

## 1.6 Laufzeit und finanzielle Auswirkungen der Gesetzgebungsinitiative

befristete Laufzeit

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

Finanzielle Auswirkungen von JJJJ bis JJJJ

unbefristete Laufzeit

Umsetzung mit einer Anlaufphase von 2024 bis 2026  
anschließend reguläre Umsetzung.

## 1.7 Vorgeschlagene Methode(n) der Mittelverwaltung<sup>45</sup>

Direkte Mittelverwaltung durch die Kommission

- X durch ihre Dienststellen, einschließlich ihres Personals in den Delegationen der Union
- durch Exekutivagenturen

Geteilte Mittelverwaltung mit Mitgliedstaaten

Indirekte Mittelverwaltung durch Übertragung von Haushaltsvollzungsaufgaben an:

internationale Einrichtungen und deren Agenturen (bitte angeben)

die EIB und den Europäischen Investitionsfonds

Einrichtungen im Sinne der Artikel 70 und 71

öffentliche Einrichtungen

privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern sie ausreichende finanzielle Garantien bieten

privatrechtliche Einrichtungen eines Mitgliedstaats, die mit der Einrichtung einer öffentlich-privaten Partnerschaft betraut werden und die ausreichende finanzielle Garantien 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.

### Anmerkungen

Maßnahmenbündel	Entwicklungsphase	Betriebsphase	Methode der Mittelverwaltung	Akteur
Entwicklung und Unterhaltung (des Routers und des EPRIS)	X	X	indirekt	eu-LISA Europol
Anpassung der Europol-	X	X	indirekt	Europol

<sup>45</sup> Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb: <https://myintracomm.ec.europa.eu/budgweb/DE/man/budgmanag/Pages/budgmanag.aspx>.

Maßnahmenbündel	Entwicklungsphase	Betriebsphase	Methode der Mittelverwaltung	Akteur
Datenbanken				
Entwicklung oder Verbesserung bestehender nationaler Datenbanken, Integration der nationalen Systeme	X	X	geteilt (oder direkt)	Kommission + Mitgliedstaaten

Die Entwicklungsphase beginnt 2024 und dauert bis zur Bereitstellung der einzelnen Komponenten der Initiative, d. h. von 2024 bis 2027.

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 müssen die Mitgliedstaaten ihre nationalen Systeme entsprechend anpassen, damit sie an den Router und das EPRIS angeschlossen werden können, und die erforderlichen Maßnahmen ergreifen, um den Austausch von Gesichtsbildern und Kriminalakten zu gewährleisten.

3. Indirekte Mittelverwaltung: eu-LISA und Europol werden für die Entwicklung des IT-Teils des Projekts verantwortlich sein, d. h. für den Router bzw. das EPRIS. Dies würde alle notwendigen Änderungen an der bestehenden Architektur einschließen, um die im Vorschlag beschriebenen Funktionen zu gewährleisten.

Während der Betriebsphase von Europol werden eu-LISA und Europol alle technischen Tätigkeiten im Zusammenhang mit der Wartung des Routers bzw. EPRIS ausführen.

Europol wird die Entwicklung und Wartung seiner Systeme übernehmen, um sicherzustellen, dass seine Daten im Zusammenhang vom Prüm-Rahmen verfügbar sind.

## 2 VERWALTUNGSMABNAHMEN

### 2.1 Überwachung und Berichterstattung

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

eu-LISA und Europol tragen dafür Sorge, dass Verfahren vorhanden sind, mit denen die Entwicklung und die Funktionsweise des Routers bzw. des EPRIS anhand der Zielvorgaben für die Planung und die Kosten bzw. für die technische Leistung, Kostenwirksamkeit, Sicherheit und Dienstleistungsqualität überwacht werden können.

Spätestens ein Jahr nach Annahme der vorgeschlagenen Verordnung und danach jedes Jahr während der Entwicklungsphase des Routers übermittelt eu-LISA dem Europäischen Parlament und dem Rat einen Bericht über den Stand der Entwicklung des Routers. Der Bericht muss ausführliche Angaben zu den entstandenen Kosten und Angaben zu etwaigen Risiken enthalten, die sich auf die Gesamtkosten auswirken könnten, welche zulasten des Gesamthaushaltsplans der Union gehen.

Sobald die Entwicklung des Routers abgeschlossen ist, übermittelt eu-LISA dem Europäischen Parlament und dem Rat einen Bericht, 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.

Spätestens ein Jahr nach Annahme der vorgeschlagenen Verordnung und danach jedes Jahr während der Entwicklungsphase des EPRIS übermittelt Europol dem Europäischen Parlament und dem Rat einen Bericht über den Stand der Vorbereitungen für die Durchführung dieser Verordnung und über den Stand der Entwicklung des EPRIS, einschließlich detaillierter Informationen über die entstandenen Kosten und Informationen über etwaige Risiken, die sich auf die aus dem Gesamthaushaltsplan der Union zu tragenden Gesamtkosten auswirken könnten.

Sobald die Entwicklung des EPRIS abgeschlossen ist, übermittelt Europol dem Europäischen Parlament und dem Rat einen Bericht, 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.

Zum Zwecke der technischen Instandhaltung erhalten eu-LISA und Europol Zugriff auf die erforderlichen Informationen über die im Router bzw. EPRIS durchgeführten Datenverarbeitungsvorgänge.

Zwei Jahre nach Inbetriebnahme des Routers und danach alle zwei Jahre übermittelt eu-LISA dem Europäischen Parlament, dem Rat und der Kommission einen Bericht über die technische Funktionsweise des Routers einschließlich der Sicherheit des Systems.

Zwei Jahre nach Inbetriebnahme des EPRIS und danach alle zwei Jahre übermittelt Europol dem Europäischen Parlament, dem Rat und der Kommission einen Bericht über die technische Funktionsweise des Routers einschließlich der Sicherheit des Systems.

Drei Jahre nach Inbetriebnahme aller Komponenten der vorgeschlagenen Verordnung und danach alle vier Jahre erstellt die Kommission eine Gesamtbewertung von Prüm II, die Folgendes umfasst:

- a) eine Beurteilung der Anwendung dieser Verordnung,

- b) eine Analyse der Ergebnisse, gemessen an den Zielen der vorliegenden Verordnung und ihrer Auswirkungen auf die Grundrechte,
- c) die Wirkung, die Effektivität und die Effizienz des Betriebs und der Arbeitspraktiken des Prüm II im Hinblick auf dessen Ziele, Mandat und Aufgaben,
- d) eine Beurteilung der Sicherheit des Prüm II.

Die Kommission übermittelt den Bewertungsbericht dem Europäischen Parlament, dem Rat, dem Europäischen Datenschutzbeauftragten und der Agentur der Europäischen für Grundrechte.

Die Mitgliedstaaten und Europol stellen eu-LISA und der Kommission die Informationen zur Verfügung, die für die Ausarbeitung der oben genannten Berichte erforderlich sind. Diese Informationen dürfen nicht zu einer Beeinträchtigung der Arbeitsverfahren führen oder Angaben enthalten, die Rückschlüsse auf Quellen, Bedienstete oder Ermittlungen der benannten Behörden ermöglichen.

Die Mitgliedstaaten stellen Europol und der Kommission die Informationen zur Verfügung, die für die Ausarbeitung der oben genannten Berichte erforderlich sind. Diese Informationen dürfen nicht zu einer Beeinträchtigung der Arbeitsverfahren führen oder Angaben enthalten, die Rückschlüsse auf Quellen, Bedienstete oder Ermittlungen der benannten Behörden ermöglichen.

eu-LISA und Europol stellen der Kommission die Informationen zur Verfügung, die zur Durchführung der Bewertungen erforderlich sind.

## 2.2 **Verwaltungs- und Kontrollsystem(e)**

### 2.2.1 *Angaben zu den ermittelten Risiken und dem/den zu deren Eindämmung eingerichteten System(en) der internen Kontrolle*

Es wurden folgende Risiken ermittelt:

- stark in Anspruch genommene operative Ressourcen aufgrund des zunehmenden Datenflusses und einer sich ständig weiterentwickelnden Landschaft krimineller Aktivitäten,
- Vervielfachung der Aufgaben und Anfragen sowohl für eu-LISA als auch für Europol,
- Fehlen hinreichender finanzieller und personeller Ressourcen zur Deckung des operativen Bedarfs,
- Fehlen von IKT-Ressourcen, was zu Verzögerungen bei den notwendigen Weiterentwicklungen und Aktualisierungen des Kernsystems führt,
- Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten durch Europol und die Notwendigkeit, die verfahrensmäßigen und technischen Garantien regelmäßig zu bewerten und anzupassen, um den Schutz von personenbezogenen Daten und Grundrechten zu gewährleisten,
- Abhängigkeiten zwischen den von eu-LISA durchzuführenden Vorbereitungen in Bezug auf den Router und den von Mitgliedstaaten und Europol durchzuführenden Vorbereitungen in Bezug auf die Einrichtung einer technischen Schnittstelle zur Übermittlung von Daten mithilfe des Routers.

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, insbesondere

1. 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-Projekte vom Auftragnehmer nicht lückenlos befolgt und angewandt werden, um die Kosten zu senken,
3. das Risiko, dass der Auftragnehmer aus projektunabhängigen Gründen in finanzielle Schwierigkeiten gerät.

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.

Europol implementiert einen speziellen internen Kontrollrahmen, der auf dem internen Kontrollrahmen der Europäischen Kommission und auf dem ursprünglichen integrierten internen Kontrollrahmen des „Committee of Sponsoring Organisations“ basiert. Das einheitliche Programmplanungsdokument muss Informationen über die internen Kontrollsysteme enthalten, während der konsolidierte Jahresbericht Informationen über die Effizienz und Wirksamkeit der internen Kontrollsysteme auch in Bezug auf die Risikobewertung enthalten muss. Aus dem konsolidierten Jahresbericht 2019 geht hervor, dass das interne Kontrollsystem von Europol auf der Grundlage der Analyse der Komponenten und Grundsätze der internen Kontrolle, die im Laufe des Jahres 2019 unter Verwendung sowohl quantitativer als auch qualitativer Elemente überwacht wurden, als vorhanden und in integrierter Weise in der gesamten Agentur funktionierend bewertet wird.

Für den von eu-LISA ausgeführten Haushalt ist ein spezifischer interner Kontrollrahmen auf der Grundlage des Internen Kontrollrahmens der Europäischen Kommission erforderlich. Das Einheitliche Programmplanungsdokument muss Informationen über die internen Kontrollsysteme bereitstellen, während der konsolidierte jährliche Tätigkeitsbericht Informationen über die Effizienz und Wirksamkeit der internen Kontrollsysteme auch in Bezug auf die Risikobewertung enthalten muss. Dem konsolidierten jährlichen Tätigkeitsbericht von 2019 zufolge konnte die Leitung der Agentur mit hinreichender Sicherheit feststellen, dass geeignete interne Kontrollen vorhanden sind, die bestimmungsgemäß funktionieren. Die größten Risiken wurden im Laufe des Jahres angemessen ermittelt und bewältigt. Dies wird auch durch die Ergebnisse der internen und externen Audits bestätigt.

Sowohl für Europol als auch für eu-LISA ist außerdem eine zusätzliche Ebene der internen Überwachung durch die interne Rechnungsprüfung von Europol auf der Grundlage eines jährlichen Prüfungsplans vorgesehen, bei dem insbesondere die Bewertung der Risiken bei Europol berücksichtigt wird. Die interne Rechnungsprüfung unterstützt Europol über einen systematischen und disziplinierten Ansatz zur Bewertung der Wirksamkeit von

Risikomanagement-, Kontroll- und Governance-Prozessen und Empfehlungen für deren Verbesserung bei der Verwirklichung ihrer Ziele.

Der Europäische Datenschutzbeauftragte (EDSB) und die Datenschutzbeauftragten der beiden Agenturen (eine unabhängige Funktion, die direkt dem Sekretariat des Verwaltungsrats zugeordnet ist) überwachen die Verarbeitung personenbezogener Daten durch die Agenturen.

Zudem führt die GD HOME als Partner-GD von Europol und eu-LISA jährlich ein Risikomanagementverfahren durch, um potenzielle hohe Risiken im Zusammenhang mit den Tätigkeiten der Agenturen zu ermitteln und zu bewerten. Risiken, die als wesentlich eingestuft sind, werden jährlich im Managementplan der GD HOME gemeldet und von einem Aktionsplan begleitet, der die Abhilfemaßnahmen anführt.

### 2.2.2 *Schätzung und Begründung der Kosteneffizienz der Kontrollen (Verhältnis zwischen den Kontrollkosten und dem Wert der betreffenden verwalteten Mittel) sowie Bewertung des erwarteten Ausmaßes des Fehlerrisikos (bei Zahlung und beim Abschluss)*

Die Kommission erstattet Bericht über das Verhältnis der Kontrollkosten zum Wert der betreffenden verwalteten Mittel. In Bezug auf die mit der indirekten Mittelverwaltung betrauten Einrichtungen und die dezentralen Agenturen, zu denen ja auch Europol und eu-LISA zählen, hat die GD HOME dieses Verhältnis in ihrem jährlichen Tätigkeitsbericht für 2020 mit 0,21 % beziffert.

Der Europäische Rechnungshof hat die Rechtmäßigkeit und Ordnungsmäßigkeit der Rechnungsführung von Europol und eu-LISA für 2019 bestätigt, was eine Fehlerquote von unter 2 % impliziert. Es gibt keine Anzeichen dafür, dass sich die Fehlerquote in den kommenden Jahren verschlechtern wird.

Darüber hinaus sieht Artikel 80 der Finanzregelung sowohl für Europol als auch für eu-LISA die Möglichkeit vor, dass die Agentur eine interne Rechnungsprüfung mit anderen, in demselben Politikbereich tätigen Unionseinrichtungen teilen kann, wenn die interne Rechnungsprüfung einer einzigen Unionseinrichtung nicht kosteneffizient ist.

## 2.3 Prävention von Betrug und Unregelmäßigkeiten

*Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen, z. B. im Rahmen der Betrugsbekämpfungsstrategie, bereits bestehen oder angedacht sind.*

Die geplanten Maßnahmen zur Betrugsbekämpfung sind in Artikel 35 der Verordnung (EU) Nr. 1077/2011 festgelegt.

Die Maßnahmen zur Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen sind unter anderem in Artikel 66 der Europol-Verordnung und in Titel X der Finanzregelung für Europol dargelegt.

Europol soll sich – im Einklang mit ihrer internen Betrugsbekämpfungsstrategie – insbesondere an den Betrugsbekämpfungsmaßnahmen des Europäischen Amtes für Betrugsbekämpfung beteiligen und die Kommission unverzüglich über mutmaßliche Betrugsfälle und andere finanzielle Unregelmäßigkeiten unterrichten.

Eine Aktualisierung der Betrugsbekämpfungsstrategie von Europol wurde vom Verwaltungsrat im Jahr 2020 angenommen.

Die Maßnahmen zur Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen werden unter anderem in Artikel 50 der eu-LISA-Verordnung und Titel X der Finanzregelung von eu-LISA dargelegt.

eu-LISA beteiligt sich vor allem an den Betrugsbekämpfungsmaßnahmen des Europäischen Amtes für Betrugsbekämpfung und informiert die Kommission entsprechend ihrer internen Betrugsbekämpfungsstrategie unverzüglich über mutmaßliche Betrugsfälle und sonstige finanzielle Unregelmäßigkeiten.

Darüber hinaus hat die GD HOME als Partner-GD ihre eigene Betrugsbekämpfungsstrategie auf der Grundlage der vom OLAF bereitgestellten Methodik entwickelt und umgesetzt. Dezentrale Agenturen, einschließlich Europol und eu-LISA, fallen in den Bereich der Strategie. In ihrem Jährlichen Tätigkeitsbericht 2020 kam die GD HOME zu dem Schluss, dass die Verfahren zur Betrugsprävention und -aufdeckung zufriedenstellend funktionierten und trug somit zur Sicherstellung bei, dass die internen Kontrollziele erreicht wurden.

## 3 GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DER GESETZGEBUNGSINITIATIVE

### 3.1 Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

Bestehende Haushaltslinien

In der Reihenfolge der Rubriken des Mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des Mehrjährigen	Haushaltslinie	Art der Ausgaben	Beitrag
-------------------------	----------------	------------------	---------

Finanzrahmens	Nummer	GM/NGM <sup>46</sup>	von EFTA-Ländern <sup>47</sup>	von Bewerberländern <sup>48</sup>	von Drittländern	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
---------------	--------	----------------------	--------------------------------	-----------------------------------	------------------	---

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Beitrag			
	Nummer	GM/NGM	von EFTA-Ländern	von Bewerberländern	von Drittländern	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
5	12.02.01 – Fonds für die innere Sicherheit	GM/NGM	NEIN	NEIN	NEIN	NEIN
5	12.01.01 – Unterstützungsausgaben für den Fonds für die innere Sicherheit	NGM	NEIN	NEIN	NEIN	NEIN
5	12.10.01 – Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol)	NGM	NEIN	NEIN	NEIN	NEIN
4	11.10.02 – Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA)	NGM	NEIN	NEIN	NEIN	NEIN

<sup>46</sup> GM = getrennte Mittel/NGM = nicht getrennte Mittel.

<sup>47</sup> EFTA: Europäische Freihandelsassoziation.

<sup>48</sup> Kandidatenländer und gegebenenfalls potenzielle Kandidatenländer des Westbalkans.

## 3.2 Geschätzte Auswirkungen auf die Ausgaben

### 3.2.1 Übersicht über die geschätzten Auswirkungen auf die Ausgaben

in Mio. EUR (3 Dezimalstellen)

<b>Rubrik des Mehrjährigen Finanzrahmens</b>	5	Sicherheit und Verteidigung
--	---	-----------------------------

Europol			Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027	INSGESAMT
Titel 1: Personalausgaben	Verpflichtungen	(1)		0,551	1,102	0,847	0,847	<b>3,347</b>
	Zahlungen	(2)		0,551	1,102	0,847	0,847	<b>3,347</b>
Titel 2: Infrastruktur- und Betriebsausgaben	Verpflichtungen	(1a)		1,49	1,052	0,516	0,516	<b>3,574</b>
	Zahlungen	(2a)		1,49	1,052	0,516	0,516	<b>3,574</b>
Titel 3: Betriebskosten	Verpflichtungen	(3a)						
	Zahlungen	(3b)						
<b>Mittel INSGESAMT für Europol</b>	Verpflichtungen	=1+1a +3a		<b>2,041</b>	<b>2,154</b>	<b>1,363</b>	<b>1,363</b>	<b>6,921</b>
	Zahlungen	=2+2a +3b		<b>2,041</b>	<b>2,154</b>	<b>1,363</b>	<b>1,363</b>	<b>6,921</b>

Anmerkung: Die im Rahmen dieses Vorschlags beantragten zusätzlichen Mittel für Europol werden aus dem Fonds für die innere Sicherheit (ISF) unter der Rubrik 5 gedeckt.

<b>Rubrik des Mehrjährigen Finanzrahmens</b>	<b>4</b>	<b>– Migration und Grenzen</b>
--	----------	--------------------------------

eu-LISA			Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027	INSGESAMT
Titel 1: Personalausgaben	Verpflichtungen	(1)		0,456	0,988	1,52	1,45	<b>4,414</b>
	Zahlungen	(2)		0,456	0,988	1,52	1,45	<b>4,414</b>
Titel 2: Infrastruktur- Betriebsausgaben und	Verpflichtungen	(1a)		4,15	3,55	1,4	0	<b>9,1</b>
	Zahlungen	(2a)		4,15	3,55	1,4	0	<b>9,1</b>
Titel 3: Betriebskosten	Verpflichtungen	(3a)		0	0	1	1,2	<b>2,2</b>
	Zahlungen	(3b)		0	0	1	1,2	<b>2,2</b>
<b>Mittel INSGESAMT für eu-LISA</b>	Verpflichtungen	=1+1a +3a		<b>4,606</b>	<b>4,538</b>	<b>3,92</b>	<b>2,65</b>	<b>15,714</b>
	Zahlungen	=2+2a +3b		<b>4,606</b>	<b>4,538</b>	<b>3,92</b>	<b>2,65</b>	<b>15,714</b>

Anmerkung: Die im Rahmen dieses Vorschlags beantragten zusätzlichen Mittel für eu-LISA werden aus dem Instrument für Grenzmanagement und Visa (BMVI) unter der Rubrik 4 gedeckt.

<b>Rubrik des Mehrjährigen Finanzrahmens</b>	5	Resilienz, Sicherheit und Verteidigung
--	---	--

GD HOME			Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 20 27	INSGESAMT
Fonds für die innere Sicherheit	Verpflichtungen	(1)		13,64	40	40		<b>93,64</b>
	Zahlungen	(2)		4,68	6,55	9,39		<b>34,65</b>
<b>Mittel INSGESAMT GD HOME</b>	Verpflichtungen			13,64	40	40		<b>93,64</b>
	Zahlungen			4,68	6,55	9,39		<b>34,65</b>

Anmerkung: Die im Rahmen dieses Vorschlags beantragten Mittel werden durch Mittel gedeckt, die bereits in dem der ISF-Verordnung zugrunde liegenden Finanzbogen festgelegt sind. Im Zusammenhang mit diesem Legislativvorschlag werden keine zusätzlichen finanziellen oder personellen Ressourcen beantragt.

Die Kosten pro Mitgliedstaat umfassen Folgendes:

- die Modernisierung nationaler Infrastruktur, um den Austausch von Webdiensten zu unterstützen und die Verbindung mit dem zentralen Router herzustellen, was wiederum Bemühungen erfordert, die neue Architekturlandschaft zu analysieren und zu definieren,
- die Modernisierung nationaler Infrastruktur, um den Austausch von Webdiensten zu unterstützen und die Verbindung mit dem zentralen Router herzustellen,
- die Konfiguration eines Systems zum Austausch von Webdiensten und den Aufbau der Verbindung mit dem zentralen Router,
- den Entwurf einer neuen nationalen Architektur und der Spezifikationen, um den Zugriff auf die nationalen Daten über die entwickelten Lösungen (Router und EPRIS) zu gewährleisten,

- die Einrichtung eines neuen Indexes oder die Bereitstellung eines bereits bestehenden Indexes für den Austausch von Kriminalakten,
- die Einrichtung einer neuen Gesichtsbilddatenbank oder die Bereitstellung einer bereits bestehenden Gesichtsbilddatenbank für den Austausch,
- die Integration der einzelstaatlichen Lösung,
- allgemeine Kosten im Zusammenhang mit der Projektverwaltung.

In der folgenden Tabelle sind die Kosten pro Kategorie aufgeführt:

Ziele und Ergebnisse angeben	GD HOME ↓	Typ	Jahr 2023		Jahr 2024		Jahr 2025		Jahr 2026		Jahr 2027		INSGESAMT	
			Anzahl	Kosten	Gesamtzahl	Gesamtkosten								
Router	Anschluss an den Router der bestehenden Datenbanken			26	2,314	26	6,787	26	6,787			26	15,89	
Gesichtsbilder	Aufbau der neuen Datenbank			13 *	2,84	13	8,329	13	8,329			13	19,5	
	Verbindung der Datenbank mit dem Router			26	2,72	26	7,996	26	7,996			26	18,72	

Kriminalakten	Einrichtung einer Datenbank für Kriminalakten und Anbindung an das EPRIS		26	5,763	26	16,959	26	16,959			26	39,7
Insgesamt				13,64		40		40				93,64

\*Geschätzte MS ohne Gesichtsbilddatenbank

<b>Rubrik des Mehrjährigen Finanzrahmens</b>	<b>7</b>	„Verwaltungsausgaben“
--	----------	-----------------------

in Mio. EUR (3 Dezimalstellen)

		Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027	INSGESAMT
<b>GD HOME</b>							
• Personalausgaben			0,608	0,684	0,608	0,608	2,508
• Sonstige Verwaltungsausgaben			0,225	0,225	0,186	0,186	0,822
<b>GD HOME INSGESAMT</b>	Mittel						

<b>Mittel INSGESAMT unter der RUBRIK 7 des Mehrjährigen Finanzrahmens</b>	(Verpflichtungen insg. = Zahlungen insg.)		0,833	0,833	0,794	0,794	3,330
---	---	--	-------	-------	-------	-------	-------

in Mio. EUR (3 Dezimalstellen)

		Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027	INSGESAMT
--	--	-----------	-----------	-----------	-----------	-----------	-----------

<b>Mittel INSGESAMT unter den RUBRIKEN 1 bis 5 des Mehrjährigen Finanzrahmens</b>	Verpflichtungen		20,287	46,692	45,283	4,013	<b>116,275</b>
	Zahlungen		11,329	13,247	14,647	18,059	<b>57,282</b>

### 3.2.2 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 angeben			Jahr		Jahr		Jahr		Jahr		Jahr		INSGESAMT	
			2023		2024		2025		2026		2027			
↓	Typ	Durchschnittskosten <sup>49</sup>	Anzahl	Kosten	Anzahl	Kosten								
<b>Europol-Kosten (nicht im Zusammenhang mit personellen Ressourcen)</b>														
- Ergebnis	Infrastruktur und Unterhaltung				0,764		0,326		0,226		0,226			1,542
- Ergebnis	Auftragnehmer				0,726		0,726		0,290		0,290			2,032
<b>GESAMTKOSTEN</b>					1,490		1,052		0,516		0,516			3,574

<sup>49</sup> Aufgrund ihres spezifischen operativen Charakters ist es nicht möglich, genaue Stückkosten je Ergebnis oder ein genaues erwartetes Volumen an Ergebnissen zu ermitteln, insbesondere da einige Ergebnisse mit Strafverfolgungsmaßnahmen zusammenhängen, die eine Reaktion auf unvorhersehbare kriminelle Aktivitäten sind.

### 3.2.3 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 angeben			Jahr		Jahr		Jahr		Jahr		Jahr		INSGESAMT	
			2023		2024		2025		2026		2027			
↓	Typ	Durchschnittskosten <sup>50</sup>	Anzahl	Kosten	Anzahl	Kosten								
<b>eu-LISA-Kosten (nicht im Zusammenhang mit personellen Ressourcen)</b>														
- Ergebnis	Infrastruktur <sup>51</sup>				1,85		2,15		0,7		0			4,7

<sup>50</sup> Aufgrund ihres spezifischen operativen Charakters ist es nicht möglich, genaue Stückkosten je Ergebnis oder ein genaues erwartetes Volumen an Ergebnissen zu ermitteln, insbesondere da einige Ergebnisse mit Strafverfolgungsmaßnahmen zusammenhängen, die eine Reaktion auf unvorhersehbare kriminelle Aktivitäten sind.

<sup>51</sup> Einschließlich Hardware, Software, Netzeinrichtungen und Sicherheit.

- Ergebnis	Auftragnehmer <sup>52</sup>					1,4		0,7		0,7		0		2,8
- Ergebnis	Mechanismus für Mikroabgleiche					0,9		0,7		0		0		
- Ergebnis	Instandhaltung					0		0		1		1,2		2,2
<b>GESAMTKOSTEN</b>						4,15		3,55		2,4		1,2		11,3

<sup>52</sup> Einschließlich professioneller Dienstleistungen, Entwurfs- und Testkosten.

### 3.2.4 Geschätzte Auswirkungen auf die personellen Ressourcen von Europol

#### 3.2.4.1 Übersicht

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 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027	INSGES AMT
--	--------------	--------------	--------------	--------------	--------------	---------------

Bedienstete auf Zeit – Ausgangsbasis						
Bedienstete auf Zeit – zusätzlich zur Ausgangsbasis (kumuliert)	0	0,551	1,101	0,847	0,847	3,347
Bedienstete auf Zeit – INSGESAMT						
Vertragsbedienstete – Ausgangsbasis						
Abgeordnete nationale Sachverständige – Ausgangsbasis (Haushaltsentwurf 2021)						

<b>INSGESAMT – nur Mehrkosten</b>	0	0,551	1,101	0,847	0,847	3,347
<b>INSGESAMT – einschließlich Ausgangsbasis und Mehrkosten</b>						

Personalbedarf (VZÄ):

	Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027
Bedienstete auf Zeit – Ausgangsbasis	<b>0</b>	<b>9,5</b>	<b>9,5</b>	<b>21,5</b>	<b>19,5</b>
Bedienstete auf Zeit – zusätzlich zur Ausgangsbasis (kumuliert)	0	6,5	6,5	5	5
Bedienstete auf Zeit – INSGESAMT		<b>16</b>	<b>16</b>	<b>26,5</b>	<b>24,5</b>
Vertragsbedienstete					
Abgeordnete nationale Sachverständige					

<b>INSGESAMT</b>	<b>0</b>	<b>16,5</b>	<b>16,5</b>	<b>26,5</b>	<b>24,5</b>
------------------	----------	-------------	-------------	-------------	-------------

Die für die Umsetzung der Ziele dieses Vorschlags erforderlichen personellen Ressourcen wurden in Zusammenarbeit mit Europol geschätzt. Bei den Schätzungen wird der erwartete Anstieg der Arbeitsbelastung berücksichtigt, da die Interessenträger die Dienste von Europol im Laufe der Zeit stärker in Anspruch nehmen, sowie die Zeit, die Europol benötigt, um Ressourcen zu binden, um eine Situation zu vermeiden, in der die Agentur nicht in der Lage wäre, ihren EU-Beitrag vollständig auszuführen und die Mittelbindungen rechtzeitig vorzunehmen.

Die für die Umsetzung der Ziele dieses Vorschlags erforderlichen personellen Ressourcen werden zum Teil durch das vorhandene Personal bei Europol (Basisszenario) und zum Teil durch zusätzliche Ressourcen (zusätzliches Personal im Vergleich zum Basisszenario) abgedeckt.

Im Finanzbogen ist keine Aufstockung der Vertragsbediensteten vorgesehen.

Für die Umsetzung von Prüm II können die für Europol benötigten Ressourcen in drei Kategorien unterteilt werden:

1) IKT-Kosten für den Anschluss an den biometrischen Router bei eu-LISA, notwendige Entwicklungsarbeiten in den Europol-Informationssystemen, um Daten von Dritten für Abfragen aus den Mitgliedstaaten zugänglich zu machen und die Abfragen in Prüm mit den Daten von Dritten in die einheitliche Europol-Suchschnittstelle USE-UI zu integrieren,

2) Kosten für Personal in der Europol-Direktion „Operative Tätigkeiten“, das die Abrufe mit Daten von Dritten durchführt, und für Biometrieexperten, die die Überprüfung der Treffer vornehmen,

3) Hosting eines zentralen Routers für Kriminalakten. Dazu gehören einmalige Hardwarekosten (einschließlich verschiedener Produktions- und Testumgebungen für die Mitgliedstaaten), IKT-Personal für die Entwicklung und das Änderungsmanagement der ADEP.EPRIS-Software, Tests mit den Mitgliedstaaten und ein 24/7-Helpdesk zur Unterstützung der Mitgliedstaaten bei Problemen. Um eine umfassende Unterstützung der Mitgliedstaaten zu gewährleisten, müssen Mitarbeiter mit unterschiedlichen Profilen im IKT-Bereich zur Verfügung stehen, z. B. Mitarbeiter für die allgemeine Koordinierung, Anforderungsingenieure, Entwickler, Tester und Systemadministratoren. Im ersten Jahr nach der Inbetriebnahme wird noch ein etwas höherer Bedarf an IKT-Personal erwartet.

Aufgrund von Sicherheitsauflagen und der vereinbarten Obergrenze für Vertragsbedienstete müssen die meisten Aufgaben im Zusammenhang mit Prüm von Europol-Personal ausgeführt werden. Bestimmte weniger sensible Tätigkeiten sollen an Auftragnehmer ausgelagert werden (Tests, einige Entwicklungsaufgaben).

<b>Bedienstete auf Zeit in VZÄ (Ausgangsbasis zusätzliches Personal)</b>	<b>2023</b>	<b>2024</b>	<b>2025</b>	<b>2026</b>	<b>2027</b>
<b>Projektmanagement</b>		1,0	1,0	0,5	0,5
<b>Experten (insgesamt)</b>		14,5	14,5	18,0	16,0

• <i>Biometrie</i>		1,0	1,0	4,0	4,0
• <i>operative Tätigkeiten</i>		0,5	0,5	4,0	4,0
• <i>IKT</i>		13,0	13,0	10,0	8,0
<b>Helpdesk- Unterstützung/Überwachung</b>		0,0	0,0	7,0	7,0
<b>Allgemeine Koordinierung</b>		1,0	1,0	1,0	1,0
<b>Insgesamt</b>		<b>16,5</b>	<b>16,5</b>	<b>26,5</b>	<b>24,5</b>

### 3.2.5 Geschätzte Auswirkungen auf das Personal von eu-LISA

#### 3.2.5.1 Übersicht

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 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027	INSGES AMT
--	--------------	--------------	--------------	--------------	--------------	---------------

Bedienstete auf Zeit – Ausgangsbasis						
Bedienstete auf Zeit – zusätzlich zur Ausgangsbasis (kumuliert)		0,456	0,988	1,52	1,368	4,332
Bedienstete auf Zeit – INSGESAMT						
Vertragsbedienstete – Ausgangsbasis						
Vertragsbedienstete – Zusätzliche					0,082	0,082
Abgeordnete nationale Sachverständige – Ausgangsbasis (Haushaltsentwurf 2021) 53						

<b>INSGESAMT – nur Mehrkosten</b>		0,456	0,988	1,52	1,45	4,414
<b>INSGESAMT – einschließlich Ausgangsbasis und Mehrkosten</b>						

Personalbedarf (VZÄ):

	Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027
Bedienstete auf Zeit – Ausgangsbasis					

<sup>53</sup> Im Haushaltsentwurf 2021 angegebener Personalbestand, berechnet auf der Grundlage der durchschnittlichen Personaleinheitskosten, die für den Finanzbogen zu Rechtsakten zu verwenden sind. Für das Jahr, in dem Personal eingestellt wird, wird die Hälfte der entsprechenden jährlichen Mittel berechnet.

Bedienstete auf Zeit – zusätzlich zur Ausgangsbasis (kumuliert)		6	7	10	9
Bedienstete auf Zeit – INSGESAMT					
Vertragsbedienstete – Ausgangsbasis					
Vertragsbedienstete – zusätzlich					2
Abgeordnete nationale Sachverständige					
<b>INSGESAMT</b>		<b>6</b>	<b>7</b>	<b>10</b>	<b>11</b>

Die für die Umsetzung der Ziele des neuen Mandats erforderlichen personellen Ressourcen wurden in Zusammenarbeit mit eu-LISA geschätzt. Bei den Schätzungen wird der erwartete Anstieg der Arbeitsbelastung berücksichtigt, da die Interessenträger die Dienste von eu-LISA im Laufe der Zeit stärker in Anspruch nehmen, sowie die Zeit, die eu-LISA benötigt, um Ressourcen zu binden, um eine Situation zu vermeiden, in der die Agentur nicht in der Lage wäre, ihren EU-Beitrag vollständig auszuführen und die Mittelbindungen rechtzeitig vorzunehmen.

Diese Schätzungen basieren auf folgender Personalausstattung:

	<b>Phasentrennstellen</b>								
	Analyse und Entwurf			Aufbau und Entwicklung			Betrieb		
Vertragsart	Bedienstete auf Zeit	Vertragsbedienstete	Insgesamt	Bedienstete auf Zeit	Vertragsbedienstete	Insgesamt	Bedienstete auf Zeit	Vertragsbedienstete	Insgesamt
Profil	Zahl	Zahl		Zahl	Zahl		Zahl	Zahl	
<b>IT-Architekt</b>	1		1	1		1	1		1
<b>Testmanagement</b>	1		1	1		1	0,5		0,5
<b>Freigabe- und Veränderungsmanagement</b>			0	1		1	1		1
<b>Netzwerk-administrator</b>	1		1	1		1	1		1
<b>Sicherheitsmanagement</b>	2		2	2		2	2		2
<b>Mitarbeiter im First-Level-Support (24x7)</b>			0			0		1	1

<b>Mitarbeiter im Second-Level-Support (24x7)</b>			0				0		1	1
<b>Programm- und Projektmanagement</b>	1		1	1			1	0,5		0,5
<b>Produktinhaber</b>			0	1			1	1		1
<b>Biometrie-Experte</b>	1		1	1			1	1		1
<b>Systemadministrator/Infra</b>	1		1	1			1	1		1
<b>Insgesamt (Vertragsbedienstete + Bedienstete auf Zeit)</b>	<b>8</b>		<b>8</b>	<b>10</b>			<b>10</b>	<b>9</b>	<b>2</b>	<b>11</b>
	<b>Profile</b>		Jahr -1 (Vorbereitung & Entwurf)	Jahr 1	Jahr 2	Jahr 3	Jahr 4	Jahr 5		
	<b>IT-Architekt (Bedienstete auf Zeit)</b>		1	1	1	1	1	1		
	<b>Testmanagement</b>			1	1	0,5	0,5	0,5		

<b>(Bedienstete auf Zeit)</b>						
<b>Freigabe- und Veränderungsmanagement (Bedienstete auf Zeit)</b>			1	1	1	1
<b>Netzwerkadministrator (Bedienstete auf Zeit)</b>	1	1	1	1	1	1
<b>Sicherheitsmanagement (Bedienstete auf Zeit)</b>	1	1	2	2	2	2
<b>Mitarbeiter im First-Level-Support (24x7) – (Vertragsbedienstete)</b>				1	1	1
<b>Mitarbeiter im Second-Level-Support (24x7) – (Vertragsbedienstete)</b>				1	1	1
<b>Programm- und Projektmanagement (Bedienstete auf Zeit)</b>	1	1	1	0,5	0,5	0,5
<b>Produktinhaber (Bedienstete auf Zeit)</b>			1	1	1	1
<b>Biometrie-Experte (Bedienstete auf Zeit)</b>	1	1	1	1	1	1
<b>Systemadministrator/ Infrastruktur (Bedienstete)</b>	1	1	1	1	1	1

<b>auf Zeit)</b>						
<b>INSGESAMT</b>	<b>6</b>	<b>7</b>	<b>10</b>	<b>11</b>	<b>11</b>	<b>11</b>

### 3.2.5.2 Geschätzter Personalbedarf bei der Partner-GD

Für den Vorschlag/die Initiative werden keine Mittel für Personal benötigt.

Für den Vorschlag/die Initiative wird das folgende Personal benötigt:

*Schätzung in ganzzahligen Werten (oder mit höchstens einer Dezimalstelle)*

	Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027
<b>• Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit):</b>					
XX 01 01 01 (am Sitz und in den Vertretungen der Kommission)		5	5	4	4
XX 01 01 02 (in den Delegationen)					
XX 01 05 01 (indirekte Forschung)					
10 01 05 01 (direkte Forschung)					
<b>• Externes Personal (in Vollzeitäquivalenten: VZÄ)<sup>54</sup></b>					
XX 01 02 01 (VB, ANS und LAK der Globaldotation)					
XX 01 02 02 (VB, ÖB, ANS, LAK und JFD in den Delegationen)					
<b>XX 01 04 JJ<sup>55</sup></b>	- Am Sitz der Kommission <sup>56</sup>				
	- in den Delegationen				
XX 01 05 02 (VB, ANS und LAK der indirekten Forschung)					
10 01 05 02 (VB, ANS, LAK – direkte Forschung)					
Sonstige Haushaltslinien (bitte angeben)					
<b>INSGESAMT</b>		<b>5</b>	<b>5</b>	<b>4</b>	<b>4</b>

**XX** steht für den jeweiligen Politikbereich bzw. Haushaltstitel.

Der Personalbedarf wird teilweise (3 VZÄ) durch der Verwaltung der Maßnahme zugeordnetes Personal der GD und/oder GD-interne Personalumsetzung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die den für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der

<sup>54</sup> VB = Vertragsbedienstete, ÖB = örtliche Bedienstete, ANS = Abgeordnete nationale Sachverständige, LAK = Leiharbeitskräfte, JFD = Juniorfachkräfte in Delegationen.

<sup>55</sup> Teilobergrenze für aus operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

<sup>56</sup> Insbesondere für die Strukturfonds, den Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) und den Europäischen Fischereifonds (EFF).

jährlichen Mittelzuweisung zugeteilt werden. Die GD benötigt außerdem zusätzliches Personal (2 VZÄ).

Beschreibung der auszuführenden Aufgaben:

Fünf 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, die Bewertung der Fortschritte der Mitgliedstaaten, Aktualisierung des abgeleiteten Rechts, einschließlich aller Entwicklungen im Zusammenhang mit den Normen. Da es sich bei dem Programm um eine zusätzliche Maßnahme zur bestehenden Arbeitsbelastung handelt, ist zusätzliches Personal erforderlich (2 VZÄ). Eine der Personalaufstockungen ist zeitlich begrenzt und deckt nur den Entwicklungszeitraum ab, die zweite betrifft die Übernahme der Aufgaben des Generalsekretariats des Rates. Da die Beschlüsse des Rates in eine Verordnung umgewandelt werden, muss die Kommission die Aufgaben des Generalsekretariats des Rates übernehmen, dessen Arbeitsvolumen 1 VZÄ beträgt.

### 3.2.6 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.

- Der Vorschlag/Die Initiative erfordert eine Inanspruchnahme des Flexibilitätsinstruments oder eine Änderung des Mehrjährigen Finanzrahmens.<sup>57</sup>

Bitte erläutern Sie den Bedarf unter Angabe der betreffenden Rubriken und Haushaltslinien sowie der entsprechenden Beträge.

[...]

### 3.2.7 Finanzierungsbeteiligung Dritter

Der Vorschlag/Die Initiative sieht keine Kofinanzierung durch Dritte vor.

Der Vorschlag/die Initiative sieht folgende Kofinanzierung durch Dritte vor:

in Mio. EUR (3 Dezimalstellen)

	Jahr N	Jahr N+1	Jahr N+2	Jahr N+3	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen			Insgesamt
Kofinanzierende Einrichtung								
Kofinanzierung INSGESAMT								

<sup>57</sup> Siehe Artikel 11 und 17 der Verordnung (EU, Euratom) Nr. 1311/2013 des Rates zur Festlegung des Mehrjährigen Finanzrahmens für die Jahre 2014–2020.

### 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 übrigen Einnahmen
- Bitte geben Sie an, ob die Einnahmen bestimmten Ausgabenlinien zugewiesen sind.

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Für das laufende Haushaltsjahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative <sup>58</sup>					Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen		
		Jahr N	Jahr N+1	Jahr N+2	Jahr N+3				
Artikel .....									

Bitte geben Sie für die sonstigen zweckgebundenen Einnahmen die betreffende(n) Ausgabenlinie(n) im Haushaltsplan an.

[...]

Bitte geben Sie an, wie die Auswirkungen auf die Einnahmen berechnet werden.

[...]

<sup>58</sup> Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d. h. abzüglich 20 % für Erhebungskosten, anzugeben.

**ANHANG 5**

**des  
BESCHLUSSES DER KOMMISSION**

**über die Internen Vorschriften für die Ausführung des Gesamthaushaltsplans der Europäischen Union (Einzelplan Kommission), gerichtet an die Dienststellen der Kommission**

**ANHANG  
des FINANZBOGENS ZU RECHTSAKTEN**



# ANHANG des FINANZBOGENS ZU RECHTSAKTEN

## Bezeichnung des Vorschlags

Vorschlag zum automatisierten Datenaustausch für die polizeiliche Zusammenarbeit („Prüm II“), zur Änderung der Verordnung (EU) 2018/1726, der Verordnung (EU) 2019/817 und der Verordnung (EU) 2019/818 sowie zur Aufhebung der Beschlüsse 2008/615/JI und 2008/616/JI des Rates

1. **VORAUSSICHTLICHER BEDARF AN PERSONAL UND MITTEL HIERFÜR**
2. **SONSTIGE VERWALTUNGSAusGABEN**
3. **VERWALTUNGSKOSTEN INSGESAMT**
4. **KOSTENSCHÄTZUNGSMETHODEN**
  - 4.1. **Personalausgaben**
  - 4.2. **Sonstige Verwaltungsausgaben**

*Bei der Einleitung der dienststellenübergreifenden Konsultation ist dieser Anhang dem Finanzbogen zu Rechtsakten beizulegen.*

*Die in diesen Tabellen enthaltenen Daten fließen in die Tabellen des Finanzbogens zu Rechtsakten ein. Die Tabellen sind als interne Dokumente ausschließlich für den Dienstgebrauch der Kommission bestimmt.*

(1) Voraussichtlicher Personalbedarf und Mittel hierfür

- Für den Vorschlag/die Initiative werden keine Mittel für Personal benötigt.  
 Für den Vorschlag/die Initiative wird das folgende Personal benötigt:

in Mio. EUR (3 Dezimalstellen)

RUBRIK 7 des Mehrjährigen Finanzrahmens	2024		2025		2026		2027								INSGESAMT		
	VZÄ	Mittelzuweisungen	VZÄ	Mittelzuweisungen	VZÄ	Mittelzuweisungen	VZÄ	Mittelzuweisungen	VZÄ	Mittelzuweisungen	VZÄ	Mittelzuweisungen	VZÄ	Mittelzuweisungen	VZÄ	Mittelzuweisungen	
• Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit)																	
20 01 02 01 – Hauptsitz und Vertretungen	AD	5	0,608	5	0,684	4	0,608	4	0,608							4	2,508
	AST																
20 01 02 03 – Delegationen der Union	AD																
	AST																
• Externes Personal <sup>59</sup>																	

<sup>59</sup> VB = Vertragsbedienstete, ÖB = örtliche Bedienstete, ANS = Abgeordnete nationale Sachverständige, LAK = Leiharbeitskräfte, JFD = Juniorfachkräfte in Delegationen.

20 02 01 und 20 02 02 – Externes Personal – Hauptsitz und Vertretungen	VB																
	ANS																
	LAK																
20 02 03 – Externes Personal – Delegationen der Union	VB																
	OB																
	ANS																
	LAK																
	JFD																
Sonstige personalbezogene Haushaltslinien (bitte angeben)																	
<b>Zwischensumme Personal – RUBRIK 7</b>		5	0,608	5	0,684	4	0,608	4	0,608							4	2,508

Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD und/oder GD-interne Personalumsetzung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die den für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD und/oder GD-interne Personalumsetzung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die den für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

(2) Sonstige Verwaltungsausgaben

- Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt.  
 Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

RUBRIK 7 des Mehrjährigen Finanzrahmens	2024	2025	2026	2027				Insgesamt
<b>Am Sitz der Kommission oder im Gebiet der Union:</b>								
20 02 06 01 – Dienstreisen und Repräsentationszwecke	0,035	0,035	0,035	0,035				0,140
20 02 06 02 – Konferenzen und Sitzungen	0,125	0,125	0,125	0,125				0,500
20 02 06 03 – Ausschüsse (Ausschuss Prüm II) <sup>60</sup>	0,065	0,065	0,026	0,026				0,182
20 02 06 04 – Untersuchungen und Konsultationen								
20 04 – IT-Ausgaben (intern) <sup>61</sup>								
Sonstige nicht personalbezogene Haushaltslinien ( <i>ggf. bitte angeben</i> )								
<b>In den Delegationen der Union:</b>								
20 02 07 01 – Dienstreise- und Repräsentationskosten, Ausgaben für Konferenzen								

<sup>60</sup> Prüm-II-Ausschuss, ca. 10 Sitzungen pro Jahr in den Jahren 2024 und 2025 und 4 Sitzungen pro Jahr danach, wobei nur die Hälfte der Sitzungen in den Kosten berücksichtigt wird (die andere Hälfte findet in Form von Videokonferenzen statt).

<sup>61</sup> Stellungnahme der GD DIGIT – Team „IT-Investitionen“ erforderlich (siehe Leitlinien zur Finanzierung von Informationstechnologie, C(2020) 6126 final vom 10.9.2020, S. 7).

20 02 07 02 – Berufliche Fortbildung des Personals								
20 03 05 – Infrastruktur und Logistik								
Sonstige nicht personalbezogene Haushaltslinien ( <i>ggf. bitte angeben</i> )								
<b>Zwischensumme Sonstiges – RUBRIK 7 des Mehrjährigen Finanzrahmens</b>	0,225	0,225	0,186	0,186				<b>0,822</b>

*in Mio. EUR (3 Dezimalstellen)*

<b>Außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens</b>	<b>2024</b>	<b>2025</b>	<b>2026</b>	<b>2027</b>				<b>Insgesamt</b>
Aus operativen Mitteln finanzierte technische und administrative Unterstützung <u>ohne</u> externes Personal (vormalige BA-Linien)								
- am Sitz der Kommission								
- in den Delegationen der Union								
Sonstige Verwaltungsausgaben für die Forschung								
IT-Ausgaben zur Politikunterstützung für operationelle Programme <sup>62</sup>								

<sup>62</sup> Stellungnahme der GD DIGIT – Team „IT-Investitionen“ erforderlich (siehe Leitlinien zur Finanzierung von Informationstechnologie, C(2020) 6126 final vom 10.9.2020, S. 7).

Interne IT-Ausgaben für operationelle Programme <sup>63</sup>								
Sonstige nicht personalbezogene Haushaltslinien ( <i>ggf. bitte angeben</i> )								
<b>Zwischensumme Sonstiges – Außerhalb der RUBRIK 7</b> des Mehrjährigen Finanzrahmens								
<b>Sonstige Verwaltungsausgaben insgesamt (alle MFR-Rubriken)</b>	0,225	0,225	0,186	0,186				0,822

<sup>63</sup> Hierunter fallen lokale Verwaltungssysteme und Beiträge zur Kofinanzierung interner IT-Systeme (siehe Leitlinien zur Finanzierung von Informationstechnologie, C(2020) 6126 final vom 10.9.2020).

(3) Verwaltungskosten insgesamt (alle MFR-Rubriken)

*in Mio. EUR (3 Dezimalstellen)*

Übersicht	2024	2025	2026	2027				Insgesamt
Rubrik 7 – Personalausgaben	0,608	0,684	0,608	0,608				2,508
Rubrik 7 – Sonstige Verwaltungsausgaben	0,225	0,225	0,186	0,186				0,822
<b>Zwischensumme Rubrik 7</b>								
Außerhalb der Rubrik 7 – Personalausgaben								
Außerhalb der Rubrik 7 – Sonstige Verwaltungsausgaben								
<b>Zwischensumme Sonstige Rubriken</b>								
<b>INSGESAMT RUBRIK 7 und Außerhalb der RUBRIK 7</b>	0,833	0,833	0,794	0,794				3,330

Der Bedarf an Verwaltungsmitteln wird aus den Mitteln gedeckt, die für die Verwaltung der Maßnahme bereits zugewiesen wurden bzw. ggf. neu zugewiesen werden. 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.

#### 4. KOSTENSCHÄTZUNGSMETHODEN

##### 4.1. Personalausgaben

*In diesem Teil ist zu erläutern, nach welcher Methode der geschätzte Personalbedarf berechnet wird (Annahmen hinsichtlich des Arbeitsaufwands mit Angabe der genauen Funktionsbezeichnungen (Arbeitsprofile nach Sysper 2), der Personalkategorie und entsprechender Durchschnittskosten)*

#### RUBRIK 7 des Mehrjährigen Finanzrahmens

Anmerkung: Für die am Sitz der Kommission tätigen Personalkategorien sind die Durchschnittskosten unter folgender Adresse abrufbar (BudgWeb):

[https://myintracomm.ec.europa.eu/budgweb/DE/pre/legalbasis/Pages/pre-040-020\\_preparation.aspx](https://myintracomm.ec.europa.eu/budgweb/DE/pre/legalbasis/Pages/pre-040-020_preparation.aspx)

Beamte und Zeitbedienstete:

Gemäß dem Rundschreiben der GD HAUSHALT an den RUF/2020/23 vom 30.11.2020 (siehe Anhang 1, Ares(2020)7207955 vom 30.11.2020) belaufen sich die Kosten für einen Beamten der Funktionsgruppe AD auf 152 000 EUR pro Jahr. Die Hälfte der entsprechenden jährlichen Mittel wird für das Jahr berechnet, in dem das Personal eingestellt wird und aus dem es ausscheidet.

Der Personalbedarf wird teilweise (3 VZÄ) durch der Verwaltung der Maßnahme zugeordnetes Personal der GD und/oder GD-interne Personalumsetzung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die den für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden. Die GD benötigt außerdem zusätzliches Personal (2 VZÄ).

Beschreibung der auszuführenden Aufgaben:

Fünf 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, die Bewertung der Fortschritte der Mitgliedstaaten, Aktualisierung des abgeleiteten Rechts, einschließlich aller Entwicklungen im Zusammenhang mit den Normen. Da es sich bei dem Programm um eine zusätzliche Maßnahme zur bestehenden Arbeitsbelastung handelt, ist zusätzliches Personal erforderlich (2 VZÄ). Eine der Personalaufstockungen ist zeitlich begrenzt und deckt nur den Entwicklungszeitraum ab, die zweite betrifft die Übernahme der Aufgaben des Generalsekretariats des Rates. Da die Beschlüsse des Rates in eine Verordnung umgewandelt werden, muss die Kommission die Aufgaben des Generalsekretariats des Rates übernehmen, dessen Arbeitsvolumen 1 VZÄ beträgt.

- Externes Personal

#### Außerhalb RUBRIK 7 des Mehrjährigen Finanzrahmens

- Nur für aus dem Forschungshaushalt finanzierte Stellen

- Externes Personal

## 4.2. Sonstige Verwaltungsausgaben

*Für jede Haushaltlinie ist die verwendete Berechnungsmethode darzulegen, insbesondere die zugrunde gelegten Annahmen (z. B. Anzahl der Sitzungen pro Jahr, Durchschnittskosten usw.)*

### RUBRIK 7 des Mehrjährigen Finanzrahmens

Schätzungsweise werden durchschnittlich 35 Dienstreisen pro Jahr stattfinden, einschließlich der Dienstreisen zu den satzungsgemäßen Sitzungen (Beratende Gruppe, Arbeitsgruppen von eu-LISA und Europol sowie Sitzungen im Zusammenhang mit dem EPRIS und Eucaris), sowie zur Teilnahme an Prüm-bezogenen Sitzungen und Konferenzen. Die Einheitskosten pro Dienstreise werden auf der Grundlage berechnet, dass ein Beamter durchschnittlich 2 Tage pro Dienstreise reist, und auf 500 EUR pro Dienstreise und Tag festgesetzt.

Die Einheitskosten pro Expertensitzung/Konferenz werden auf 25 000 EUR für 50 Teilnehmer festgesetzt. Es werden voraussichtlich 5 Sitzungen pro Jahr organisiert werden.

Die Einheitskosten pro Ausschuss werden auf 13 000 EUR für 26 Teilnehmer festgelegt, wobei von der Erstattung eines Teilnehmers pro Mitgliedstaat für eine eintägige Dienstreise zur Teilnahme an der Sitzung des Ausschusses ausgegangen wird. Es werden voraussichtlich 10 Sitzungen pro Jahr in den Jahren 2024 und 2025 (5 physische Sitzungen und 5 Videokonferenzen) und 4 Sitzungen pro Jahr ab 2026 (2 physische Sitzungen und 2 Videokonferenzen) organisiert werden.

### Außerhalb RUBRIK 7 des Mehrjährigen Finanzrahmens