



EUROPÄISCHE UNION

DAS EUROPÄISCHE PARLAMENT

DER RAT

Brüssel, den 14. Februar 2024
(OR. en)

2021/0410 (COD)

PE-CONS 75/23

IXIM 237
ENFOPOL 525
JAI 1599
CODEC 2358

GESETZGEBUNGSAKTE UND ANDERE RECHTSINSTRUMENTE

Betr.: VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die automatisierte Abfrage und den Austausch von Daten für die polizeiliche Zusammenarbeit und 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 (Prüm-II-Verordnung)

VERORDNUNG (EU) 2024/...
DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom ...

**über die automatisierte Abfrage und den Austausch
von Daten für die polizeiliche Zusammenarbeit
und 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
(Prüm-II-Verordnung)**

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 Sozialausschusses¹,

gemäß dem ordentlichen Gesetzgebungsverfahren²,

¹ ABl. C 323 vom 26.8.2022, S. 69.

² Standpunkt des Europäischen Parlaments vom 8. Februar 2024 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom

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 soll unter anderem mittels geeigneter Maßnahmen zur Verhütung und Bekämpfung von Kriminalität und anderen Bedrohungen der öffentlichen Sicherheit, einschließlich der organisierten Kriminalität und des Terrorismus, im Einklang mit der Mitteilung der Kommission vom 24. Juli 2020 mit dem Titel „EU-Strategie für eine Sicherheitsunion“ erreicht werden. Dieses Ziel setzt voraus, dass die Strafverfolgungsbehörden Daten effizient und zeitnah austauschen, um Straftaten wirksam zu verhüten, aufzudecken und zu untersuchen.
- (2) Ziel dieser Verordnung ist es, den Austausch von kriminalpolizeilichen Informationen und Fahrzeugzulassungsdaten zwischen den zuständigen Behörden der Mitgliedstaaten zum Zwecke der Verhütung, Aufdeckung und Untersuchung von Straftaten und zwischen den Mitgliedstaaten und der durch die Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates³ errichteten Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) unter uneingeschränkter Wahrung der Grundrechte und der Datenschutzbestimmungen zu verbessern, zu optimieren und zu erleichtern .

³ 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).

(3) Die Beschlüsse 2008/615/JI⁴ und 2008/616/JI⁵ des Rates, in denen die Vorschriften für den Informationsaustausch zwischen den für die Verhütung und Untersuchung von Straftaten zuständigen Behörden durch die automatisierte Übermittlung von DNA-Profilen, daktyloskopischen Daten und bestimmten Fahrzeugzulassungsdaten festgelegt sind, haben sich für die Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität als wichtig erwiesen, wodurch die innere Sicherheit der Union und die Sicherheit ihrer Bürgerinnen und Bürger geschützt werden.

⁴ 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).

⁵ 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).

(4) Aufbauend auf bestehenden Verfahren für die automatisierte Abfrage von Daten werden in dieser Verordnung die Bedingungen und Verfahren für das automatisierte Abfragen und Austauschen von DNA-Profilen, daktyloskopischen Daten, Fahrzeugzulassungsdaten, Gesichtsbildern und Polizeiakten festgelegt. Dies sollte die Verarbeitung dieser Daten im Schengener Informationssystem (SIS), den Austausch damit verbundener Zusatzinformationen zu diesen Daten über die SIRENE-Büros gemäß der Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates⁶ sowie die Rechte von Personen, deren Daten in diesem System verarbeitet werden, unberührt lassen.

⁶ 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).

- (5) Mit dieser Verordnung wird ein Rahmen für den Informationsaustausch zwischen den für die Verhütung, Aufdeckung und Untersuchung von Straftaten zuständigen Behörden geschaffen (im Folgenden „Prüm-II-Rahmen“). Im Einklang mit Artikel 87 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) deckt sie alle zuständigen Behörden der Mitgliedstaaten ab, einschließlich, aber nicht beschränkt auf Polizei, Zoll und andere spezialisierte Strafverfolgungsbehörden im Zusammenhang mit der Verhütung, Aufdeckung und Untersuchung von Straftaten. Daher sollte im Zusammenhang mit dieser Verordnung jede Behörde, die für die Verwaltung einer unter diese Verordnung fallenden nationalen Datenbank zuständig ist oder die eine justizielle Genehmigung zur Freigabe von Daten erteilt, als in den Anwendungsbereich dieser Verordnung fallend betrachtet werden, solange die Informationen zur Verhütung, Aufdeckung und Untersuchung von Straftaten ausgetauscht werden.
- (6) Keine Verarbeitung und kein Austausch personenbezogener Daten für die Zwecke dieser Verordnung sollte zu einer Diskriminierung von Personen aus egal welchen Gründen führen. Die Würde und Integrität des Menschen 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) Jede Verarbeitung und jeder Austausch personenbezogener Daten sollte den Datenschutzvorschriften des Kapitels 6 dieser Verordnung und sofern anwendbar der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates⁷ oder den Verordnungen (EU) 2018/1725⁸, (EU) 2016/794 oder (EU) 2016/679⁹ des Europäischen Parlaments und des Rates unterliegen. Die Richtlinie (EU) 2016/680 gilt für die Verwendung des Prüm-II-Rahmens bei der Abfrage nach vermissten Personen und die Identifizierung nicht identifizierter menschlicher Überreste zur Verhütung, Aufdeckung und Untersuchung von Straftaten. Die Verordnung (EU) 2016/679 gilt für die Verwendung des Prüm-II-Rahmens bei der Abfrage nach vermissten Personen und die Identifizierung nicht identifizierter menschlicher Überreste für andere Zwecke.

⁷ 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).

⁸ 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).

⁹ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

- (8) Da diese Verordnung die automatisierte Abfrage von DNA-Profilen, daktyloskopischen Daten, bestimmten Fahrzeugzulassungsdaten, Gesichtsbildern und Polizeiakten vorsieht, besteht ihr Zweck auch darin, die Abfrage nach vermissten Personen und die Identifizierung nicht identifizierter menschlicher Überreste zu ermöglichen. Diese automatisierten Abfragen sollten nach den in dieser Verordnung festgelegten Regeln und Verfahren erfolgen. Diese automatisierten Abfragen lassen die Eingabe von Ausschreibungen von vermissten Personen in das SIS und den Austausch von Zusatzinformationen zu solchen Ausschreibungen gemäß der Verordnung (EU) 2018/1862 unberührt.
- (9) Wenn Mitgliedstaaten den Prüm-II-Rahmen zur Abfrage nach vermissten Personen und zur Identifizierung menschlicher Überreste verwenden wollen, sollten sie nationale Rechtsvorschriften erlassen, in denen die für diesen Zweck zuständigen nationalen Behörden benannt und die spezifischen Verfahren, Bedingungen und Kriterien für diesen Zweck festgelegt werden. Für die Abfrage nach vermissten Personen außerhalb des Bereichs strafrechtlicher Ermittlungen sollten die humanitären Gründe, aus denen eine Abfrage nach vermissten Personen durchgeführt werden kann, in den nationalen Legislativmaßnahmen eindeutig festgelegt werden. Diese Suchen sollten dem Grundsatz der Verhältnismäßigkeit entsprechen. Die humanitären Gründe sollten Naturkatastrophen und vom Menschen verursachte Katastrophen sowie andere gleichermaßen gerechtfertigte Gründe wie den Verdacht auf Selbstmord einschließen.

- (10) In dieser Verordnung werden die Bedingungen und Verfahren für die automatisierte Abfrage von DNA-Profilen, daktyloskopischen Daten, bestimmten Fahrzeugzulassungsdaten, Gesichtsbildern und Polizeiakten sowie die Vorschriften für den Austausch von Kerndaten nach einer bestätigten Übereinstimmung biometrischer Daten festgelegt. Sie gilt nicht für den über die Bestimmungen dieser Verordnung hinausgehenden Austausch zusätzlicher Informationen, der durch die Richtlinie (EU) 2023/977 des Europäischen Parlaments und des Rates¹⁰ geregelt wird.
- (11) Die Richtlinie (EU) 2023/977 bietet einen kohärenten Rechtsrahmen der Union, der dafür sorgt, dass die zuständigen Behörden eines Mitgliedstaats einen gleichwertigen Zugang zu Informationen anderer Mitgliedstaaten haben, wenn sie diese Informationen zur Bekämpfung von Kriminalität und Terrorismus benötigen. Zur Verbesserung des Informationsaustauschs formalisiert und präzisiert die genannte Richtlinie die Regeln und Verfahren für den Informationsaustausch zwischen den zuständigen Behörden der Mitgliedstaaten, insbesondere zu Ermittlungszwecken, einschließlich der Rolle der „zentralen Kontaktstelle“ jedes Mitgliedstaats für diesen Austausch.
- (12) Die Zwecke des Austauschs von DNA-Profilen im Rahmen dieser Verordnung lassen die ausschließliche Zuständigkeit der Mitgliedstaaten für die Entscheidung über den Zweck ihrer nationalen DNA-Datenbanken, einschließlich der Verhütung oder Aufdeckung von Straftaten, unberührt.

¹⁰ Richtlinie (EU) 2023/977 des Europäischen Parlaments und des Rates vom 10. Mai 2023 über den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten und zur Aufhebung des Rahmenbeschlusses 2006/960/JI des Rates (ABl. L 134 vom 22.5.2023, S. 1).

- (13) Die Mitgliedstaaten sollten zum Zeitpunkt der ersten Verbindung mit dem durch diese Verordnung eingerichteten Router automatisierte Abfragen von DNA-Profilen durchführen, indem sie alle in ihren Datenbanken gespeicherten DNA-Profile mit den in den Datenbanken aller anderen Mitgliedstaaten und den in den Europol-Daten gespeicherten DNA-Profilen abgleichen. Zweck dieser ersten automatisierten Abfrage ist es, Lücken bei der Ermittlung von Übereinstimmungen zwischen den in der Datenbank eines Mitgliedstaats gespeicherten DNA-Profilen und den in den Datenbanken aller anderen Mitgliedstaaten und in den Europol-Daten gespeicherten DNA-Profilen zu vermeiden. Die erste automatisierte Abfrage sollte bilateral erfolgen und nicht unbedingt mit den Datenbanken aller anderen Mitgliedstaaten und den Europol-Daten gleichzeitig durchgeführt werden. Die Modalitäten für die Durchführung dieser Abfragen, einschließlich des Zeitplans und der Menge je Charge, sollten bilateral und im Einklang mit den in dieser Verordnung festgelegten Regeln und Verfahren vereinbart werden.
- (14) Nach der ersten automatisierten Abfrage von DNA-Profilen sollten die Mitgliedstaaten automatisierte Abfragen durchführen, indem sie alle neu in die Datenbanken aufgenommenen DNA-Profile mit allen in den Datenbanken der anderen Mitgliedstaaten und von Europol gespeicherten DNA-Profilen abgleichen. Diese automatisierte Abfrage neuer DNA-Profile sollte regelmäßig durchgeführt werden. Können diese Abfragen nicht durchgeführt werden, sollte der betreffende Mitgliedstaat diese zu einem späteren Zeitpunkt durchführen können, um sicherzustellen, dass Übereinstimmungen nicht übersehen wurden. Die Modalitäten für die Durchführung dieser späteren Abfragen, einschließlich des Zeitplans und der Menge je Charge, sollten bilateral und im Einklang mit den in dieser Verordnung festgelegten Regeln und Verfahren vereinbart werden.

- (15) Für die automatisierte Abfrage von Fahrzeugzulassungsdaten sollten die Mitgliedstaaten und Europol 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 und alle teilnehmenden Mitgliedstaaten in einem Netzwerk miteinander verbindet. Für die Herstellung der Kommunikation ist keine zentrale Komponente erforderlich, da jeder Mitgliedstaat direkt mit den anderen angeschlossenen Mitgliedstaaten kommuniziert und Europol direkt mit den verbundenen Datenbanken kommuniziert.
- (16) Die Identifizierung von Straftätern ist für eine erfolgreiche strafrechtliche Ermittlung und Strafverfolgung von entscheidender Bedeutung. Die automatisierte Abfrage von nach nationalem Recht erfassten Gesichtsbildern von Personen, die der Begehung einer Straftat verdächtigt werden oder wegen einer Straftat verurteilt wurden, oder – sofern dies nach dem nationalen Recht des ersuchten Mitgliedstaats zulässig ist – von Opfern, die im Einklang mit dem nationalen Recht erhoben wurden, könnte zusätzliche Informationen für die erfolgreiche Identifizierung von Straftätern und Bekämpfung von Kriminalität liefern. Angesichts der Sensibilität der betreffenden Daten sollte es nur möglich sein, automatisierte Abfragen zum Zwecke der Verhütung, Aufdeckung oder Untersuchung einer Straftat durchzuführen, die nach dem Recht des ersuchenden Mitgliedstaats mit einer Freiheitsstrafe im Höchstmaß von mindestens einem Jahr bedroht ist.
- (17) Die automatisierte Abfrage biometrischer Daten durch für die Verhütung, Aufdeckung und Untersuchung von Straftaten zuständige Behörden der Mitgliedstaaten gemäß dieser Verordnung sollte nur Daten betreffen, die in für die Verhütung, Aufdeckung und Untersuchung von Straftaten eingerichteten Datenbanken enthalten sind.

(18) Die Beteiligung an der automatisierten Abfrage und dem Austausch von Polizeiakten sollte freiwillig bleiben. Wenn sich Mitgliedstaaten für eine Teilnahme entscheiden, sollte es ihnen gemäß dem Grundsatz der Gegenseitigkeit nur möglich sein, die Datenbanken anderer Mitgliedstaaten abzufragen, wenn sie ihre eigenen Datenbanken ebenso für Abfragen anderer Mitgliedstaaten verfügbar machen. Die teilnehmenden Mitgliedstaaten sollten die nationalen Polizeiaktennachweise erstellen. Die Mitgliedstaaten sollten entscheiden, welche nationalen Datenbanken, die zur Verhütung, Aufdeckung und Untersuchung von Straftaten eingerichtet wurden, sie zur Erstellung ihrer nationalen Polizeiaktennachweise nutzen werden. Diese Nachweise umfassen Daten aus nationalen Datenbanken, die üblicherweise von der Polizei geprüft werden, wenn sie Auskunftsersuchen von anderen Strafverfolgungsbehörden erhält. Mit dieser Verordnung wird das Europäische Polizeiaktennachweissystem (EPRIS) im Einklang mit dem Grundsatz des „Datenschutzes durch Technikgestaltung“ eingerichtet. Zu den Sicherheitsvorkehrungen für den Datenschutz gehört die Pseudonymisierung, da Nachweise und Abfragen keine Klarpersonalien enthalten, sondern alphanumerische Zeichenfolgen. Es ist wichtig, dass das EPRIS die Mitgliedstaaten oder Europol daran hindert, die Pseudonymisierung rückgängig zu machen und die identifizierenden Daten, die zu der Übereinstimmung geführt haben, offenzulegen. Angesichts der Sensibilität der betreffenden Daten sollte der Austausch von nationalen Polizeiaktennachweisen im Rahmen dieser Verordnung nur die Daten von Personen betreffen, die wegen einer Straftat verurteilt wurden oder einer solchen Straftat verdächtigt werden. Darüber hinaus sollte es nur möglich sein, automatisierte Abfragen von nationalen Polizeiaktennachweisen zum Zwecke der Verhütung, Aufdeckung und Untersuchung einer Straftat durchzuführen, die nach dem Recht des ersuchenden Mitgliedstaats mit einer Freiheitsstrafe im Höchstmaß von mindestens einem Jahr bedroht ist.

- (19) Der Austausch von Polizeiakten nach dieser Verordnung berührt nicht den Austausch von Strafregisterinformationen im Rahmen des bestehenden durch den Rahmenbeschlusses 2009/315/JI des Rates¹¹ eingerichteten Europäischen Strafregisterinformationssystems (ECRIS).
- (20) In den letzten Jahren hat Europol von Behörden aus Drittländern gemäß der Verordnung (EU) 2016/794 eine große Menge biometrischer Daten von Verdächtigen und Personen, die wegen Terrorismus und Straftaten verurteilt wurden, erhalten, einschließlich Gefechtsfeldinformationen aus Kriegsgebieten. In vielen Fällen konnten diese Daten nicht in vollem Umfang genutzt werden, da sie den zuständigen Behörden der Mitgliedstaaten nicht immer zur Verfügung stehen. Die Aufnahme der von Europol gespeicherten Daten aus Drittländern in den Prüm-II-Rahmen und somit die Bereitstellung dieser Daten für die zuständigen Behörden der Mitgliedstaaten entsprechend der Rolle Europols als zentrale Plattform der Union für kriminalpolizeiliche Informationen ist erforderlich, um schwere Straftaten besser zu verhüten, aufzudecken und zu untersuchen. Zudem trägt sie dazu bei, Synergien zwischen verschiedenen Strafverfolgungsinstrumenten zu schaffen, und stellt sicher, dass die Daten möglichst effizient genutzt werden.

¹¹ Rahmenbeschluss 2009/315/JI des Rates vom 26. Februar 2009 über die Durchführung und den Inhalt des Austauschs von Informationen aus dem Strafregister zwischen den Mitgliedstaaten (ABl. L 93 vom 7.4.2009, S. 23).

- (21) Europol sollte die Datenbanken der Mitgliedstaaten gemäß dem Prüm-II-Rahmen anhand von von Drittlandsbehörden erhaltenen Daten unter vollständiger Einhaltung der in der Verordnung (EU) 2016/794 vorgesehenen Vorschriften und Bedingungen abfragen können, um grenzüberschreitende Verbindungen zwischen Strafsachen herzustellen, für die Europol zuständig ist. Die Möglichkeit, neben anderen Europol zur Verfügung stehenden Datenbanken auch Prüm-Daten nutzen zu können, würde eine vollständigere und fundiertere Analyse ermöglichen, sodass Europol die zuständigen Behörden bei der Verhütung, Aufdeckung und Untersuchung von Straftaten besser unterstützen kann.
- (22) Europol sollte sicherstellen, dass seine Abfrageersuchen die von den Mitgliedstaaten festgelegten Abfragekapazitäten für daktyloskopische Daten und Gesichtsbilder nicht überschreiten. Bei Übereinstimmungen zwischen den für die Abfrage verwendeten Daten und in den Datenbanken der Mitgliedstaaten gespeicherten Daten sollten die Mitgliedstaaten entscheiden können, ob sie Europol die zur Erfüllung seiner Aufgaben erforderlichen Informationen zur Verfügung stellen.
- (23) Die Verordnung (EU) 2016/794 gilt in ihrer Gesamtheit für die Beteiligung von Europol am Prüm-II-Rahmen. Jede Verwendung von Daten aus Drittstaaten durch Europol ist in Artikel 19 der Verordnung (EU) 2016/794 geregelt. Jede Verwendung von Daten, die bei automatisierten Abfragen im Prüm-II-Rahmen gewonnen wurden, durch Europol sollte vorbehaltlich der Zustimmung des Mitgliedstaats, der die Daten bereitgestellt hat, und gemäß Artikel 25 der Verordnung (EU) 2016/794 erfolgen, wenn die Daten an Drittstaaten übermittelt werden.

- (24) Die Beschlüsse 2008/615/JI und 2008/616/JI des Rates sehen ein Netzwerk bilateraler Verbindungen zwischen den nationalen Datenbanken der Mitgliedstaaten vor. Infolge dieser technischen Architektur musste jeder Mitgliedstaat eine Verbindung zu jedem am automatisierten Austausch teilnehmenden Mitgliedstaat, d. h. mindestens 26 Verbindungen pro Mitgliedstaat je Datenkategorie, herstellen. Der Router und das EPRIS werden 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 vorschreiben. Das EPRIS sollte eine einzige Verbindung je teilnehmenden Mitgliedstaat in Bezug auf Polizeiakten vorschreiben.

(25) Der Router sollte mit dem durch die Verordnungen (EU) 2019/817¹² und (EU) 2019/818¹³ des Europäischen Parlaments und des Rates eingerichteten Europäischen Suchportal verbunden sein, damit die zuständigen Behörden der Mitgliedstaaten und Europol zu Gefahrenabwehr- und Strafverfolgungszwecken im Einklang mit diesen Verordnungen Abfragen in nationalen Datenbanken gemäß der vorliegenden Verordnung gleichzeitig mit Abfragen in dem mit den genannten Verordnungen eingerichteten gemeinsamen Speicher für Identitätsdaten durchführen können. Daher sollten die genannten Verordnungen entsprechend geändert werden. Die Verordnung (EU) 2019/818 sollte darüber hinaus geändert werden, damit Berichte und Statistiken des Routers im zentralen Speicher für Berichte und Statistiken gespeichert werden können.

¹² 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 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).

¹³ 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).

- (26) Es sollte möglich sein, dass die Referenznummern biometrischer Daten eine vorläufige Referenznummer oder eine Transaktions-Kontrollnummer sind.
- (27) Automatisierte daktyloskopische Identifizierungssysteme und Gesichtsbilderkennungssysteme verwenden biometrische Templates, die aus Daten bestehen, die aus einem Merkmalsauszug tatsächlicher biometrischer Proben abgeleitet sind. Biometrische Templates sollten zwar aus biometrischen Daten generiert werden, aber es sollte nicht möglich sein, dieselben biometrischen Daten aus den biometrischen Templates zu erhalten.
- (28) Der Router sollte – sofern der ersuchende Mitgliedstaat dies beschließt und sofern anwendbar nach der Art der biometrischen Daten – die Antworten des ersuchten Mitgliedstaats oder der ersuchten Mitgliedstaaten oder von Europol mittels eines Abgleichs der für die Abfrage verwendeten biometrischen Daten und der in den Antworten des ersuchten Mitgliedstaats oder der ersuchten Mitgliedstaaten oder von Europol mitgeteilten biometrischen Daten in eine Rangfolge bringen.

(29) Bei einer Übereinstimmung zwischen den für die Abfrage verwendeten Daten und den in der nationalen Datenbank des ersuchten Mitgliedstaats oder der ersuchten Mitgliedstaaten gespeicherten Daten sollte der ersuchte Mitgliedstaat nach einer manuellen Bestätigung der Übereinstimmung durch einen qualifizierten Mitarbeiter des ersuchenden Mitgliedstaats und nach der Übermittlung einer Sachverhaltsdarstellung und des zugrundeliegenden Straftatbestands unter Verwendung der gemeinsamen Tabelle der Kategorien von Straftatbeständen, die in einem gemäß dem Rahmenbeschluss 2009/315/JI zu erlassenden Durchführungsrechtsakt festgelegt wird, einen begrenzten Kerndatensatz zurücksenden, insoweit diese Kerndaten vorhanden sind. Der begrenzte Kerndatensatz sollte über den Router zurückgesendet werden, und zwar innerhalb von 48 Stunden nachdem die entsprechenden Bedingungen erfüllt wurden, außer wenn nach Maßgabe des nationalen Rechts eine Genehmigung durch eine Justizbehörde erforderlich ist. Diese Frist stellt einen schnellen Informationsaustausch zwischen den zuständigen Behörden der Mitgliedstaaten sicher. Die Mitgliedstaaten sollten die Kontrolle über die Freigabe dieses begrenzten Kerndatensatzes behalten. Bei den wichtigsten Etappen des Prozesses, unter anderem bei der Entscheidung über die Einleitung eines Abfrageersuchens, bei der Entscheidung über die Bestätigung einer Übereinstimmung, bei der Entscheidung über die Einleitung eines Ersuchens um Übermittlung des Kerndatensatzes nach der Bestätigung der Übereinstimmung und bei der Entscheidung, personenbezogene Daten an den ersuchenden Mitgliedstaat weiterzugeben, sollten Eingriffe von Menschen weiterhin möglich sein, um sicherzustellen, dass keine Kerndaten auf automatisierte Weise ausgetauscht werden.

- (30) Im spezifischen Fall einer DNA sollte auch der ersuchte Mitgliedstaat eine Übereinstimmung zwischen zwei DNA-Profilen bestätigen können, wenn dies für die Untersuchung von Straftaten relevant ist. Daher sollte der ersuchende Mitgliedstaat nach Bestätigung dieser Übereinstimmung durch den ersuchten Mitgliedstaat und nach Übermittlung einer Sachverhaltsdarstellung und des zugrundeliegenden Straftatbestands unter Verwendung der gemeinsamen Tabelle der Kategorien von Straftatbeständen, die in einem gemäß dem Rahmenbeschluss 2009/315/JI zu erlassenden Durchführungsrechtsakt aufgeführt wird, innerhalb von 48 Stunden nachdem die entsprechenden Bedingungen erfüllt wurden einen begrenzten Kerndatensatz über den Router zurücksenden, außer wenn nach Maßgabe des nationalen Rechts eine Genehmigung durch eine Justizbehörde erforderlich ist.
- (31) Rechtmäßig übermittelte und empfangene Daten unterliegen den gemäß der Richtlinie (EU) 2016/680 festgelegten Fristen für die Speicherung und Überprüfung.
- (32) Bei der Entwicklung des Routers und des EPRIS sollte soweit anwendbar das universelle Nachrichtenformat (Universal Message Format, im Folgenden „UMF“) verwendet werden. Bei jedem automatisierten Datenaustausch gemäß dieser Verordnung sollte soweit anwendbar der UMF-Standard verwendet werden. Die zuständigen Behörden der Mitgliedstaaten und Europol werden auch dazu angehalten, den UMF-Standard 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.

- (33) Über den Prüm-II-Rahmen sollten nur nicht als Verschlussache eingestufte Informationen ausgetauscht werden.
- (34) Jeder Mitgliedstaat sollte den anderen Mitgliedstaaten, der Kommission, der durch die Verordnung (EU) 2018/1726 des Europäischen Parlaments und des Rates¹⁴ errichteten Agentur der Europäischen Union für das Betriebsmanagement von Großinformationssystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) und Europol den Inhalt seiner nationalen Datenbanken, die über den Prüm-II-Rahmen zur Verfügung gestellt werden, und die Bedingungen für automatisierte Abfragen mitteilen.

¹⁴ 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).

- (35) 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 die automatisierte Abfrage, die Standards für den Datenaustausch, einschließlich Mindestqualitätsstandards, und die auszutauschenden Datenelemente. Zur Sicherstellung einheitlicher Bedingungen für die Durchführung dieser Verordnung im Hinblick auf diese Aspekte sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates¹⁵ ausgeübt werden.
- (36) Die Datenqualität ist als Schutzmaßnahme von größter Bedeutung und eine wesentliche Voraussetzung für die Sicherstellung der Wirksamkeit dieser Verordnung. Im Zusammenhang mit automatisierten Abfragen biometrischer Daten und um sicherzustellen, dass die übermittelten Daten von ausreichender Qualität sind und das Risiko falscher Übereinstimmungen verringert wird, sollte ein Mindestqualitätsstandard festgelegt werden, der regelmäßig überprüft werden sollte.

¹⁵ 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).

- (37) Angesichts des Umfangs und der Sensibilität der für die Zwecke dieser Verordnung ausgetauschten personenbezogenen Daten und der unterschiedlichen nationalen Vorschriften für die Speicherung von Informationen über natürliche Personen in nationalen Datenbanken ist es wichtig sicherzustellen, dass die für die automatisierte Abfrage im Rahmen dieser Verordnung verwendeten Datenbanken im Einklang mit dem nationalen Recht und der Richtlinie (EU) 2016/680 eingerichtet werden. Daher sollten die Mitgliedstaaten, bevor sie ihre nationalen Datenbanken mit dem Router oder dem EPRIS verbinden, eine Datenschutz-Folgenabschätzung gemäß der Richtlinie (EU) 2016/680 durchführen und die in dieser Richtlinie vorgesehene Aufsichtsbehörde konsultieren.
- (38) Die Mitgliedstaaten und Europol sollen die Richtigkeit und die Relevanz der gemäß dieser Verordnung verarbeiteten personenbezogenen Daten sicherstellen. Stellt ein Mitgliedstaat oder Europol fest, dass die übermittelten Daten unrichtig oder nicht länger aktuell sind oder nicht hätten übermittelt werden dürfen, übermittelt worden sind, so sollte er dies dem ersuchenden Mitgliedstaat oder Europol unverzüglich mitteilen. Alle betroffenen Mitgliedstaaten oder Europol sollen unverzüglich die Daten entsprechend berichtigen oder löschen. Hat der Mitgliedstaat, der die Daten erhalten hat, oder Europol Grund zu der Annahme, dass die mitgeteilten Daten unrichtig sind oder gelöscht werden sollten, so sollte er den Mitgliedstaat, der die Daten bereitgestellt hat, unverzüglich darüber unterrichten.

- (39) Eine umfassende Überwachung der Umsetzung dieser Verordnung ist äußerst wichtig. Insbesondere sollten für die Einhaltung der Bestimmungen über die Verarbeitung personenbezogener Daten wirksame Garantien vorgesehen und eine regelmäßige Überwachung und Prüfungen durch für die Datenverarbeitung Verantwortliche, Aufsichtsbehörden und den Europäischen Datenschutzbeauftragten soweit erforderlich sichergestellt werden. Es sollten Bestimmungen bestehen, die eine regelmäßige Prüfung der Zulässigkeit von Abfragen ermöglichen, und die Rechtmäßigkeit der Datenverarbeitung solle ebenfalls gegeben sein.
- (40) Die Aufsichtsbehörden und der Europäische Datenschutzbeauftragte sollten im Rahmen ihrer Zuständigkeiten eine koordinierte Aufsicht über die Anwendung dieser Verordnung sicherstellen, insbesondere wenn sie größere Diskrepanzen zwischen den Verfahren der Mitgliedstaaten, potenziell unrechtmäßige Übermittlungen oder potenzielle politisch motivierte Ersuchen feststellen.
- (41) Bei der Umsetzung dieser Verordnung ist es von entscheidender Bedeutung, dass die Mitgliedstaaten und Europol die Rechtsprechung des Gerichtshofs der Europäischen Union zum Austausch biometrischer Daten zur Kenntnis nehmen.
- (42) Drei Jahre nach Inbetriebnahme des Routers und des EPRIS und danach alle vier Jahre sollte die Kommission einen Bewertungsbericht erstellen, der eine Bewertung der Anwendung dieser Verordnung durch die Mitgliedstaaten und Europol und insbesondere betreffend die Einhaltung der einschlägigen Datenschutzgarantien durch die Mitgliedstaaten umfasst. Bewertungsberichte sollten auch eine Prüfung der im Hinblick auf die Ziele dieser Verordnung erzielten Ergebnisse und der Auswirkungen auf die Grundrechte enthalten. Im Rahmen der Bewertungsberichte sollten auch die Auswirkungen, die Leistung, die Wirksamkeit, die Effizienz, die Sicherheit und die Arbeitsverfahren des Prüm-II-Rahmens bewertet werden.

- (43) Da diese Verordnung die Festlegung eines neuen Prüm-Rahmens vorsieht, sollten die Bestimmungen der Beschlüsse 2008/615/JI und 2008/616/JI, die nicht mehr relevant sind, gestrichen werden. Diese Beschlüsse sollten entsprechend geändert werden.
- (44) Da der Router von eu-LISA entwickelt und verwaltet werden soll, sollte die Verordnung (EU) 2018/1726 so geändert werden, dass diese Aufgaben zu den Aufgaben von eu-LISA hinzugefügt werden.
- (45) Da die Ziele dieser Verordnung, nämlich die grenzüberschreitende polizeiliche Zusammenarbeit zu verstärken und den zuständigen Behörden der Mitgliedstaaten die Abfrage nach vermissten Personen und die Identifizierung nicht identifizierter menschlicher Überreste zu ermöglichen, von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen des Umfangs und der Wirkungen der Maßnahme auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union (EUV) verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieser Ziele erforderliche Maß hinaus.
- (46) Nach den Artikeln 1 und 2 des dem EUV und dem AEUV 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.

- (47) Nach Artikel 3 des dem EUV und dem AEUV beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts hat Irland mitgeteilt, dass es sich an der Annahme und der Anwendung dieser Verordnung beteiligen möchte.
- (48) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 angehört und hat am 2. März 2022¹⁶ eine Stellungnahme abgegeben —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

¹⁶ ABl. C 225 vom 9.6.2022, S. 6.

Kapitel 1

Allgemeine Bestimmungen

Artikel 1

Gegenstand

Mit dieser Verordnung wird ein Rahmen für die Abfrage und den Austausch von Informationen zwischen den zuständigen Behörden der Mitgliedstaaten geschaffen (im Folgenden „Prüm-II-Rahmen“), indem Folgendes festgelegt wird:

- a) die Bedingungen und Verfahren für die automatisierte Abfrage von DNA-Profilen, bestimmten Fahrzeugzulassungsdaten, daktyloskopischen Daten, Gesichtsbildern und Polizeiakten; sowie
- b) die Vorschriften für den Austausch von Kerndaten nach einer bestätigten Übereinstimmung bei biometrischen Daten.

Artikel 2

Ziel

Das Ziel des Prüm-II-Rahmens besteht darin, die grenzübergreifende Zusammenarbeit in Angelegenheiten, die unter Teil III Titel V Kapitel 4 und 5 des Vertrags über die Arbeitsweise der Europäischen Union fallen, zu intensivieren, insbesondere durch die Erleichterung des Informationsaustauschs zwischen den zuständigen Behörden der Mitgliedstaaten unter uneingeschränkter Achtung der Grundrechte natürlicher Personen einschließlich des Rechts auf Achtung des Privatlebens und das Recht des Schutzes personenbezogener Daten im Einklang mit der Charta der Grundrechte der Europäischen Union.

Des Weiteren soll mit Prüm-II-Rahmen den zuständigen Behörden der Mitgliedstaaten die Abfrage nach vermissten Personen im Rahmen strafrechtlicher Ermittlungen oder aus humanitären Gründen und die Identifizierung von menschlichen Überresten gemäß Artikel 29 ermöglicht werden, sofern diese Behörden nach nationalem Recht befugt sind, derartige Suchmaßnahmen und derartige Identifizierungen durchzuführen.

Artikel 3

Anwendungsbereich

Diese Verordnung findet Anwendung auf die Datenbanken, die nach nationalem Recht eingerichtet sind und die für die automatisierte Übermittlung von DNA-Profilen, daktyloskopischen Daten, bestimmten Fahrzeugzulassungsdaten, Gesichtsbildern, und Polizeiakten im Einklang mit der Richtlinie (EU) 2016/680 oder der Verordnungen (EU) 2018/1725, (EU) 2016/794 oder der Verordnung (EU) 2016/679 verwendet werden.

Artikel 4

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Loci“ (Singular: „Locus“) DNA-Orte, die Identifikationsmerkmale einer analysierten menschlichen DNA-Probe enthalten;
2. „DNA-Profil“ einen Buchstaben- bzw. Zahlencode, der eine Reihe von Loci oder die spezielle Molekularstruktur an den verschiedenen Loci darstellt;

3. „DNA-Fundstellendatensatz“ ein in Artikel 7 genanntes DNA-Profil und die entsprechende Referenznummer;
4. „identifiziertes DNA-Profil“ das DNA-Profil einer identifizierten Person;
5. „nicht identifiziertes DNA-Profil“ ein DNA-Profil einer noch nicht identifizierten Person, das im Zuge der Untersuchung von Straftaten gewonnen wurde, einschließlich eines aus Spuren gewonnenen DNA-Profils;
6. „daktyloskopische Daten“ Bilder von Fingerabdrücken, Bilder von Fingerabdruckspuren, Bilder von Handabdrücken, Bilder von Handabdruckspuren und Templates derartiger Abdrücke (codierte Minutien), die in einer automatisierten Datenbank gespeichert und verarbeitet werden;
7. „daktyloskopischer Fundstellendatensatz“ die in Artikel 12 genannten daktyloskopischen Daten und die entsprechende Referenznummer;
8. „nicht identifizierte daktyloskopische Daten“ die bei der Untersuchung einer Straftat erhobenen daktyloskopischen Daten einer noch nicht identifizierten Person, einschließlich aus Spuren gewonnener daktyloskopischer Daten;
9. „identifizierte daktyloskopische Daten“ die daktyloskopischen Daten einer identifizierten Person;
10. „Einzelfall“ eine einzelne Akte im Zusammenhang mit der Verhütung, Aufdeckung oder Untersuchung einer Straftat, der Abfrage nach einer vermissten Person oder der Identifizierung nicht identifizierter menschlicher Überreste;

11. „Gesichtsbild“ eine digitale Aufnahme des Gesichts einer Person;
12. „Fundstellendatensatz zu Gesichtsbildern“ ein in Artikel 21 genanntes Gesichtsbild und die entsprechende Referenznummer;
13. „nicht identifiziertes Gesichtsbild“ ein bei der Untersuchung einer Straftat erhobenes Gesichtsbild, das zu einer noch nicht identifizierten Person gehört, einschließlich eines aus Spuren gewonnenen Gesichtsbildes;
14. „identifiziertes Gesichtsbild“ das Gesichtsbild einer identifizierten Person;
15. „biometrische Daten“ DNA-Profile, daktyloskopische Daten oder Gesichtsbilder;
16. „alphanumerische Daten“ Daten in Form von Buchstaben, Ziffern, Sonderzeichen, Leerzeichen und Satzzeichen;
17. „Übereinstimmung“ eine Übereinstimmung als Ergebnis eines automatischen Abgleichs zwischen in einer Datenbank gespeicherten personenbezogenen Daten;
18. „Kandidat“ Daten, mit denen eine Übereinstimmung festgestellt wurde;
19. „ersuchender Mitgliedstaat“ einen Mitgliedstaat, der eine Abfrage über den Prüm-II-Rahmen durchführt;
20. „ersuchter Mitgliedstaat“ den Mitgliedstaat, in dessen Datenbanken ein ersuchender Mitgliedstaat eine Abfrage über den Prüm-II-Rahmen durchführt;

21. „Polizeiakten“ biografische Daten von Verdächtigen und verurteilten Personen, die in für die Verhütung, Aufdeckung und Untersuchung von Straftaten eingerichteten nationalen Datenbanken verfügbar sind;
22. „Pseudonymisierung“ Pseudonymisierung im Sinne des Artikels 3 Nummer 5 der Richtlinie (EU) 2016/680;
23. „Verdächtiger“ eine Person im Sinne des Artikels 6 Buchstabe a der Richtlinie (EU) 2016/680;
24. „personenbezogene Daten“ personenbezogene Daten im Sinne des Artikels 3 Nummer 1 der Richtlinie (EU) 2016/680;
25. „Europol-Daten“ alle operativen personenbezogenen Daten, die von Europol gemäß der Verordnung (EU) 2016/794 verarbeitet werden;
26. „zuständige Behörde“ jede für die Verhütung, Aufdeckung oder Untersuchung von Straftaten zuständige staatliche Stelle oder jede andere Stelle oder Einrichtung, die nach dem Recht eines Mitgliedstaats mit der Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse für die Zwecke der Verhütung, Aufdeckung oder Untersuchung von Straftaten betraut ist;
27. „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 41 der Richtlinie (EU) 2016/680 eingerichtete unabhängige staatliche Stelle;

28. „SIENA“ die von Europol verwaltete und entwickelte Netzanwendung für sicheren Datenaustausch gemäß der Verordnung (EU) 2016/794;
29. „Vorfall“ einen Vorfall im Sinne des Artikels 6 Nummer 6 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates¹⁷;
30. „erheblicher Vorfall“ einen Vorfall mit Ausnahme eines Vorfalls, der begrenzte Auswirkungen hat und in Bezug auf die Methode oder Technologie wahrscheinlich bereits wohlbekannt ist;
31. „erhebliche Cyberbedrohung“ eine Cyberbedrohung mit der Möglichkeit und der Fähigkeit und deren Zweck es ist, einen erheblichen Vorfall zu verursachen;
32. „erhebliche Schwachstelle“ eine Schwachstelle, die wahrscheinlich zu einem erheblichen Vorfall führt, wenn sie genutzt wird.

¹⁷ Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80).

Kapitel 2

Austausch von Daten

ABSCHNITT 1

DNA-PROFILE

Artikel 5

DNA-Fundstellendatensätze

- (1) Die Mitgliedstaaten stellen sicher, dass DNA-Fundstellendatensätze aus ihren nationalen DNA-Datenbanken für die Zwecke automatisierter Abfragen durch andere Mitgliedstaaten und Europol gemäß dieser Verordnung verfügbar sind.

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

Nicht identifizierte DNA-Profile müssen als solche erkennbar sein.

- (2) Die Verarbeitung von DNA-Fundstellendatensätzen erfolgt gemäß dieser Verordnung und unter Beachtung des für die Verarbeitung dieser Daten geltenden nationalen Rechts.

- (3) Die Kommission erlässt einen Durchführungsrechtsakt zur Festlegung der Identifikationsmerkmale der auszutauschenden DNA-Profile. Der betreffende Durchführungsrechtsakt wird nach dem in Artikel 77 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 6

Automatisierte Abfrage von DNA-Profilen

- (1) Zur Untersuchung von Straftaten führen die Mitgliedstaaten zum Zeitpunkt der Erstverbindung mit dem Router über ihre nationalen Kontaktstellen eine automatisierte Abfrage mittels eines Abgleichs aller DNA-Profile, die in ihren DNA-Datenbanken gespeichert sind, mit allen in den DNA-Datenbanken aller anderen Mitgliedstaaten und von Europol gespeicherten DNA-Profilen durch. Die Mitgliedstaaten und Europol vereinbaren bilateral mit jedem anderen Mitgliedstaat die Modalitäten dieser automatisierten Abfragen im Einklang mit den in dieser Verordnung festgelegten Vorschriften und Verfahren.
- (2) Zur Untersuchung von Straftaten führen die Mitgliedstaaten über ihre nationalen Kontaktstellen automatisierte Abfragen mittels eines Abgleichs aller der neuen DNA-Profile, die ihren DNA-Datenbanken hinzugefügt wurden, mit allen in den DNA-Datenbanken aller anderen Mitgliedstaaten und von Europol-Daten gespeicherten DNA-Profilen durch.

- (3) Konnten die in Absatz 2 genannten Abfragen nicht stattfinden, so kann der betroffene Mitgliedstaat bilateral mit jedem anderen Mitgliedstaat und mit Europol vereinbaren, sie zu einem späteren Zeitpunkt durchzuführen, indem sie DNA-Profile mit allen in den DNA-Datenbanken aller anderen Mitgliedstaaten und in den Europol-Daten gespeicherten DNA-Profilen abgleichen. Der betroffene Mitgliedstaat vereinbart bilateral mit jedem anderen Mitgliedstaat und mit Europol die Modalitäten für diese automatisierte Abfrage im Einklang mit den in dieser Verordnung festgelegten Vorschriften und Verfahren.
- (4) Abfragen gemäß den Absätzen 1, 2 und 3 werden nur im Rahmen von Einzelfällen und nur nach Maßgabe des nationalen Rechts des ersuchenden Mitgliedstaats erfolgen.
- (5) Wird im Zuge einer automatisierten Abfrage eine Übereinstimmung eines übermittelten DNA-Profils mit DNA-Profilen festgestellt, die in der Datenbank bzw. den Datenbanken 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.
- (6) Die nationale Kontaktstelle des ersuchenden Mitgliedstaats kann entscheiden, eine Übereinstimmung zwischen zwei DNA-Profilen zu bestätigen. Wenn sie sich entscheidet, eine Übereinstimmung zwischen zwei DNA-Profilen zu bestätigen, unterrichtet sie den ersuchten Mitgliedstaat und sorgt dafür, dass mindestens ein qualifizierter Mitarbeiter eine manuelle Überprüfung durchführt, um diese Übereinstimmung mit den vom ersuchten Mitgliedstaat erhaltenen DNA-Fundstellendaten zu bestätigen.

- (7) Soweit es für die Untersuchung von Straftaten relevant ist, kann die nationale Kontaktstelle des ersuchten Mitgliedstaats entscheiden, eine Übereinstimmung zwischen zwei DNA-Profilen zu bestätigen. Wenn sie sich entscheidet, eine Übereinstimmung zwischen zwei DNA-Profilen zu bestätigen, unterrichtet sie den ersuchenden Mitgliedstaat und sorgt dafür, dass mindestens ein qualifizierter Mitarbeiter eine manuelle Überprüfung durchführt, um diese Übereinstimmung mit den vom ersuchenden Mitgliedstaat erhaltenen DNA-Fundstellendaten zu bestätigen.

Artikel 7
Referenznummern von DNA-Profilen

Die Referenznummern von DNA-Profilen bestehen aus einer Kombination folgender Elemente:

- a) einer Referenznummer, die es den Mitgliedstaaten im Fall einer Übereinstimmung ermöglicht, weitere Daten und sonstige Informationen in ihren nationalen DNA-Datenbanken abzurufen, um sie einem, mehreren oder allen anderen Mitgliedstaaten gemäß Artikel 47 oder Europol gemäß Artikel 49 Absatz 6 zu übermitteln;
- b) einer Referenznummer, die es Europol im Fall einer Übereinstimmung ermöglicht, weitere Daten und sonstige Informationen für die Zwecke des Artikels 48 Absatz 1 dieser Verordnung abzurufen, um sie gemäß der Verordnung (EU) 2016/794 einem, mehreren oder allen Mitgliedstaaten zu übermitteln;
- c) einem Code zur Angabe des Mitgliedstaats, dem das DNA-Profil vorliegt;

- d) einem Code, der anzeigt, ob es sich bei dem DNA-Profil um ein identifiziertes DNA-Profil oder ein nicht identifiziertes DNA-Profile handelt.

Artikel 8

Grundsätze des Austauschs von DNA-Profilen

- (1) Die Mitgliedstaaten treffen geeignete Maßnahmen zur Wahrung der Vertraulichkeit und Integrität der an andere Mitgliedstaaten oder Europol weitergeleiteten DNA-Fundstellendatensätze, einschließlich ihrer Verschlüsselung. Europol ergreift geeignete Maßnahmen zur Wahrung der Vertraulichkeit und Integrität der an die Mitgliedstaaten übermittelten DNA-Fundstellendatensätze, einschließlich ihrer Verschlüsselung, zu gewährleisten.
- (2) Jeder Mitgliedstaat und Europol stellen sicher, dass die von ihnen übermittelten DNA-Profiles von ausreichender Qualität für einen automatisierten Abgleich sind. Die Kommission legt im Wege von Durchführungsrechtsakten einen Mindestqualitätsstandard fest, um den Abgleich von DNA-Profilen zu ermöglichen.
- (3) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der einschlägigen europäischen oder internationalen Standards, die von den Mitgliedstaaten und Europol für den Austausch von DNA-Fundstellendatensätzen zu verwenden sind.
- (4) Die in den Absätzen 2 und 3 des vorliegenden Artikels genannten Durchführungsrechtsakte werden nach dem in Artikel 77 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 9

Regeln für Ersuchen und Antworten in Bezug auf DNA-Profile

- (1) Ein Ersuchen um eine automatisierte Abfrage von DNA-Profilen enthält ausschließlich die folgenden Informationen:
- a) Code des ersuchenden Mitgliedstaats;
 - b) Datum, Uhrzeit und Kennnummer des Ersuchens;
 - c) die DNA--Fundstellendatensätze;
 - d) ob die übermittelten DNA-Profile nicht identifizierte DNA-Profile oder identifizierte DNA-Profile sind.
- (2) Eine Antwort auf ein in Absatz 1 genanntes Ersuchen enthält ausschließlich folgende Informationen:
- a) Angabe, ob eine oder mehrere Übereinstimmungen oder keine Übereinstimmungen vorliegen;
 - b) Datum, Uhrzeit und Kennnummer des Ersuchens;
 - c) Datum, Uhrzeit und Kennnummer der Antwort;
 - d) Codes des ersuchenden und des ersuchten Mitgliedstaats;

- e) Referenznummern der DNA-Profile des ersuchenden und des ersuchten Mitgliedstaats;
 - f) ob die übermittelten DNA-Profile nicht identifizierte DNA-Profile oder identifizierte DNA-Profile sind;
 - g) die übereinstimmenden DNA-Profile.
- (3) Einer Übereinstimmung wird nur dann automatisch erfolgen, wenn die automatisierte Abfrage eine Übereinstimmung eines Minimums an Loci ergeben hat. Die Kommission erlässt im Wege von Durchführungsrechtsakten das Minimum an Loci nach dem in Artikel 77 Absatz 2 genannten Prüfverfahren.
- (4) Ergibt eine Abfrage 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 der Abfrage durch einen anderen Mitgliedstaat eine Übereinstimmung für das betreffende DNA-Profil vorliegt. Die Markierung enthält die Referenznummer des von dem ersuchenden Mitgliedstaat verwendeten DNA-Profils.
- (5) Die Mitgliedstaaten stellen sicher, dass die Ersuchen gemäß Absatz 1 des vorliegenden Artikels mit den Mitteilungen gemäß Artikel 74 übereinstimmen. Diese Mitteilungen sind in dem in Artikel 79 genannten Handbuch wiederzugeben.

ABSCHNITT 2

DAKTYLOSKOPISCHE DATEN

Artikel 10

Daktyloskopische Fundstellendatensätze

- (1) Die Mitgliedstaaten stellen sicher, dass daktyloskopische Fundstellendatensätze aus ihren nationalen Datenbanken, die zur Verhütung, Aufdeckung und Untersuchung von Straftaten errichtet wurden, verfügbar sind.
- (2) Daktyloskopische Fundstellendatensätze dürfen keine zusätzlichen Daten enthalten, aufgrund deren eine Person unmittelbar identifiziert werden kann.
- (3) Nicht identifizierte daktyloskopische Daten müssen als solche erkennbar sein.

Artikel 11

Automatisierte Abfrage 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 nationalen Datenbanken, um automatisierte Abfragen mittels eines Abgleichs von daktyloskopischen Fundstellendatensätzen durchzuführen.

Abfragen gemäß Unterabsatz 1 dürfen nur im Rahmen von Einzelfällen und nur nach Maßgabe des nationalen Rechts des ersuchenden Mitgliedstaats erfolgen.

- (2) Die nationale Kontaktstelle des ersuchenden Mitgliedstaats kann entscheiden, eine Übereinstimmung zwischen zwei daktyloskopischen Daten zu bestätigen. Wenn sie sich dafür entscheidet die Übereinstimmung zwischen zwei daktyloskopischen Daten zu bestätigen, unterrichtet sie den ersuchten Mitgliedstaat und sorgt dafür, dass mindestens ein qualifizierter Mitarbeiter eine manuelle Überprüfung durchführt, um diese Übereinstimmung mit den vom ersuchten Mitgliedstaat erhaltenen daktyloskopischen Fundstellendatensätzen zu bestätigen.

Artikel 12
Referenznummern daktyloskopischer Daten

Die Referenznummern daktyloskopischer Daten bestehen aus einer Kombination folgender Elemente:

- a) einer Referenznummer, die es den Mitgliedstaaten im Fall einer Übereinstimmung ermöglicht, weitere Daten und sonstige Informationen in ihren in Artikel 10 genannten Datenbanken abzurufen, um sie einem, mehreren oder allen anderen Mitgliedstaaten gemäß Artikel 47 oder Europol gemäß Artikel 49 Absatz 6 zu übermitteln;
- b) einer Referenznummer, die es Europol im Fall einer Übereinstimmung ermöglicht, weitere Daten und sonstige Informationen für die Zwecke des Artikels 48 Absatz 1 dieser Verordnung abzurufen, um sie gemäß der Verordnung (EU) 2016/794 einem, mehreren oder allen Mitgliedstaaten zu übermitteln;

- c) einem Code zur Angabe des Mitgliedstaats, dem die daktyloskopischen Daten vorliegen.

Artikel 13

Grundsätze des Austauschs daktyloskopischer Daten

- (1) Die Mitgliedstaaten treffen geeignete Maßnahmen, um die Vertraulichkeit und Integrität der an andere Mitgliedstaaten oder Europol übermittelten daktyloskopischen Daten, einschließlich ihrer Verschlüsselung, zu wahren. Europol trifft geeignete Maßnahmen, um die Vertraulichkeit und Integrität der an Mitgliedstaaten übermittelten daktyloskopischen Daten, einschließlich ihrer Verschlüsselung, zu wahren.
- (2) Jeder Mitgliedstaat und Europol stellen sicher, dass die von ihnen übermittelten daktyloskopischen Daten für einen automatisierten Abgleich von ausreichender Qualität sind. Die Kommission legt im Wege von Durchführungsrechtsakten einen Mindestqualitätsstandard fest, um den Abgleich daktyloskopischer Daten zu ermöglichen.
- (3) Die daktyloskopischen Daten werden digitalisiert und gemäß europäischen oder internationalen Standards an die anderen Mitgliedstaaten oder Europol übermittelt. Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der einschlägigen europäischen oder internationalen Standards, die die Mitgliedstaaten und Europol für den Austausch von daktyloskopischen Daten verwenden müssen.
- (4) Die in den Absätzen 2 und 3 des vorliegenden Artikels genannten Durchführungsrechtsakte werden nach dem in Artikel 77 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 14

Abfragekapazitäten für daktyloskopische Daten

- (1) Jeder Mitgliedstaat stellt sicher, dass sein Abfrageersuchen nicht die Abfragekapazitäten überschreitet, die der jeweilige ersuchte Mitgliedstaat oder Europol angegeben hat, um die Bereitschaft des Systems aufrechtzuerhalten und eine Systemüberlastung zu verhindern. Zu demselben Zweck stellt Europol sicher, dass ihr Abfrageersuchen nicht die Abfragekapazitäten überschreitet, die der jeweilige ersuchte Mitgliedstaat angegeben hat.

Die Mitgliedstaaten unterrichten die anderen Mitgliedstaaten, die Kommission, eu-LISA und Europol über ihre maximalen täglichen Abfragekapazitäten für identifizierte und nicht identifizierte daktyloskopische Daten. Europol unterrichtet die Mitgliedstaaten, die Kommission und eu-LISA über ihre maximalen täglichen Abfragekapazitäten für identifizierte und nicht identifizierte daktyloskopische Daten. Die Mitgliedstaaten oder Europol können diese Abfragekapazitäten jederzeit, auch in dringenden Fällen, vorübergehend oder dauerhaft erhöhen. Erhöht ein Mitgliedstaat diese maximalen Abfragekapazitäten, so teilt er den anderen Mitgliedstaaten, der Kommission, eu-LISA und Europol die neuen maximalen Abfragekapazitäten mit. Erhöht Europol diese maximalen Abfragekapazitäten, so teilt sie den anderen Mitgliedstaaten, der Kommission und eu-LISA die neuen maximalen Abfragekapazitäten mit.

- (2) Zur Festlegung der Höchstzahl der pro Übermittlung für einen Abgleich akzeptierten Kandidaten und der Aufteilung ungenutzter Abfragekapazitäten zwischen den Mitgliedstaaten erlässt die Kommission Durchführungsrechtsakte nach dem in Artikel 77 Absatz 2 genannten Verfahren.

Artikel 15

Regeln für Ersuchen und Antworten in Bezug auf daktyloskopische Daten

- (1) Ein Ersuchen um eine automatisierte Abfrage daktyloskopischer Daten enthält ausschließlich die folgenden Informationen:
- a) Code des ersuchenden Mitgliedstaats;
 - b) Datum, Uhrzeit und Kennnummer des Ersuchens;
 - c) die in Artikel 12 genannten daktyloskopischen Fundstellendatensätze.
- (2) Eine Antwort auf ein in Absatz 1 genanntes Ersuchen enthält ausschließlich folgende Informationen:
- a) Angabe, ob eine oder mehrere Übereinstimmungen oder keine Übereinstimmungen vorliegen;
 - b) Datum, Uhrzeit und Kennnummer des Ersuchens;
 - c) Datum, Uhrzeit und Kennnummer der Antwort;

- d) Codes des ersuchenden und des ersuchten Mitgliedstaats;
 - e) Referenznummern der daktyloskopischen Daten des ersuchenden und des ersuchten Mitgliedstaats;
 - f) die übereinstimmenden daktyloskopischen Daten.
- (3) Die Mitgliedstaaten stellen sicher, dass die Ersuchen gemäß Absatz 1 des vorliegenden Artikels mit den Mitteilungen gemäß Artikel 74 übereinstimmen. Diese Mitteilungen sind in dem in Artikel 79 genannten Handbuch wiederzugeben.

ABSCHNITT 3

FAHRZEUGZULASSUNGSDATEN

Artikel 16

Automatisierte Abfrage von Fahrzeugzulassungsdaten

- (1) Die Mitgliedstaaten gestatten den nationalen Kontaktstellen anderer Mitgliedstaaten und Europol zur Verhütung, Aufdeckung und Untersuchung von Straftaten den Zugriff auf folgende nationale Fahrzeugzulassungsdaten, um in Einzelfällen automatisierte Abfragen durchzuführen:
- a) Daten zum Eigentümer oder Halter;
 - b) Daten zum Fahrzeug.

- (2) Die in Absatz 1 genannten Abfragen erfolgen nur anhand folgender Daten:
- a) einer vollständigen Fahrzeug-Identifizierungsnummer;
 - b) eines vollständigen Kennzeichens; oder
 - c) der Daten zum Eigentümer oder Halter des Fahrzeugs, sofern dies nach dem nationalen Recht des ersuchten Mitgliedstaats zulässig ist.
- (3) Die in Absatz 1 genannten Abfragen anhand von Daten zum Eigentümer oder Halter des Fahrzeugs werden nur bei Verdächtigen oder verurteilten Personen durchgeführt. Für diese Abfragen werden alle folgenden Identifizierungsdaten verwendet:
- a) wenn es sich bei dem Eigentümer oder Halter des Fahrzeugs um eine natürliche Person handelt:
 - i) Vorname(n) der natürlichen Person,
 - ii) Familienname(n) der natürlichen Person und
 - iii) Geburtsdatum der natürlichen Person;
 - b) wenn es sich bei dem Eigentümer oder Halter des Fahrzeugs um eine juristische Person handelt, der Name dieser juristischen Person.
- (4) Die in Absatz 1 genannten Abfragen erfolgen nur nach Maßgabe des nationalen Rechts des ersuchenden Mitgliedstaats.

Artikel 17

Grundsätze der automatisierten Abfrage von Fahrzeugzulassungsdaten

- (1) Für die automatisierte Abfrage von Fahrzeugzulassungsdaten verwenden die Mitgliedstaaten das Europäische Fahrzeug- und Führerschein-Informationssystem (EUCARIS).
- (2) Die über das EUCARIS ausgetauschten Informationen werden verschlüsselt übertragen.
- (3) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der Datenelemente der Fahrzeugzulassungsdaten, die ausgetauscht werden dürfen, und des technischen Verfahrens für die Abfrage der Datenbanken der Mitgliedstaaten über das EUCARIS. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 77 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 18

Führen von Protokollen

- (1) Jeder Mitgliedstaat führt Protokolle über die Abfragen, die zum Austausch von Fahrzeugzulassungsdaten ordnungsgemäß ermächtigten Mitarbeiter seiner zuständigen Behörden durchführen, sowie Protokolle über die Abfrageersuchen von anderen Mitgliedstaaten. Europol führt Protokolle über Abfragen seiner ordnungsgemäß ermächtigten Mitarbeiter.

Jeder Mitgliedstaat und Europol führt Protokolle über alle Datenverarbeitungsvorgänge im Zusammenhang mit Fahrzeugzulassungsdaten. Diese Protokolle enthalten folgende Angaben:

- a) ob ein Mitgliedstaat oder Europol das Abfrageersuchen eingeleitet hat; wenn ein Mitgliedstaat das Abfrageersuchen eingeleitet hat, den betreffenden Mitgliedstaat;
- b) Datum und Uhrzeit des Ersuchens;
- c) Datum und Uhrzeit der Antwort;
- d) nationale Datenbanken, an die ein Abfrageersuchen gerichtet wurde;
- e) nationale Datenbanken, die eine positive Antwort übermittelt haben.

(2) Die in Absatz 1 genannten Protokolle werden nur zur Erhebung von Statistiken und zur datenschutzrechtlichen Kontrolle, einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit und -integrität verwendet. Diese Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und drei Jahre nach ihrer Erstellung gelöscht. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, so werden sie gelöscht, sobald die Protokolle nicht mehr für das Kontrollverfahren benötigt werden.

- (3) Zum Zwecke der datenschutzrechtlichen Kontrolle, einschließlich zur Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung haben die für die Verarbeitung Verantwortlichen Zugang zu den Protokollen für die Eigenkontrolle nach Artikel 55.

ABSCHNITT 4

GESICHTSBILDER

Artikel 19

Fundstellendatensätze zu Gesichtsbildern

- (1) Die Mitgliedstaaten gewährleisten, dass Fundstellendatensätze zu Gesichtsbildern von Verdächtigen, verurteilten Personen und, sofern nach innerstaatlichem Recht zulässig, Opfern aus ihren zur Verhütung, Aufdeckung und Untersuchung von Straftaten errichteten nationalen Datenbanken verfügbar sind.
- (2) Fundstellendatensätze zu Gesichtsbildern dürfen keine zusätzlichen Daten enthalten, aufgrund deren eine Person unmittelbar identifiziert werden kann.
- (3) Nicht identifizierte Gesichtsbilder sind als solche erkennbar .

Artikel 20
Automatisierte Abfrage von Gesichtsbildern

- (1) Die Mitgliedstaaten gestatten den nationalen Kontaktstellen anderer Mitgliedstaaten und Europol zur Verhütung, Aufdeckung und Untersuchung von Straftaten, die nach dem Recht des ersuchenden Mitgliedstaats mit einer Freiheitsstrafe im Höchstmaß von mindestens einem Jahr geahndet werden, den Zugriff auf die in ihren nationalen Datenbanken gespeicherten Fundstellendatensätze zu Gesichtsbildern, um automatisierte Abfragen durchzuführen.

Die in Unterabsatz 1 genannten Abfragen erfolgen nur im Rahmen von Einzelfällen und nur nach Maßgabe des nationalen Rechts des ersuchenden Mitgliedstaats .

Das Profiling gemäß Artikel 11 Absatz 3 der Richtlinie (EU) 2016/680 ist untersagt.

- (2) Die nationale Kontaktstelle des ersuchenden Mitgliedstaats kann entscheiden, eine Übereinstimmung zwischen zwei Gesichtsbildern zu bestätigen. Falls sie entscheidet die Übereinstimmung zwischen zwei Gesichtsbildern zu bestätigen, unterrichtet sie den ersuchten Mitgliedstaat und sorgt dafür, dass mindestens ein qualifizierter Mitarbeiter eine manuelle Überprüfung durchführt, um diese Übereinstimmung mit den vom ersuchten Mitgliedstaat erhaltenen Fundstellendatensätzen zu Gesichtsbildern zu bestätigen.

Artikel 21
Referenznummern von Gesichtsbildern

Die Referenznummern von Gesichtsbildern bestehen aus einer Kombination folgender Elemente:

- a) einer Referenznummer, die es den Mitgliedstaaten im Fall einer Übereinstimmung ermöglicht, weitere Daten und sonstige Informationen in ihren Datenbanken gemäß Artikel 19 abzurufen, um sie einem, mehreren oder allen anderen Mitgliedstaaten gemäß Artikel 47 oder Europol gemäß Artikel 49 Absatz 6 zu übermitteln;
- b) einer Referenznummer, die es Europol im Fall einer Übereinstimmung ermöglicht, weitere Daten und sonstige Informationen für die Zwecke von Artikel 48 Absatz 1 der vorliegenden Verordnung abzurufen, um sie einem, mehreren oder allen Mitgliedstaaten gemäß der Verordnung (EU) 2016/794 mitzuteilen;
- c) einem Code zur Angabe des Mitgliedstaats, dem die Gesichtsbilder vorliegen.

Artikel 22
Grundsätze des Austauschs von Gesichtsbildern

- (1) Die Mitgliedstaaten treffen geeignete Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität der an andere Mitgliedstaaten oder Europol übermittelten Gesichtsbilder, einschließlich ihrer Verschlüsselung. Europol trifft geeignete Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität der an Mitgliedstaaten übermittelten Gesichtsbilder, einschließlich ihrer Verschlüsselung

- (2) Jeder Mitgliedstaat und Europol stellen sicher, dass die von ihnen übermittelten Gesichtsbilder von ausreichender Qualität für einen automatisierten Abgleich sind. Die Kommission legt im Wege von Durchführungsrechtsakten einen Mindestqualitätsstandard fest, um den Abgleich von Gesichtsbildern zu ermöglichen. Ergibt sich aus dem Bericht nach Artikel 80 Absatz 7 ein hohes Risiko falscher Übereinstimmungen, so überprüft die Kommission diese Durchführungsrechtsakte.
- (3) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der einschlägigen europäischen oder internationalen Standards, die die Mitgliedstaaten und Europol für den Austausch von Gesichtsbildern verwenden müssen.
- (4) Diese in den Absätzen 2 und 3 genannten Durchführungsrechtsakte werden nach dem in Artikel 77 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 23

Abfragekapazitäten für Gesichtsbilder

- (1) Jeder Mitgliedstaat stellt sicher, dass seine Abfrageersuchen nicht die Abfragekapazitäten überschreiten, die der jeweilige ersuchte Mitgliedstaat oder Europol angegeben hat, um die Bereitschaft des Systems sicherzustellen und eine Systemüberlastung zu verhindern. Zu demselben Zweck stellt Europol sicher, dass ihre Abfrageersuchen nicht die Abfragekapazitäten überschreiten, die der jeweilige ersuchte Mitgliedstaat angegeben hat.

Die Mitgliedstaaten unterrichten die anderen Mitgliedstaaten, die Kommission, eu-LISA und Europol über ihre maximalen täglichen Abfragekapazitäten für identifizierte und nicht identifizierte Gesichtsbilder. Europol unterrichtet die Mitgliedstaaten, die Mitgliedstaaten, die Kommission und eu-LISA über ihre maximalen täglichen Abfragekapazitäten für identifizierte und nicht identifizierte Gesichtsbilder. Mitgliedstaaten oder Europol können diese Abfragekapazitäten jederzeit, auch in dringenden Fällen, vorübergehend oder dauerhaft erhöhen. Erhöht ein Mitgliedstaat diese maximalen Abfragekapazitäten, so teilt er den anderen Mitgliedstaaten, der Kommission, eu-LISA und Europol die neuen maximalen Abfragekapazitäten mit. Erhöht Europol diese maximalen Abfragekapazitäten, so teilt sie den Mitgliedstaaten, der Kommission und eu-LISA die neuen maximalen Abfragekapazitäten mit.

- (2) Zur Festlegung der Höchstzahl der pro Übermittlung für einen Abgleich akzeptierten Kandidaten und der Aufteilung ungenutzter Abfragekapazitäten zwischen den Mitgliedstaaten erlässt die Kommission Durchführungsrechtsakte nach dem in Artikel 77 Absatz 2 genannten Prüfverfahren.

Artikel 24

Regeln für Ersuchen und Antworten in Bezug auf Gesichtsbilder

- (1) Ein Ersuchen um eine automatisierte Abfrage von Gesichtsbildern enthält ausschließlich die folgenden Informationen:
 - a) Code des ersuchenden Mitgliedstaats;

- b) Datum, Uhrzeit und Kennnummer des Ersuchens;
 - c) die Fundstellendatensätze des Gesichtsbildes.
- (2) Eine Antwort auf ein Ersuchen gemäß Absatz 1 enthält ausschließlich folgende Informationen:
- a) Angabe, ob eine oder mehrere Übereinstimmungen oder keine Übereinstimmungen vorliegen;
 - b) Datum, Uhrzeit und Kennnummer des Ersuchens;
 - c) Datum, Uhrzeit und Kennnummer der Antwort;
 - d) Codes des ersuchenden und des ersuchten Mitgliedstaats;
 - e) Referenznummern der Gesichtsbilder des ersuchenden und des ersuchten Mitgliedstaats;
 - f) die übereinstimmenden Gesichtsbilder.
- (3) Die Mitgliedstaaten stellen sicher, dass die in Absatz 1 des vorliegenden Artikels genannten Ersuchen mit den Mitteilungen gemäß Artikel 74 übereinstimmen. Diese Mitteilungen sind in dem Handbuch gemäß Artikel 79 wiederzugeben.

ABSCHNITT 5

POLIZEIAKten

Artikel 25

Polizeiakten

- (1) Die Mitgliedstaaten können sich am automatisierten Austausch von Polizeiakten beteiligen. Zum Zwecke dieses Austauschs stellen die teilnehmenden Mitgliedstaaten sicher, dass nationale Polizeiaktennachweise verfügbar sind, die Datensätze mit biografischen Daten von Verdächtigen und verurteilten Personen aus ihren nationalen Datenbanken enthalten, die zur Verhütung, Aufdeckung und Untersuchung von Straftaten eingerichtet wurden. Diese Datensätze enthalten ausschließlich die folgenden Daten, sofern sie verfügbar sind:
- a) Vorname(n);
 - b) Familienname(n);
 - c) Aliasname(n) und früher verwendete(r) Name(n);
 - d) Geburtsdatum;
 - e) Staatsangehörigkeit(en);
 - f) Geburtsland;
 - g) Geschlecht.

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

Artikel 26

Automatisierte Abfrage von nationalen Polizeiakten nachweisen

Die am automatisierten Austausch von Polizeiakten teilnehmenden Mitgliedstaaten gestatten den nationalen Kontaktstellen anderer teilnehmender Mitgliedstaaten und Europol für die Verhütung, Aufdeckung und Untersuchung von Straftaten, die nach dem Recht des ersuchenden Mitgliedstaats mit einer Freiheitsstrafe im Höchstmaß von mindestens einem Jahr geahndet werden, den Zugriff auf Daten aus ihren nationalen Polizeiakten nachweisen, um automatisierte Abfragen durchzuführen.

Die in Absatz 1 genannten Abfragen erfolgen nur im Rahmen von Einzelfällen und nur nach Maßgabe des nationalen Rechts des ersuchenden Mitgliedstaats .

Artikel 27

Referenznummern von Polizeiakten

Die Referenznummern von Polizeiakten bestehen aus einer Kombination folgender Elemente:

- a) einer Referenznummer, die es den Mitgliedstaaten im Fall einer Übereinstimmung ermöglicht, biografische Daten und sonstige Informationen in ihren nationalen Polizeiakten nachweisen gemäß Artikel 25 abzurufen, um sie einem, mehreren oder allen anderen Mitgliedstaaten gemäß Artikel 44 zu übermitteln;
- b) einem Code zur Angabe des Mitgliedstaats, der im Besitz der Polizeiakten ist.

Artikel 28

Regeln für Ersuchen und Antworten in Bezug auf Polizeiakten

- (1) Ein Ersuchen um eine automatisierte Abfrage von nationalen Polizeiaktennachweisen enthält ausschließlich die folgenden Informationen:
- a) Code des ersuchenden Mitgliedstaats;
 - b) Datum, Uhrzeit und Kennnummer des Ersuchens;
 - c) die Daten gemäß Artikel 25, soweit sie verfügbar sind.
- (2) Die Antwort auf ein Ersuchen gemäß Absatz 1 enthält ausschließlich folgende Informationen:
- a) Angabe der Zahl der Übereinstimmungen ;
 - b) Datum, Uhrzeit und Kennnummer des Ersuchens;
 - c) Datum, Uhrzeit und Kennnummer der Antwort;
 - d) Codes des ersuchenden und des ersuchten Mitgliedstaats;
 - e) Referenznummern der Polizeiakten des ersuchenden und des ersuchten Mitgliedstaats.
- (3) Die Mitgliedstaaten stellen sicher, dass die in Absatz 1 des vorliegenden Artikels genannten Ersuchen mit den Mitteilungen gemäß Artikel 74 übereinstimmen. Diese Mitteilungen sind in dem Handbuch gemäß Artikel 79 wiederzugeben.

ABSCHNITT 6

GEMEINSAME BESTIMMUNGEN

Artikel 29

Vermisste Personen und nicht identifizierte menschliche Überreste

- (1) Wurde eine nationale Behörde durch nationale Legislativmaßnahmen gemäß Absatz 2 dazu ermächtigt, so darf sie automatisierte Abfragen unter Verwendung des Prüm-II-Rahmens ausschließlich zu folgenden Zwecken durchführen:
- a) Abfrage nach vermissten Personen im Zuge von strafrechtlichen Ermittlungen oder aus humanitären Gründen;
 - b) Identifizierung menschlicher Überreste.
- (2) Mitgliedstaaten, die die in Absatz 1 vorgesehene Möglichkeit nutzen möchten, benennen durch nationale Legislativmaßnahmen die für die dort genannten Zwecke zuständigen nationalen Behörden und legen die Verfahren, Bedingungen und Kriterien einschließlich der humanitären Gründe fest, für die automatisierte Abfragen nach vermissten Personen gemäß Absatz 1 Buchstabe a zulässig sind.

Artikel 30

Nationale Kontaktstellen

Jeder Mitgliedstaat benennt eine nationale Kontaktstelle oder mehrere nationale Kontaktstellen für die Zwecke der Artikel 6, 11, 16, 20 und 26.

Artikel 31

Durchführungsmaßnahmen

Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der technischen Ausgestaltung der Verfahren für die Mitgliedstaaten in Bezug auf die Artikel 6, 11, 16, 20 und 26. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 77 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 32

Verfügbarkeit des automatisierten Datenaustauschs auf nationaler Ebene

- (1) Die Mitgliedstaaten treffen alle notwendigen Vorkehrungen, damit die automatisierte Abfrage von DNA-Profilen, daktyloskopischen Daten, bestimmten Fahrzeugzulassungsdaten, Gesichtsbildern und Polizeiakten 24 Stunden täglich, an sieben Tagen pro Woche möglich ist.

- (2) Die nationalen Kontaktstellen unterrichten einander, die Kommission, eu-LISA und Europol unverzüglich über jede Nichtverfügbarkeit des automatisierten Datenaustauschs, sowie gegebenenfalls über etwaige technische Störungen, die diese Nichtverfügbarkeit verursacht haben.

Die nationalen Kontaktstellen vereinbaren gemäß dem geltenden Unionsrecht und den geltenden nationalen Rechtsvorschriften vorübergehende Alternativen für den Informationsaustausch, die verwendet werden, wenn der automatisierte Datenaustausch nicht verfügbar ist.

- (3) Ist der automatisierte Datenaustausch nicht verfügbar, stellen die nationalen Kontaktstellen sicher, dass dieser unverzüglich wiederhergestellt wird.

Artikel 33

Begründung für die Datenverarbeitung

- (1) Jeder Mitgliedstaat bewahrt die Begründungen der von seinen zuständigen Behörden durchgeführten Abfragen auf.

Europol bewahrt die Begründungen ihrer Abfragen auf.

- (2) Die in Absatz 1 genannten Begründungen enthalten folgende Angaben:
- a) Zweck der Abfrage, einschließlich einer Bezugnahme auf den konkreten Fall oder die konkrete Untersuchung und gegebenenfalls die Straftat;

- b) Angabe, ob die Abfrage einen Verdächtigen oder eine wegen einer Straftat verurteilte Person, ein Opfer einer Straftat, eine vermisste Person oder nicht identifizierte menschliche Überreste betrifft;
 - c) Angabe, ob die Abfrage darauf abzielt, eine Person zu identifizieren oder mehr Daten zu einer bekannten Person zu erhalten.
- (3) Die in Absatz 1 dieses Artikels genannten Begründungen müssen den in den Artikeln 18, 40 und 45 genannten Protokollen zugeordnet werden können. Diese Begründungen dürfen nur zur Beurteilung verwendet werden, ob die Abfragen verhältnismäßig und erforderlich für die Zwecke der Verhütung, Aufdeckung oder Untersuchung einer Straftat sind, und zwar im Rahmen der datenschutzrechtlichen Kontrolle, einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung, sowie im Rahmen der Sicherstellung der Datensicherheit und -integrität. Die Begründungen sind durch geeignete Maßnahmen gegen unbefugten Zugriff zu schützen und werden drei Jahre nach ihrer Erstellung gelöscht. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, werden sie gelöscht, sobald sie nicht mehr für das Kontrollverfahren benötigt werden.
- (4) Zur Beurteilung der Verhältnismäßigkeit und Erforderlichkeit von Abfragen zum Zwecke der Verhütung, Aufdeckung oder Untersuchung einer Straftat oder zur 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 55.

Artikel 34
Verwendung des universellen Nachrichtenformats

- (1) Bei der Entwicklung des in Artikel 35 dieser Verordnung genannten Routers und des Europäischen Polizeiaktennachweissystems (EPRIS) wird das in Artikel 38 der Verordnung (EU) 2019/818 eingerichtete universelle Nachrichtenformat (Universal Message Format, UMF) so weit wie möglich verwendet.
- (2) Für den gesamten automatisierten Datenaustausch gemäß dieser Verordnung wird der UMF-Standard so weit wie möglich verwendet.

Kapitel 3

Architektur

ABSCHNITT 1

ROUTER

Artikel 35

Router

- (1) Es wird ein Router eingerichtet, um die Herstellung von Verbindungen zwischen den Mitgliedstaaten und zwischen den Mitgliedstaaten und Europol zum Zwecke der Abfrage mit, des Abrufs von und der Bewertung (Scoring) von biometrischen Daten und des Abrufs alphanumerischer 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, 10 und 19 genannten nationalen Datenbanken und der Europol-Daten ermöglicht;
 - b) einem sicheren Kommunikationskanal zwischen der zentralen Infrastruktur und den zuständigen Behörden, die befugt sind, den Router gemäß Artikel 36 zu nutzen, und Europol;

- c) einer sicheren Kommunikationsinfrastruktur zwischen der zentralen Infrastruktur und dem Europäischen Suchportal, das durch Artikel 6 der Verordnung (EU) 2019/817 und Artikel 6 der Verordnung (EU) 2019/818 für die Zwecke des Artikels 39 eingerichtet wurde.

Artikel 36

Nutzung des Routers

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

Artikel 37

Prozesse

- (1) Die zuständigen Behörden, die gemäß Artikel 36 befugt sind, den Router zu nutzen, oder Europol ersuchen um eine Abfrage, indem sie dem Router biometrische Daten übermitteln. Der Router versendet das Abfrageersuchen an die Datenbanken aller oder bestimmter Mitgliedstaaten und die Europol-Daten gleichzeitig mit den vom Nutzer übermittelten Daten nach Maßgabe der jeweiligen Zugriffsrechte.

- (2) Nach Erhalt eines vom Router übermittelten Abfrageersuchens leitet jeder ersuchte Mitgliedstaat unverzüglich eine automatisierte Abfrage seiner Datenbanken ein. Nach Erhalt eines vom Router übermittelten Abfrageersuchens leitet Europol unverzüglich eine automatisierte Abfrage ihrer Datenbanken ein.
- (3) Sämtliche Übereinstimmungen infolge der Abfragen im Sinne des Absatzes 2 werden automatisch an den Router zurückgesendet. Der ersuchende Mitgliedstaat wird automatisch benachrichtigt, wenn keine Übereinstimmung vorliegt.
- (4) Der Router bringt die Antworten, sofern der ersuchende Mitgliedstaat dies beschließt und sofern anwendbar mittels eines Abgleichs der für die Abfrage verwendeten biometrischen Daten und der in den Antworten des ersuchten Mitgliedstaats oder der ersuchten Mitgliedstaaten oder Europols mitgeteilten biometrischen Daten in eine Rangfolge.
- (5) Der Router sendet die Liste der übereinstimmenden biometrischen Daten und ihrer Rangfolge (Scores) an den Nutzer des Routers zurück.
- (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 auf solche Abfragen und der technischen Vorschriften für den Abgleich und die Festlegung der Rangfolge der Übereinstimmung zwischen biometrischen Daten. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 77 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 38

Qualitätsprüfung

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

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

Artikel 39

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

- (1) Sind die benannten Behörden im Sinne des Artikels 4 Nummer 20 der Verordnung (EU) 2019/817 und des Artikels 4 Nummer 20 der Verordnung (EU) 2019/818 zur Nutzung des Routers gemäß Artikel 36 der vorliegenden Verordnung befugt, so können sie eine Abfrage der Datenbanken der Mitgliedstaaten und der Europol-Daten gleichzeitig mit einer Abfrage des durch Artikel 17 der Verordnung (EU) 2019/817 und Artikel 17 der Verordnung (EU) 2019/818 eingerichteten gemeinsamen Speichers für Identitätsdaten durchführen, sofern die einschlägigen Bedingungen des Unionsrechts erfüllt sind und die Abfrage nach Maßgabe ihrer Zugangsrechte durchgeführt wird. 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 dieser Abfragen werden über das Europäische Suchportal übermittelt.

Gleichzeitige Abfragen der Datenbanken der Mitgliedstaaten, der Europol-Daten und des gemeinsamen Speichers für Identitätsdaten werden nur vorgenommen, wenn berechtigter Grund zu der Annahme besteht, dass 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 führt Protokolle aller Datenverarbeitungsvorgänge im Router. Diese Protokolle enthalten folgende Angaben:
- ob ein Mitgliedstaat oder Europol um die Abfrage ersucht hat; wenn es ein Mitgliedstaat war, der um die Abfrage ersucht hat, der betroffene Mitgliedstaat;
 - Datum und Uhrzeit des Ersuchens;

- c) Datum und Uhrzeit der Antwort;
 - d) nationale Datenbanken oder Europol-Daten, an die ein Abfrageersuchen gerichtet wurde;
 - e) nationale Datenbanken oder Europol-Daten, die eine Antwort übermittelt haben;
 - f) die etwaige Bestätigung, dass eine gleichzeitige Abfrage des gemeinsamen Speichers für Identitätsdaten vorgenommen wurde.
- (2) Jeder Mitgliedstaat protokolliert die Abfragen, die die zur Nutzung des Routers ordnungsgemäß ermächtigten Mitarbeiter seiner zuständigen Behörden durchführen, und die Abfrageersuchen von anderen Mitgliedstaaten.
- Europol protokolliert die Abfragen seiner ordnungsgemäß ermächtigten Mitarbeiter.
- (3) Die in den Absätzen 1 und 2 genannten Protokolle werden nur zur Erhebung von Statistiken und zur datenschutzrechtlichen Kontrolle einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Wahrung der Datensicherheit und -integrität verwendet. Diese Protokolle sind durch geeignete Maßnahmen vor unbefugtem Zugriff zu schützen und drei Jahre nach ihrer Erstellung zu löschen. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, so 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 Verantwortlichen für die in Artikel 55 genannte Eigenkontrolle Zugang zu den Protokollen.

Artikel 41

Meldeverfahren bei technischer Nichtnutzbarkeit des Routers

- (1) Ist die Nutzung des Routers zur Abfrage einer oder mehrerer nationaler Datenbanken oder der Europol-Daten aufgrund eines Ausfalls des Routers technisch nicht möglich, so benachrichtigt eu-LISA die in Artikel 36 genannten Nutzer des Routers automatisch. eu-LISA ergreift unverzüglich geeignete Maßnahmen zur Behebung der Nichtnutzbarkeit des Routers.
- (2) Ist die Nutzung des Routers zur Abfrage einer oder mehrerer nationaler Datenbanken aufgrund eines Ausfalls der nationalen Infrastruktur eines Mitgliedstaats technisch nicht möglich, so benachrichtigt der betroffene Mitgliedstaat die anderen Mitgliedstaaten, die Kommission, eu-LISA und Europol automatisch. Der betroffene Mitgliedstaat ergreift unverzüglich geeignete Maßnahmen zur Behebung der technischen Nichtnutzbarkeit des Routers.
- (3) Ist die Nutzung des Routers zur Abfrage der Europol-Daten aufgrund eines Ausfalls der Infrastruktur von Europol technisch nicht möglich, so benachrichtigt Europol die Mitgliedstaaten, die Kommission und eu-LISA automatisch. Europol ergreift unverzüglich geeignete Maßnahmen zur Behebung der technischen Nichtnutzbarkeit des Routers.

ABSCHNITT 2

EPRIS

Artikel 42

EPRIS

- (1) Das Europäische Polizeiaktennachweissystem (EPRIS) wird hiermit eingerichtet. Für die in Artikel 26 genannte automatisierte Abfrage nationaler Polizeiaktennachweise verwenden die Mitgliedstaaten und Europol das EPRIS.
- (2) Das EPRIS setzt sich zusammen aus
 - a) einer dezentralen Infrastruktur in den Mitgliedstaaten einschließlich einer Suchfunktion, die die gleichzeitige Abfrage der nationalen Polizeiaktennachweise auf der Grundlage nationaler Datenbanken ermöglicht;
 - b) einer zentralen Infrastruktur, die die Suchfunktion unterstützt, die die gleichzeitige Abfrage nationaler Polizeiaktennachweise ermöglicht;
 - c) einem sicheren Kommunikationskanal zwischen der zentralen Infrastruktur, den Mitgliedstaaten und Europol.

Artikel 43

Verwendung des EPRIS

- (1) Für die über das EPRIS erfolgende Abfrage von nationalen Polizeiakten nachweisen werden mindestens zwei der folgenden Datensätze verwendet:
- a) Vorname(n);
 - b) Familienname(n);
 - c) Geburtsdatum.
- (2) Sofern verfügbar, können auch die folgenden Datensätze verwendet werden:
- a) Aliasname(n) und früher verwendete(r) Name(n);
 - b) Staatsangehörigkeit(en);
 - c) Geburtsland;
 - d) Geschlecht.
- (3) Die in Absatz 1 Buchstaben a und b sowie in Absatz 2 Buchstabe a genannten Daten werden pseudonymisiert.

Artikel 44

Prozesse

- (1) Wenn ein Mitgliedstaat oder Europol um eine Abfrage ersucht, übermittelt er die in Artikel 43 genannten Daten.

Das EPRIS versendet das Abfrageersuchen an die nationalen Polizeiaktennachweise der Mitgliedstaaten mit den vom ersuchenden Mitgliedstaat oder von Europol übermittelten Daten und gemäß dieser Verordnung.

- (2) Nach Eingang des vom EPRIS übermittelten Abfrageersuchens leitet jeder ersuchte Mitgliedstaat unverzüglich eine automatisierte Abfrage seines nationalen Polizeiaktennachweises ein.
- (3) Sämtliche bei einer Abfrage gemäß Absatz 1 in den nationalen Polizeiaktennachweisen des jeweiligen ersuchten Mitgliedstaats erzielte Übereinstimmungen werden automatisch an das EPRIS zurückgesendet.
- (4) Die Liste der Übereinstimmungen wird vom EPRIS automatisch an den ersuchenden Mitgliedstaat oder an Europol zurückgesandt. In der Liste der Übereinstimmungen werden die Qualität der Übereinstimmung und der Mitgliedstaat oder die Mitgliedstaaten angegeben, dessen bzw. deren Polizeiaktennachweise Daten enthalten, die zu der Übereinstimmung bzw. den Übereinstimmungen geführt haben.

- (5) Nach Eingang der Liste der Übereinstimmungen entscheidet der ersuchende Mitgliedstaat, welche Übereinstimmungen weiterverfolgt werden müssen, und übermittelt dem ersuchten Mitgliedstaat oder den ersuchten Mitgliedstaaten über SIENA ein Nachfolgeersuchen mit einer Begründung und den in Artikeln 25 und 27 genannten Daten sowie etwaigen weiteren sachdienlichen Informationen. Der ersuchte Mitgliedstaat oder die Mitgliedstaaten bearbeiten derartige Ersuchen unverzüglich, um zu entscheiden, ob die in seiner oder ihrer Datenbank gespeicherten Daten weitergegeben werden.
- (6) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung des technischen Verfahrens für die vom EPRIS durchgeführte Abfrage der Polizeiaktennachweise der Mitgliedstaaten und des Formates sowie der Höchstanzahl der Antworten. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 77 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 45

Protokollierung

- (1) Jeder teilnehmende Mitgliedstaat und Europol führt Protokolle über alle im EPRIS durchgeführten Datenverarbeitungsvorgänge. Diese Protokolle enthalten folgende Angaben:
- a) ob ein Mitgliedstaat oder Europol um die Abfrage ersucht hat; wenn es ein Mitgliedstaat war, der um die Abfrage ersucht hat, der betroffene Mitgliedstaat;
 - b) Datum und Uhrzeit des Ersuchens;
 - c) Datum und Uhrzeit der Antwort;

- d) nationale Datenbanken, an die ein Abfrageersuchen gerichtet wurde;
 - e) nationale Datenbanken, die eine Antwort übermittelt haben.
- (2) Jeder teilnehmende Mitgliedstaat protokolliert die Abfrageersuchen der ordnungsgemäß zur Nutzung des EPRIS ermächtigten Mitarbeiter seiner zuständigen Behörden. Europol protokolliert die Abfrageersuchen seiner ordnungsgemäß ermächtigten Mitarbeiter.
- (3) Die in den Absätzen 1 und 2 genannten Protokolle werden nur zur Erhebung von Statistiken und zur datenschutzrechtlichen Kontrolle einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Wahrung der Datensicherheit und -integrität verwendet. Diese Protokolle sind durch geeignete Maßnahmen vor unbefugtem Zugriff zu schützen und drei Jahre nach ihrer Erstellung zu löschen. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, so 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 Verantwortlichen für die in Artikel 55 genannte Eigenkontrolle Zugang zu den Protokollen.

Artikel 46

Meldeverfahren bei technischer Nichtnutzbarkeit des EPRIS

- (1) Ist die Nutzung des EPRIS zur Abfrage einer oder mehrerer nationaler Polizeiakten nachweise aufgrund eines Ausfalls der Infrastruktur von Europol technisch nicht möglich, so benachrichtigt Europol die Mitgliedstaaten automatisch. Europol ergreift unverzüglich Maßnahmen zur Behebung der technischen Nichtnutzbarkeit des EPRIS.
- (2) Ist die Nutzung des EPRIS zur Abfrage einer oder mehrerer nationaler Polizeiakten nachweise aufgrund eines Ausfalls der nationalen Infrastruktur eines Mitgliedstaats technisch nicht möglich, so benachrichtigt der betroffene Mitgliedstaat die anderen teilnehmenden Mitgliedstaaten, die Kommission und Europol automatisch. Die Mitgliedstaaten ergreifen unverzüglich Maßnahmen zur Behebung der technischen Nichtnutzbarkeit des EPRIS.

Kapitel 4

Datenauausch nach einer Übereinstimmung

Artikel 47

Austausch von Kerndaten

- (1) Innerhalb von 48 Stunden ist ein Kerndatensatz über den Router zurückzusenden, sofern alle folgenden Bedingungen erfüllt sind:
- a) Die in den Artikeln 6, 11 oder 20 genannten Verfahren ergeben eine Übereinstimmung zwischen den für die Abfrage verwendeten Daten und den in der Datenbank des ersuchten Mitgliedstaats bzw. der ersuchten Mitgliedstaaten gespeicherten Daten;
 - b) die Übereinstimmung gemäß Buchstabe a dieses Absatzes wurde von einem qualifizierten Mitarbeiter des ersuchenden Mitgliedstaats gemäß Artikel 6 Absatz 6, Artikel 11 Absatz 2 und Artikel 20 Absatz 2 oder, im Fall der in Artikel 6 Absatz 7 genannten DNA-Profile, vom ersuchten Mitgliedstaats manuell bestätigt;

- c) der ersuchende Mitgliedstaat oder, im Fall der in Artikel 6 Absatz 7 genannten DNA-Profile, der ersuchte Mitgliedstaat hat eine Sachverhaltsdarstellung und die zugrundeliegende Straftat unter Verwendung der gemeinsamen Tabelle der Kategorien von Straftaten, die in einem gemäß Artikel 11b Absatz 1 Buchstabe a des Rahmenbeschlusses 2009/315/JI zu erlassenden Durchführungsrechtsakt aufgeführt wird, übermittelt, damit die Verhältnismäßigkeit des Ersuchens, einschließlich der Schwere der Straftat, derentwegen eine Abfrage durchgeführt wurde, im Einklang mit dem nationalen Recht des Mitgliedstaats, der den Kerndatensatz bereitstellt, beurteilt werden kann.
- (2) Darf ein Mitgliedstaat nach Maßgabe des nationalen Rechts einen bestimmten Kerndatensatz erst nach Einholung einer Genehmigung durch eine Justizbehörde zur Verfügung stellen, so kann dieser Mitgliedstaat von der in Absatz 1 genannten Frist abweichen, soweit dies für die Einholung der Genehmigung erforderlich ist.
- (3) Der in Absatz 1 dieses Artikels genannte Kerndatensatz wird vom ersuchten Mitgliedstaat oder, im Fall der in Artikel 6 Absatz 7 genannten DNA-Profile, vom ersuchenden Mitgliedstaat zurückgesandt.
- (4) Betrifft die bestätigte Übereinstimmung identifizierte Daten einer Person, so enthält der in Absatz 1 genannte Kerndatensatz die folgenden Daten in dem Maße, wie sie verfügbar sind:
- a) Vorname(n);
 - b) Familienname(n);
 - c) Aliasname(n) und zuvor verwendete(r) Name(n);

- d) Geburtsdatum;
 - e) Staatsangehörigkeit(en);
 - f) Geburtsort und -land;
 - g) Geschlecht;
 - h) Datum und Ort der Erfassung der biometrischen Daten;
 - i) Straftat, zu der die biometrischen Daten erhoben wurden;
 - j) Aktenzeichen der Strafsache;
 - k) für die Strafsache zuständige Strafverfolgungsbehörde.
- (5) Betrifft die bestätigte Übereinstimmung nicht identifizierte Daten oder Spuren, so enthält der in Absatz 1 genannte Kerndatensatz die folgenden Daten, insoweit sie verfügbar sind:
- a) Datum und Ort der Erfassung der biometrischen Daten;
 - b) Straftat, zu der die biometrischen Daten erhoben wurden;
 - c) Aktenzeichen der Strafsache;
 - d) für die Strafsache zuständige Strafverfolgungsbehörde.
- (6) Die Rücksendung der Kerndaten durch den ersuchten Mitgliedstaat oder, im Fall der in Artikel 6 Absatz 6 genannten DNA-Profile, durch den ersuchenden Mitgliedstaat unterliegt der Entscheidung eines Menschen.

Kapitel 5

Europol

Artikel 48

Zugang der Mitgliedstaaten zu von Drittländern bereitgestellten und von Europol gespeicherten biometrischen Daten

- (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 Daten über den Router abfragen.
- (2) Führt eine Abfrage gemäß Absatz 1 zu einer Übereinstimmung zwischen den für die Abfrage verwendeten Daten, die von einem Drittland bereitgestellt und von Europol gespeichert wurden, so erfolgt die weitere Bearbeitung gemäß der Verordnung (EU) 2016/794.

Artikel 49

Zugang von Europol zu in den Datenbanken der Mitgliedstaaten gespeicherten Daten unter Verwendung von Drittländern bereitgestellten Daten

- (1) Soweit es für die Erreichung der in Artikel 3 der Verordnung (EU) 2016/794 festgelegten Ziele erforderlich ist, hat Europol im Einklang mit der genannten Verordnung und der vorliegenden Verordnung Zugang zu Daten, die von den Mitgliedstaaten in ihren nationalen Datenbanken und Polizeiaktennachweisen 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 Fahrzeugzulassungsdaten als Suchkriterium verwendet werden, werden mittels des EUCARIS durchgeführt.
- (4) Von Europol vorgenommene Abfragen, bei denen biografische Daten von in Artikel 25 genannten Verdächtigen und verurteilten Personen als Suchkriterium verwendet werden, werden über das EPRIS durchgeführt.
- (5) Europol führt Abfragen mit von Drittländern bereitgestellten Daten nach den Absätzen 1 bis 4 des vorliegenden Artikels nur durch, wenn es für die Wahrnehmung ihrer Aufgaben für die Zwecke des Artikels 18 Absatz 2 Buchstaben a und c der Verordnung (EU) 2016/794 erforderlich ist.
- (6) Ergibt sich bei den in den Artikeln 6, 11 oder 20 genannten Verfahren eine Übereinstimmung zwischen den für die Abfrage verwendeten Daten und den in der nationalen Datenbank des ersuchten Mitgliedstaats bzw. der ersuchten Mitgliedstaaten gespeicherten Daten, so unterrichtet Europol ausschließlich den betroffenen Mitgliedstaat bzw. die betroffenen Mitgliedstaaten.

Der ersuchte Mitgliedstaat entscheidet nach Bestätigung dieser Übereinstimmung durch Europol, ob er innerhalb von 48 Stunden einen Kerndatensatz über den Router übermittelt, sofern alle folgenden Bedingungen erfüllt sind:

- a) Eine Übereinstimmung gemäß Unterabsatz 1 wurde von einem qualifizierten Mitarbeiter von Europol manuell bestätigt;

- b) eine Sachverhaltsdarstellung und die zugrundeliegende Straftat wurden von Europol unter Verwendung der gemeinsamen Tabelle der Kategorien von Straftaten, die in einem gemäß Artikel 11b Absatz 1 Buchstabe a des Rahmenbeschlusses 2009/315/JI zu erlassenden Durchführungsrechtsakt aufgeführt wird, übermittelt, um die Verhältnismäßigkeit des Ersuchens, einschließlich der Schwere der Straftat, dererwegen eine Abfrage durchgeführt wurde, im Einklang mit dem nationalen Recht des Mitgliedstaats, der den Kerndatensatz bereitstellt, zu beurteilen;
- c) der Name des Drittlands, das die Daten bereitgestellt hat, wurde übermittelt.

Darf ein Mitgliedstaat nach Maßgabe des nationalen Rechts einen bestimmten Kerndatensatz erst nach Einholung einer Genehmigung durch eine Justizbehörde zur Verfügung stellen, so kann dieser Mitgliedstaat von der in Unterabsatz 2 genannten Frist abweichen, soweit dies für die Einholung der Genehmigung erforderlich ist.

Betrifft die bestätigte Übereinstimmung identifizierte Daten einer Person, so enthält der in Unterabsatz 2 genannte Kerndatensatz die folgenden Daten, insoweit sie verfügbar sind:

- a) Vorname(n);
- b) Familienname(n);
- c) Aliasname(n) und zuvor verwendete(r) Name(n);
- d) Geburtsdatum;

- e) Staatsangehörigkeit(en);
- f) Geburtsort und -land;
- g) Geschlecht.
- h) Datum und Ort der Erfassung der biometrischen Daten;
- i) Straftat, zu der die biometrischen Daten erhoben wurden;
- j) Aktenzeichen der Strafsache;
- k) für die Strafsache zuständige Strafverfolgungsbehörde.

Betrifft die bestätigte Übereinstimmung nicht identifizierte Daten oder Spuren, so enthält der in Unterabsatz 2 genannte Kerndatensatz die folgenden Daten, insoweit sie verfügbar sind:

- a) Datum und Ort der Erfassung der biometrischen Daten;
- b) Straftat, zu der die biometrischen Daten erhoben wurden;
- c) Aktenzeichen der Strafsache;
- d) für die Strafsache zuständige Strafverfolgungsbehörde.

Die Rücksendung der Kerndaten durch den ersuchten Mitgliedstaat unterliegt der Entscheidung eines Menschen.

- (7) Die Verwendung der Informationen, die Europol bei einer Abfrage nach diesem Artikel und durch den Austausch eines Kerndatensatzes 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 50

Zweck der Datenverarbeitung

- (1) Die Verarbeitung personenbezogener Daten, die von einem Mitgliedstaat oder Europol empfangen werden, ist nur für die Zwecke zulässig, für die die Daten von dem Mitgliedstaat, der die Daten bereitgestellt hat, nach Maßgabe dieser Verordnung übermittelt wurden. Eine Verarbeitung zu anderen Zwecken ist nur mit vorheriger Genehmigung des Mitgliedstaats, der die Daten bereitgestellt hat, zulässig.
- (2) Die Verarbeitung von Daten, die durch einen Mitgliedstaat oder Europol gemäß den Artikeln 6, 11, 16, 20 oder 26 übermittelt wurden, ist ausschließlich bei Bedarf zu folgenden Zwecken zulässig:
- a) Prüfung der dem Abgleich unterzogenen DNA-Profile, daktyloskopischen Daten, Fahrzeugzulassungsdaten, Gesichtsbilder oder Polizeiakten auf Übereinstimmungen;
 - b) Austausch eines Kerndatensatzes gemäß Artikel 47;
 - c) Vorbereitung und Einreichung eines polizeilichen oder justiziellen Amts- oder Rechtshilfeersuchens im Fall der Übereinstimmung;
 - d) Führung von Protokollen gemäß den Artikeln 18, 40 und 45.

- (3) Die von einem Mitgliedstaat oder Europol erhaltenen Daten werden nach der automatisierten Antwort auf eine Abfrage unverzüglich gelöscht, sofern die Weiterverarbeitung nicht für die in Absatz 2 genannten Zwecke erforderlich oder gemäß Absatz 1 zulässig ist.
- (4) Bevor die Mitgliedstaaten ihre nationalen Datenbanken mit dem Router oder dem EPRIS verbinden, führen sie eine in Artikel 27 der Richtlinie (EU) 2016/680 genannte Datenschutz-Folgenabschätzung durch und konsultieren je nach Sachlage die in Artikel 28 der genannten Richtlinie genannte Aufsichtsbehörde. Die Aufsichtsbehörde kann von ihren Befugnissen gemäß Artikel 47 der genannten Richtlinie im Einklang mit Artikel 28 Absatz 5 der genannten Richtlinie Gebrauch machen.

Artikel 51

Richtigkeit, Relevanz und Datenspeicherung

- (1) Die Mitgliedstaaten und Europol gewährleisten die Richtigkeit und die Relevanz der gemäß dieser Verordnung verarbeiteten personenbezogenen Daten. Stellen ein Mitgliedstaat oder Europol fest, dass Daten, die unrichtig oder nicht länger aktuell sind, oder Daten, die nicht hätten übermittelt werden dürfen, übermittelt worden sind, so teilen sie dies unverzüglich dem Mitgliedstaat, der die Daten erhalten hat, oder Europol mit. Alle betroffenen Mitgliedstaaten oder Europol müssen die Daten entsprechend unverzüglich berichtigen oder löschen. Haben der Mitgliedstaat, der die Daten erhalten hat, oder Europol Grund zu der Annahme, dass die mitgeteilten Daten unrichtig sind oder gelöscht werden sollten, so unterrichten sie unverzüglich den Mitgliedstaat, der die Daten bereitgestellt hat darüber.

- (2) Die Mitgliedstaaten und Europol treffen geeignete Maßnahmen zur Aktualisierung der für die Zwecke der vorliegenden Verordnung relevanten Daten.
- (3) Bestreitet eine betroffene Person die Richtigkeit von Daten, die sich im Besitz eines Mitgliedstaats oder von Europol befinden, und kann die Richtigkeit von dem betreffenden Mitgliedstaat oder von Europol nicht zuverlässig festgestellt werden und wird von der betroffenen Person beantragt, so werden die betreffenden Daten mit einer Kennzeichnung versehen. Ist eine solche Kennzeichnung vorhanden, dürfen die Mitgliedstaaten oder Europol sie nur mit Zustimmung der betroffenen Person oder aufgrund einer Entscheidung des zuständigen Gerichts, der Aufsichtsbehörde oder, sofern relevant, des Europäischen Datenschutzbeauftragten entfernen.
- (4) 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) nach Ablauf der im nationalen Recht des Mitgliedstaats, der die Daten übermittelt hat, vorgesehenen Höchstfrist für die Aufbewahrung der Daten, wenn dieser Mitgliedstaat, den Mitgliedstaat, der die Daten erhalten hat, oder Europol zum Zeitpunkt der Übermittlung der Daten über diese Höchstfrist informiert hat; oder
 - c) nach Ablauf der in der Verordnung (EU) 2016/794 festgelegten Höchstfrist für die Aufbewahrung von Daten.

Besteht Grund zu der Annahme, dass die Löschung von Daten die Interessen der betroffenen Person beeinträchtigen würde, so werden diese Daten nicht gelöscht, sondern ihre Verarbeitung wird eingeschränkt. Wurde die Verarbeitung der Daten eingeschränkt, dürfen sie nur für den Zweck, für den ihre Löschung unterblieben ist, verarbeitet werden.

Artikel 52
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 im Sinne von Artikel 3 Nummer 12 der Verordnung (EU) 2018/1725 für die Verarbeitung von personenbezogenen Daten über das EPRIS.

Artikel 53
Sicherheit der Verarbeitung

- (1) Die zuständigen Behörden der Mitgliedstaaten, eu-LISA und Europol gewährleisten die Sicherheit der Verarbeitung personenbezogener Daten gemäß dieser Verordnung. Die zuständigen Behörden der Mitgliedstaaten, eu-LISA und Europol 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 und der zugehörigen Kommunikationsinfrastruktur zu gewährleisten.

- (3) eu-LISA ergreift die erforderlichen Maßnahmen in Bezug auf den Router und Europol ergreift die erforderlichen Maßnahmen in Bezug auf das EPRIS, um
- a) die Daten physisch zu schützen, unter anderem durch Aufstellung von Notfallplänen für den Schutz der kritischen Infrastruktur;
 - 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 mithilfe von Datenübertragungsgeräten automatisierte Datenverarbeitungssysteme benutzen;
 - g) sicherzustellen, dass die zum Zugriff auf den Router oder 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 mithilfe von Datenübertragungsgeräten übermittelt werden können;

- 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 zum oder vom EPRIS oder während des Transports von Datenträgern zu verhindern, insbesondere durch geeignete Verschlüsselungsverfahren;
- k) sicherzustellen, dass eingesetzte Systeme im Störungsfall für den Normalbetrieb wiederhergestellt werden können;
- l) die Zuverlässigkeit sicherzustellen, indem dafür Sorge getragen wird, dass etwaige Funktionsstörungen des Routers oder 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.

Die in Unterabsatz 1 genannten erforderlichen Maßnahmen umfassen einen Sicherheitsplan, einen Notfallplan zur Aufrechterhaltung des Geschäftsbetriebs und einen Notfallwiederherstellungsplan.

Artikel 54
Sicherheitsvorfälle

- (1) Jedes Ereignis, das sich auf die Sicherheit des Routers oder des EPRIS auswirkt oder auswirken kann und im Router oder im EPRIS gespeicherte Daten beschädigen oder ihren Verlust herbeiführen kann, ist als Sicherheitsvorfall anzusehen; dies gilt insbesondere, wenn möglicherweise ein unbefugter Datenzugriff erfolgt ist oder die Verfügbarkeit, die Integrität und die Vertraulichkeit von Daten tatsächlich oder möglicherweise nicht mehr gewährleistet gewesen ist.
- (2) Bei einem Sicherheitsvorfall, der den Router betrifft, arbeiten eu-LISA und die betroffenen Mitgliedstaaten oder Europol zusammen, damit eine rasche, wirksame und angemessene Reaktion sichergestellt ist.
- (3) Bei einem Sicherheitsvorfall, der das EPRIS betrifft, arbeiten die betroffenen Mitgliedstaaten und Europol zusammen, damit eine rasche, wirksame und angemessene Reaktion sichergestellt ist.
- (4) Die Mitgliedstaaten melden ihren zuständigen Behörden unverzüglich alle Sicherheitsvorfälle.

Unbeschadet des Artikels 92 der Verordnung (EU) 2018/1725 meldet eu-LISA im Fall eines Sicherheitsvorfalls in Bezug auf die zentrale Infrastruktur des Routers dem Cybersicherheitsdienst für die Organe, Einrichtungen und sonstigen Stellen der Union (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 Voraberkennung, eine geeignete Reaktion oder geeignete Abhilfemaßnahmen ermöglichen, werden dem CERT-EU unverzüglich mitgeteilt.

Unbeschadet des Artikels 34 der Verordnung (EU) 2016/794 und des Artikels 92 der Verordnung (EU) 2018/1725 im Fall eines Sicherheitsvorfalls in Bezug auf die zentrale Infrastruktur des EPRIS 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 Voraberkennung, eine geeignete Reaktion oder geeignete Abhilfemaßnahmen ermöglichen, werden dem CERT-EU unverzüglich mitgeteilt.

- (5) 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.

- (6) 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 55

Eigenkontrolle

- (1) Die Mitgliedstaaten stellen sicher, dass jede zur Anwendung des Prüm-II-Rahmens befugte Behörde die erforderlichen Maßnahmen zur Einhaltung dieser Verordnung trifft und erforderlichenfalls mit der Aufsichtsbehörde zusammenarbeitet. Europol ergreift die erforderlichen Maßnahmen, um zu überwachen, ob sie diese Verordnung einhält, und arbeitet erforderlichenfalls mit dem Europäischen Datenschutzbeauftragten zusammen.
- (2) Die Verantwortlichen treffen die erforderlichen Maßnahmen, um die Ordnungsgemäßheit der Datenverarbeitung gemäß dieser Verordnung wirksam zu überwachen, unter anderem durch häufige Überprüfung der gemäß den Artikeln 18, 40 und 45 zu erstellenden Protokolle. Sie arbeiten erforderlichenfalls und je nach Sachlage mit den Aufsichtsbehörden oder dem Europäischen Datenschutzbeauftragten zusammen.

Artikel 56

Sanktionen

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

Artikel 57

Haftung

Verursacht eine Verletzung der in dieser Verordnung festgelegten Pflichten durch einen Mitgliedstaat oder, bei der Durchführung von Abfragen gemäß Artikel 49, durch Europol einen Schaden am Router oder am EPRIS, haftet dieser Mitgliedstaat oder Europol für den entstandenen Schaden, sofern und soweit es eu-LISA, Europol oder ein anderer durch diese Verordnung gebundener Mitgliedstaat nicht versäumt haben, angemessene Maßnahmen zur Verhinderung des Schadens oder zur Verringerung seiner Auswirkungen zu ergreifen.

Artikel 58

Prüfungen durch den Europäischen Datenschutzbeauftragten

- (1) Der Europäische Datenschutzbeauftragte trägt dafür Sorge, dass die durch eu-LISA und Europol für die Zwecke der vorliegenden 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 Stelle der Union übermittelt. eu-LISA und Europol 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 all ihren Räumlichkeiten. Dieser Absatz gilt unbeschadet der Befugnisse des Europäischen Datenschutzbeauftragten gemäß Artikel 58 der Verordnung (EU) 2018/1725 und im Hinblick auf Europol gemäß Artikel 43 Absatz 3 der Verordnung (EU) 2016/794.

Artikel 59

Zusammenarbeit zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten

- (1) Die Aufsichtsbehörden und der Europäische Datenschutzbeauftragte arbeiten — jeweils innerhalb ihres Kompetenzbereichs — im Rahmen ihrer jeweiligen Zuständigkeiten aktiv zusammen, um für eine koordinierte Aufsicht der Anwendung dieser Verordnung zu sorgen, insbesondere wenn der Europäische Datenschutzbeauftragte oder eine Aufsichtsbehörde größere Diskrepanzen zwischen den Verfahrensweisen der Mitgliedstaaten feststellt oder möglicherweise unrechtmäßige Übermittlungen über die Kommunikationskanäle des Prüm-II-Rahmens bemerkt.
- (2) In den in Absatz 1 genannten Fällen wird eine koordinierte Aufsicht gemäß Artikel 62 der Verordnung (EU) 2018/1725 sichergestellt.

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

Artikel 60

Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen

Ein Mitgliedstaat übermittelt gemäß dieser Verordnung erhobene personenbezogene Daten nur dann an ein Drittland oder eine internationale Organisation, wenn dies im Einklang mit Kapitel V der Richtlinie (EU) 2016/680 steht und unter der Voraussetzung, dass der ersuchte Mitgliedstaat vor der Übermittlung seine Genehmigung erteilt hat.

Europol übermittelt personenbezogene Daten, die sie gemäß dieser Verordnung erhalten hat, nur dann an ein Drittland oder eine internationale Organisation, wenn die in Artikel 25 der Verordnung (EU) 2016/794 festgelegten Voraussetzungen erfüllt sind und der ersuchte Mitgliedstaat vor der Übermittlung seine Genehmigung erteilt hat.

Artikel 61

Bezug zu anderen Rechtsakten zum Datenschutz

Jedwede Verarbeitung personenbezogener Daten für die Zwecke dieser Verordnung erfolgt im Einklang mit diesem Kapitel und, sofern anwendbar, der Richtlinie (EU) 2016/680 oder der Verordnungen (EU) 2018/1725, (EU) 2016/794 oder (EU) 2016/679.

Kapitel 7

Verantwortlichkeiten

Artikel 62

Verantwortlichkeiten in Bezug auf die Sorgfaltspflicht

Die Mitgliedstaaten und Europol prüfen mit der gebotenen Sorgfalt, ob der automatisierte Datenaustausch unter den in Artikel 2 genannten Zweck des Prüm-II-Rahmens fällt und ob die darin festgelegten Bedingungen, insbesondere in Bezug auf die Grundrechte, erfüllt sind.

Artikel 63

Schulungen

Ermächtigte Mitarbeiter der zuständigen nationalen Behörden der Mitgliedstaaten, der nationalen Aufsichtsbehörden und von Europol erhalten je nach Zuständigkeit angemessene Ressourcen und Schulungen, auch zum Datenschutz und zur genauen Überprüfung von Übereinstimmungen, damit sie die Aufgaben im Rahmen dieser Verordnung wahrnehmen können.

Artikel 64

Verantwortlichkeiten der Mitgliedstaaten

- (1) Jeder Mitgliedstaat ist verantwortlich für
 - a) die Anbindung an die Infrastruktur des Routers;

- b) die Integration seiner bestehenden nationalen Systeme und Infrastrukturen mit dem Router;
- c) die Organisation, die Verwaltung, den Betrieb und die Instandhaltung ihrer bestehenden nationalen Infrastruktur und ihrer Anbindung an den Router;
- d) ihre Anbindung an die Infrastruktur des EPRIS;
- e) die Integration seiner bestehenden nationalen Systeme und Infrastrukturen in das EPRIS;
- f) die Organisation, die Verwaltung, den Betrieb und die Instandhaltung ihrer bestehenden nationalen Infrastruktur und ihrer Anbindung an das EPRIS;
- g) die Verwaltung und Regelung des Zugangs der ordnungsgemäß ermächtigten Mitarbeiter seiner zuständigen Behörden zum Router gemäß dieser Verordnung sowie die Erstellung und regelmäßige Aktualisierung einer Liste dieser Mitarbeiter und ihrer Profile;
- h) die Verwaltung und Regelung des Zugangs der ordnungsgemäß ermächtigten Mitarbeiter seiner zuständigen Behörden zum EPRIS gemäß dieser Verordnung sowie die Erstellung und regelmäßige Aktualisierung einer Liste dieser Mitarbeiter und ihrer Profile;
- i) die Verwaltung und Regelung des Zugangs der ordnungsgemäß ermächtigten Mitarbeiter seiner zuständigen Behörden zum EUCARIS gemäß dieser Verordnung sowie die Erstellung und regelmäßige Aktualisierung einer Liste dieser Mitarbeiter und ihrer Profile;
- j) die manuelle Bestätigung einer in Artikel 6 Absatz 6, Artikel 6 Absatz 7, Artikel 11 Absatz 2 und Artikel 20 Absatz 2 genannten Übereinstimmung durch einen qualifizierten Mitarbeiter;

- k) die Sicherstellung der Verfügbarkeit der für den Datenaustausch erforderlichen Daten gemäß den Artikeln 5, 10, 16, 19 und 25;
 - l) den Austausch von Informationen gemäß den Artikeln 6, 11, 16, 20 und 26;
 - m) die Berichtigung, Aktualisierung oder Löschung aller von einem ersuchten Mitgliedstaat eingegangenen Daten innerhalb von 48 Stunden nach der Mitteilung des ersuchten Mitgliedstaats, dass die übermittelten Daten unrichtig sind 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 Behörden an den Router, an das EPRIS und an das EUCARIS verantwortlich.

Artikel 65

Verantwortlichkeiten von Europol

- (1) Europol ist für die Verwaltung und die Regelung des Zugangs seiner ordnungsgemäß ermächtigten Mitarbeiter zum Router, zum EPRIS und zum EUCARIS im Einklang mit dieser Verordnung verantwortlich.
- (2) Europol ist 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) Unbeschadet der Abfragen durch Europol gemäß Artikel 49 hat Europol keinen Zugang zu den über das EPRIS verarbeiteten personenbezogenen Daten.
- (5) 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 ist für die technische Verwaltung des EPRIS zuständig. 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 täglich, an sieben Tagen pro Woche ununterbrochene Dienste zu bieten. Dazu gehören die Wartungsarbeiten und technischen Entwicklungen, die erforderlich sind, damit die Funktionen des EPRIS gemäß den technischen Spezifikationen, insbesondere in Bezug auf die Reaktionszeit für Abfragen der nationalen Datenbanken, mit zufriedenstellender technischer Qualität genutzt werden können.

- (6) Europol führt Schulungen über die technische Nutzung des EPRIS durch.
- (7) Europol ist für Verfahren gemäß den Artikeln 48 und 49 verantwortlich.

Artikel 66

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

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

- (2) Der Router wird an ihren technischen Standorten von eu-LISA betrieben und bietet die in dieser Verordnung vorgesehenen Funktionen gemäß den in Artikel 67 Absatz 1 festgelegten Bedingungen für die Sicherheit, Verfügbarkeit, Qualität und Leistung.
- (3) eu-LISA ist verantwortlich für die Entwicklung des Routers sowie für jegliche technischen Anpassungen, die für den Betrieb des Routers erforderlich sind.
- (4) eu-LISA hat keinen Zugang zu den über den Router verarbeiteten personenbezogenen Daten.
- (5) eu-LISA bestimmt die Konzeption der physischen Architektur des Routers einschließlich seiner sicheren Kommunikationsinfrastruktur, legt die technischen Spezifikationen fest und bestimmt seine Weiterentwicklung in Bezug auf die zentrale Infrastruktur und die sichere Kommunikationsinfrastruktur. Der Verwaltungsrat von eu-LISA nimmt die Gestaltung vorbehaltlich einer befürwortenden Stellungnahme der Kommission an. eu-LISA nimmt zudem etwaige erforderlichen Anpassungen der Interoperabilitätskomponenten vor, die für die Herstellung des Routers notwendig und in dieser Verordnung vorgesehen sind.
- (6) 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.
- (7) 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 regelmäßig zusammen. Er stellt die angemessene Verwaltung der Konzept- und Entwicklungsphase des Routers sicher.

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

Die in Artikel 78 genannte Beratergruppe für Interoperabilität tritt bis zur Inbetriebnahme des Routers regelmäßig zusammen. Nach jeder Zusammenkunft erstattet sie dem Programmverwaltungsrat 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 67

Verantwortlichkeiten von eu-LISA nach der Inbetriebnahme des Routers

- (1) Nach der Inbetriebnahme des Routers übernimmt eu-LISA die technische Verwaltung der zentralen Infrastruktur des Routers, einschließlich ihrer Wartung und technologischen Weiterentwicklung. 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 täglich, an sieben Tagen pro Woche ununterbrochene Dienste gemäß dieser Verordnung zu bieten. Dazu gehören die Wartungsarbeiten und technischen Anpassungen, die erforderlich sind, um das Funktionieren des Routers gemäß den technischen Spezifikationen sicherzustellen, insbesondere in Bezug auf die Verfügbarkeit und auf die Reaktionszeit für Abfragen der nationalen Datenbanken und von Europol-Daten, mit zufriedenstellender technischer Qualität.

Der Router wird so entwickelt und verwaltet, dass ein schneller, effizienter und kontrollierter Zugang, eine uneingeschränkte und ununterbrochene Verfügbarkeit und eine Reaktionszeit sichergestellt 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 Rates¹⁸ 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 im Router 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 erfüllt Aufgaben im Zusammenhang mit der Durchführung von Schulungen zur technischen Nutzung des Routers.

¹⁸

ABl. L 56 vom 4.3.1968, S. 1.

Kapitel 8

Änderungen anderer bestehender Instrumente

Artikel 68

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

- (1) In dem Beschluss 2008/615/JI werden Artikel 1 Buchstabe a, 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 75 Absatz 1 festgelegten Geltungsbereich der sich auf den Router beziehenden Bestimmungen dieser Verordnung ersetzt. Daher werden Artikel 1 Buchstabe a, die Artikel 2 bis 6 sowie Kapitel 2 Abschnitte 2 und 3 des Beschlusses 2008/615/JI ab dem in Artikel 75 Absatz 1 festgelegten Geltungsbereich 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 75 Absatz 1 festgelegten Geltungsbereich 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 75 Absatz 1 festgelegten Geltungsbereich der sich auf den Router beziehenden Bestimmungen dieser Verordnung gestrichen.

Artikel 69

Änderung der Verordnung (EU) 2018/1726

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

1. Folgender Artikel wird eingefügt:

„Artikel 8d

Aufgaben im Zusammenhang mit dem Prüm-II-Router

In Bezug auf den Prüm-II-Router erfüllt die Agentur die ihr durch die Verordnung (EU)

.../... des Europäischen Parlaments und des Rates^{*+} übertragenen Aufgaben.

* Verordnung (EU) 2024/... des Europäischen Parlaments und des Rates vom ... über die automatisierte Abfrage und den Austausch von Daten für die polizeiliche Zusammenarbeit und 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 (Prüm-II-Verordnung) (ABl. L ..., vom ... ELI: ...);“

2. Artikel 17 Absatz 3 Unterabsatz 2 erhält folgende Fassung:

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

+ ABl.: Bitte im Text die Nummer der im Dokument PE-CONS xx/xx (2021/0410(COD)) enthaltenen Verordnung und in der Fußnote die Nummer, das Datum, den Titel und die Amtsblattfundstelle der genannten Verordnung einfügen.

3. Artikel 19 Absatz 1 wird wie folgt geändert:

a) Folgender Buchstabe wird eingefügt:

„eeb) Berichte über den Stand der Entwicklung des Prüm-II-Routers gemäß Artikel 80 Absatz 2 der Verordnung (EU) .../...⁺ anzunehmen.“

b) Buchstabe ff erhält folgende Fassung:

„ff) nimmt die Berichte über die technische Funktionsweise der folgenden Systeme an

i) SIS nach Artikel 60 Absatz 7 der Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates^{*} und Artikel 74 Absatz 8 der Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates^{**},

ii) VIS nach Artikel 50 Absatz 3 der Verordnung (EG) Nr. 767/2008 und Artikel 17 Absatz 3 des Beschlusses 2008/633/JI,

iii) EES nach Artikel 72 Absatz 4 der Verordnung (EU) 2017/2226,

iv) ETIAS nach Artikel 92 Absatz 4 der Verordnung (EU) 2018/1240,

v) ECRIS-TCN und der ECRIS-Referenzimplementierung nach Artikel 36 Absatz 8 der Verordnung (EU) 2019/816,

⁺ ABl.: Bitte in den Text die Nummer der Verordnung in Dokument PE-CONS 75/23 (2021/0410(COD)) einfügen.

- vi) die Interoperabilitätskomponenten nach Artikel 78 Absatz 3 der Verordnung (EU) 2019/817 und Artikel 74 Absatz 3 der Verordnung (EU) 2019/818;
- vii) e-CODEX-System nach Artikel 16 Absatz 1 der Verordnung (EU) 2022/850;
- viii) die Plattform für die Zusammenarbeit gemeinsamer Ermittlungsgruppen gemäß Artikel 26 Absatz 6 der Verordnung (EU) 2023/969;
- ix) der Prüm-II-Router nach Artikel 80 Absatz 5 der Verordnung (EU) .../...⁺;

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

⁺ ABl.: Bitte in den Text die Nummer der Verordnung in Dokument PE-CONS 75/23 (2021/0410(COD)) einfügen.

c) Buchstabe hh erhält folgende Fassung:

„hh) förmliche Stellungnahmen zu den Berichten des Europäischen Datenschutzbeauftragten über seine Überprüfungen nach Artikel 56 Absatz 2 der Verordnung (EU) 2018/1861, Artikel 42 Absatz 2 der Verordnung (EG) Nr. 767/2008 und Artikel 31 Absatz 2 der Verordnung (EU) Nr. 603/2013, Artikel 56 Absatz 2 der Verordnung (EU) 2017/2226, Artikel 67 der Verordnung (EU) 2018/1240, Artikel 29 Absatz 2 der Verordnung (EU) 2019/816, Artikel 52 der Verordnungen (EU) 2019/817 und (EU) 2019/818 und Artikel 58 Absatz 1 der Verordnung (EU) .../...⁺ anzunehmen und für geeignete Folgemaßnahmen zu diesen Überprüfungen zu sorgen;“

⁺ ABI.: Bitte im Text die Nummer der im Dokument PE-CONS 75/23 (2021/0410(COD)) enthaltenen Verordnung einfügen.

Artikel 70

Änderungen der Verordnung (EU) 2019/817

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

- „d) eine sichere Kommunikationsinfrastruktur zwischen dem ESP und dem durch die Verordnung (EU) .../... des Europäischen Parlaments und des Rates^{*+} eingerichteten Router.

* Verordnung (EU) 2024/... des Europäischen Parlaments und des Rates vom ... über die automatisierte Abfrage und den Austausch von Daten für die polizeiliche Zusammenarbeit und 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 (Prüm-II-Verordnung) (ABl. L ... vom ..., ELI: ...)“.

+ ABl.: Bitte im Text die Nummer der im Dokument PE-CONS 75/23 (2021/0410(COD)) enthaltenen Verordnung und in der Fußnote die Nummer, das Datum, den Titel und die Amtsblattfundstelle der genannten Verordnung einfügen.

Artikel 71

Änderungen der Verordnung (EU) 2019/818

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

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

- „d) eine sichere Kommunikationsinfrastruktur zwischen dem ESP und dem durch die Verordnung (EU) .../... des Europäischen Parlaments und des Rates^{*+} eingerichteten Router.

* Verordnung (EU) 2024/... des Europäischen Parlaments und des Rates vom ... über die automatisierte Abfrage und den Austausch von Daten für die polizeiliche Zusammenarbeit und 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 (Prüm-II-Verordnung) (ABl. L ... vom ... ELI: ...)“

+ ABl.: Bitte im Text die Nummer der im Dokument PE-CONS 75/23 (2021/0410(COD)) enthaltenen Verordnung und in der Fußnote die Nummer, das Datum, den Titel und die Amtsblattfundstelle der genannten Verordnung einfügen.

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 und 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 der Verordnung (EU) .../...⁺.
- (2) eu-LISA sorgt an ihren technischen Standorten für die Einrichtung, die Implementierung und das Hosting des CRRS, der logisch nach den EU-Informationssystemen getrennt die in Artikel 74 der Verordnung (EU) 2018/1862 und Artikel 32 der Verordnung (EU) 2019/816 genannten Daten und Statistiken enthält. eu-LISA erhebt auch die Daten und Statistiken des in Artikel 72 Absatz 1 der Verordnung (EU) .../...⁺ 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 72 Absatz 1 der Verordnung (EU) .../...⁺ genannten Behörden ausschließlich zu Berichterstattungs- und Statistikzwecken gewährt.“

⁺ ABI.: Bitte in den Text die Nummer der Verordnung in Dokument PE-CONS 75/23 (2021/0410(COD)) einfügen.

Kapitel 9

Schlussbestimmungen

Artikel 72

Berichte und Statistiken

- (1) Erforderlichenfalls haben die dazu ordnungsgemäß ermächtigten Mitarbeiter der zuständigen Behörden der Mitgliedstaaten, der Kommission, von eu-LISA und von Europol ausschließlich zur Erstellung von Berichten und Statistiken Zugriff auf die folgenden Daten zum Router, soweit sie relevant sind:
- a) die Zahl der Abfragen je Mitgliedstaat und die Zahl der Abfragen von Europol je Datenkategorie;
 - b) die Zahl der Abfragen in den einzelnen angeschlossenen Datenbanken;
 - c) die Zahl der Übereinstimmungen mit der Datenbank der einzelnen Mitgliedstaaten je Datenkategorie;
 - d) die Zahl der Übereinstimmungen mit Europol-Daten je Datenkategorie;
 - e) die Zahl der bestätigten Übereinstimmungen, bei denen Kerndaten ausgetauscht wurden,
 - f) die Zahl der bestätigten Übereinstimmungen, bei denen keine Kerndaten ausgetauscht wurden;
 - g) die Zahl der über den Router erfolgten Abfragen im gemeinsamen Speicher für Identitätsdaten; und

- h) die Zahl der Übereinstimmungen nach Datentyp:
 - i) identifizierte Daten (Person) – nicht identifizierte Daten (Spur);
 - ii) nicht identifizierte Daten (Spur) – identifizierte Daten (Person);
 - iii) nicht identifizierte Daten (Spur) – nicht identifizierte Daten (Spur);
 - iv) identifizierte Daten (Person) – identifizierte Daten (Person).

Die Identifizierung einzelner Personen auf der Grundlage der in Unterabsatz 1 genannten Daten darf nicht möglich sein.

- (2) Die dazu ordnungsgemäß ermächtigten Mitarbeiter der zuständigen Behörden der Mitgliedstaaten, der Kommission und Europol haben ausschließlich zur Erstellung von Berichten und Statistiken Zugriff auf die folgenden Daten zum EUCARIS:

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

Die Identifizierung einzelner Personen auf der Grundlage der in Unterabsatz 1 genannten Daten darf nicht möglich sein.

- (3) Die dazu ordnungsgemäß ermächtigten Mitarbeiter der zuständigen Behörden der Mitgliedstaaten, der Kommission und Europol haben ausschließlich zur Erstellung von Berichten und Statistiken Zugriff auf die folgenden Daten zum EPRIS:
- a) die Zahl der Abfragen je Mitgliedstaat und die Zahl der Abfragen von Europol;
 - b) die Zahl der Abfragen in den einzelnen angeschlossenen Polizeiaktennachweisen und
 - c) die Zahl der Übereinstimmungen mit der Datenbank der einzelnen Mitgliedstaaten.

Die Identifizierung einzelner Personen auf der Grundlage der in Unterabsatz 1 genannten Daten darf nicht möglich sein.

- (4) eu-LISA speichert die in Absatz 1 des vorliegenden Artikels genannten Daten in dem gemäß Artikel 39 der Verordnung (EU) 2019/818 eingerichteten zentralen Speicher für Berichte und Statistiken. Europol speichert die in Absatz 3 genannten Daten. Diese Daten müssen es den zuständigen Behörden der Mitgliedstaaten, der Kommission, eu-LISA und Europol ermöglichen, anpassbare Berichte und Statistiken einzuholen, um die Effizienz der Zusammenarbeit der Strafverfolgungsbehörden zu verbessern.

Artikel 73

Kosten

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

(2) Die Kosten im Zusammenhang mit der Integration der bestehenden nationalen Infrastruktur, ihrer Anbindung an den Router und das EPRIS und der Einrichtung nationaler Gesichtsbilddatenbanken und nationaler Polizeiaktennachweise 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, Betriebs und Wartung nationaler Kommunikationsnetze.

(3) Jeder Mitgliedstaat trägt die Kosten, die ihm aus der Verwaltung, der Verwendung und der Pflege des EUCARIS entstehen.

(4) Jeder Mitgliedstaat trägt die Kosten, die ihm aus der Verwaltung, Verwendung und Instandhaltung seiner Verbindungen zum Router und zum EPRIS entstehen.

Artikel 74
Mitteilungen

- (1) Die Mitgliedstaaten teilen eu-LISA die in Artikel 36 genannten zuständigen Behörden mit. Diese Behörden dürfen den Router nutzen oder Zugang zum Router haben.
- (2) eu-LISA teilt der Kommission den erfolgreichen Abschluss der in Artikel 75 Absatz 1 Buchstabe b genannten Tests mit.
- (3) Europol teilt der Kommission den erfolgreichen Abschluss der in Artikel 75 Absatz 3 Buchstabe b genannten Tests mit.
- (4) Jeder Mitgliedstaat teilt den anderen Mitgliedstaaten, der Kommission, eu-LISA und Europol den Inhalt seiner nationalen DNA-Datenbanken und die Bedingungen für automatisierte Abfragen mit, auf die die Artikel 5 und 6 Anwendung finden.
- (5) Jeder Mitgliedstaat unterrichtet die anderen Mitgliedstaaten, die Kommission, eu-LISA und Europol über den Inhalt seiner nationalen daktyloskopischen Datenbanken und die Bedingungen für automatisierte Abfragen, auf die die Artikel 10 und 11 Anwendung finden.
- (6) Jeder Mitgliedstaat unterrichtet die anderen Mitgliedstaaten, die Kommission, eu-LISA und Europol über den Inhalt seiner nationalen Gesichtsbilddatenbanken und die Bedingungen für automatisierte Abfragen, auf die die Artikel 19 und 20 Anwendung finden.

- (7) Die Mitgliedstaaten, die sich am automatisierten Austausch von Polizeiakten gemäß den Artikeln 25 und 26 beteiligen, teilen den anderen Mitgliedstaaten, der Kommission und Europol den Inhalt ihrer nationalen Polizeiaktennachweise und die für die Erstellung dieser Nachweise verwendeten nationalen Datenbanken und die Bedingungen für automatisierte Abfragen mit.
- (8) Die Mitgliedstaaten teilen der Kommission, eu-LISA und Europol ihre gemäß Artikel 30 benannte nationale Kontaktstelle mit. Die Kommission erstellt ein Verzeichnis der ihr mitgeteilten nationalen Kontaktstellen und stellt es allen Mitgliedstaaten zur Verfügung.

Artikel 75

Aufnahme des Betriebs

- (1) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, zu welchem Zeitpunkt die Mitgliedstaaten und Europol den Router verwenden können, sobald folgende Voraussetzungen erfüllt wurden:
- a) Die Maßnahmen nach Artikel 5 Absatz 3, Artikel 8 Absätze 2 und 3, Artikel 13 Absätze 2 und 3, Artikel 17 Absatz 3, Artikel 22 Absätze 2 und 3, Artikel 31 und 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 zuständigen Behörden der Mitgliedstaaten und Europol durchgeführt hat.

Die Kommission legt im Wege des in Unterabsatz 1 genannten Durchführungsrechtsakts den Zeitpunkt fest, ab dem die Mitgliedstaaten und Europol mit der Verwendung des Routers beginnen sollen. Dieser Zeitpunkt liegt ein Jahr nach dem gemäß Unterabsatz 1 festgelegten Zeitpunkt.

Die Kommission kann den Zeitpunkt, ab dem die Mitgliedstaaten und Europol mit der Nutzung des Routers beginnen sollen, um höchstens ein Jahr verschieben, falls eine Bewertung der Implementierung des Routers ergeben hat, dass eine solche Verschiebung erforderlich ist.

- (2) Die Mitgliedstaaten stellen zwei Jahre nach Aufnahme des Betriebs des Routers sicher, dass in Artikel 19 genannte Gesichtsbilder für die Zwecke der in Artikel 20 genannten automatisierten Abfrage von Gesichtsbildern verfügbar sind.
- (3) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, ab welchem Zeitpunkt die Mitgliedstaaten und Europol das EPRIS verwenden müssen, sobald folgende Voraussetzungen erfüllt sind:
 - a) Die in Artikel 44 Absatz 6 genannten Maßnahmen wurden angenommen;
 - b) Europol hat den erfolgreichen Abschluss eines umfangreichen Tests des EPRIS festgestellt, den es in Zusammenarbeit mit den zuständigen mitgliedstaatlichen Behörden durchgeführt hat.

- (4) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, ab welchem Zeitpunkt Europol den Mitgliedstaaten biometrische Daten aus Drittländern gemäß Artikel 48 zur Verfügung stellt, sobald folgende Voraussetzungen erfüllt sind:
- a) Der Router ist in Betrieb;
 - b) Europol hat den erfolgreichen Abschluss eines umfangreichen Tests ihrer Verbindung zum Router festgestellt, den es in Zusammenarbeit mit den zuständigen Behörden der Mitgliedstaaten und eu-LISA durchgeführt hat.
- (5) Die Kommission bestimmt im Wege eines Durchführungsrechtsakts, ab welchem Zeitpunkt Europol Zugang zu den in den Datenbanken der Mitgliedstaaten gespeicherten Daten gemäß Artikel 49 erhält, sobald folgende Voraussetzungen erfüllt sind:
- a) Der Router ist in Betrieb;
 - b) Europol hat den erfolgreichen Abschluss eines umfangreichen Tests ihrer Verbindung zum Router festgestellt, den es in Zusammenarbeit mit den zuständigen mitgliedstaatlichen Behörden und eu-LISA durchgeführt hat.
- (6) Die in diesem Artikel genannten Durchführungsrechtsakte werden nach dem in Artikel 77 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 76
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 19 bis 22, Artikel 47 und Artikel 49 Absatz 6 ab dem gemäß Artikel 75 Absatz 1 Unterabsatz 1 festgelegten Zeitpunkt an.
- (2) Die Mitgliedstaaten und die Agenturen der Union wenden die Artikel 25 bis 28 und Artikel 49 Absatz 4 ab dem gemäß Artikel 75 Absatz 3 festgelegten Zeitpunkt an.
- (3) Die Mitgliedstaaten und die Agenturen der Union wenden den Artikel 48 ab dem gemäß Artikel 75 Absatz 4 festgelegten Zeitpunkt an.
- (4) Die Mitgliedstaaten und die Agenturen der Union wenden Artikel 49 Absätze 1, 2, 3, 5 und 7 ab dem gemäß Artikel 75 Absatz 5 festgelegten Zeitpunkt an.

Artikel 77
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 78

Beratergruppe für Interoperabilität

Die Verantwortlichkeiten der durch Artikel 75 der Verordnung (EU) 2019/817 und Artikel 71 der Verordnung (EU) 2019/818 eingerichteten Beratergruppe für Interoperabilität 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 79

Handbuch

Die Kommission stellt in enger Zusammenarbeit mit den Mitgliedstaaten, eu-LISA, Europol und der Agentur der Europäischen Union für Grundrechte 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 vor Aufnahme des Betriebs des Routers bzw. des EPRIS in Form einer Empfehlung an. Die Kommission aktualisiert das Handbuch regelmäßig und bei Bedarf.

Artikel 80
Überwachung und Bewertung

(1) eu-LISA stellt sicher, dass Verfahren vorhanden sind, um die Entwicklung des Routers anhand von Zielen für Planung und Kosten sowie seine Funktionsweise anhand von Zielen in Bezug auf die technische Leistung, Kostenwirksamkeit, Sicherheit und Dienstqualität zu überwachen.

Europol stellt sicher, dass Verfahren vorhanden sind, um die Entwicklung des EPRIS anhand von Zielen für Planung und Kosten wo sie seine Funktionsweise anhand von Zielen in Bezug auf die technische Leistung, Kostenwirksamkeit, Sicherheit und Dienstqualität zu überwachen.

(2) Bis zum ... [ein Jahr nach dem Tag des Inkrafttretens der vorliegenden 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. Diese Berichte müssen genaue Angaben über die angefallenen Kosten und Informationen über etwaige Risiken enthalten, die sich auf die Gesamtkosten auswirken könnten, die gemäß Artikel 73 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 dem Tag des Inkrafttretens 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 Entwicklung des EPRIS. Diese Berichte enthalten genaue Angaben über die angefallenen Kosten und Informationen über etwaige Risiken, die sich auf die Gesamtkosten auswirken könnten, die gemäß Artikel 73 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 erhält eu-LISA Zugang zu den erforderlichen Informationen über die im Router durchgeführten Datenverarbeitungsvorgänge. Zum Zwecke der technischen Instandhaltung erhält Europol Zugang zu den erforderlichen Informationen über die 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 der in Artikel 75 genannten Inbetriebnahme des Routers und des EPRIS und danach alle vier Jahre erstellt die Kommission eine Gesamtbewertung des Prüm-II-Rahmens.

Ein Jahr nach Inbetriebnahme des Routers und danach alle zwei Jahre erstellt die Kommission einen Bericht zur Bewertung der Verwendung von Gesichtsbildern gemäß dieser Verordnung.

Die in den Unterabsätzen 1 und 2 genannten Berichte umfassen Folgendes:

- a) eine Beurteilung der Anwendung dieser Verordnung einschließlich ihrer Nutzung durch die einzelnen Mitgliedstaaten und Europol;
- 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 des Prüm-II-Rahmens und seiner Arbeitsverfahren im Hinblick auf seine Ziele, sein Mandat und seine Aufgaben;
- d) eine Bewertung der Sicherheit des Prüm-II-Rahmens.

Die Kommission übermittelt diese Berichte dem Europäischen Parlament, dem Rat, dem Europäischen Datenschutzbeauftragten und der Agentur der Europäischen Union für Grundrechte.

- (8) Die Kommission widmet in den in Absatz 7 Unterabsatz 1 genannten Berichten den folgenden neuen Datenkategorien besondere Aufmerksamkeit: Gesichtsbilder und Polizeiakten. Die Kommission umfasst in diesen Berichten die Nutzung dieser neuen Datenkategorien durch die einzelnen Mitgliedstaaten und Europol und ihre Auswirkungen, Wirksamkeit und Effizienz. In den in Absatz 7 Unterabsatz 2 genannten Berichten achtet die Kommission besonders auf das Risiko falscher Übereinstimmungen und die Datenqualität.
- (9) Die Mitgliedstaaten und Europol stellen eu-LISA und der Kommission die Informationen zur Verfügung, die für die Ausarbeitung der in den Absätzen 2 und 5 genannten Berichte erforderlich sind. Diese Informationen dürfen nicht zu einer Beeinträchtigung der Arbeitsverfahren führen oder Rückschlüsse auf Quellen, Mitarbeiter oder Ermittlungen der zuständigen Behörden der Mitgliedstaaten ermöglichen.
- (10) Die Mitgliedstaaten stellen der Kommission und Europol die Informationen zur Verfügung, die für die Ausarbeitung der in den Absätzen 3 und 6 genannten Berichte erforderlich sind. Diese Informationen dürfen nicht zu einer Beeinträchtigung der Arbeitsverfahren führen oder Rückschlüsse auf Quellen, Mitarbeiter oder Ermittlungen der zuständigen Behörden der Mitgliedstaaten ermöglichen.
- (11) Unbeschadet der Vertraulichkeitsanforderungen stellen die Mitgliedstaaten, eu-LISA und Europol der Kommission die für die in Absatz 7 genannten Berichte erforderlichen Informationen zur Verfügung. Die Mitgliedstaaten teilen der Kommission zudem die Zahl der bestätigten Übereinstimmungen mit der Datenbank der einzelnen Mitgliedstaaten je Datenkategorie und Datentyp mit. Diese Informationen dürfen nicht zu einer Beeinträchtigung der Arbeitsverfahren führen oder Rückschlüsse auf Quellen, Mitarbeiter oder Ermittlungen der zuständigen Behörden der Mitgliedstaaten ermöglichen.

Artikel 81

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 ...

Im Namen des Europäischen Parlaments

Die Präsidentin

Im Namen des Rates

Der Präsident/Die Präsidentin