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

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 82 Absatz 1 Unterabsatz 2 Buchstabe d, Artikel 85 Absatz 1, Artikel 87 Absatz 2 Buchstabe a und Artikel 88 Absatz 2 Buchstabe a,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

gemäß dem ordentlichen Gesetzgebungsverfahren ([1]),

in Erwägung nachstehender Gründe:

(1) Das Schengener Informationssystem (im Folgenden „SIS“) stellt ein wichtiges Instrument für die Anwendung der Bestimmungen des in den Rahmen der Europäischen Union einbezogenen Schengen-Besitzstands dar. Das SIS gehört zu den wichtigsten Ausgleichsmaßnahmen und trägt zur Wahrung eines hohen Maßes an Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts der Union bei, indem es die operative Zusammenarbeit zwischen den nationalen zuständigen Behörden, insbesondere Grenzschutz, Polizei, Zollbehörden, Einwanderungsbehörden und für die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder für die Strafvollstreckung zuständigen Behörden unterstützt.

(2) Das SIS wurde ursprünglich gemäß den Bestimmungen des Titels IV des Übereinkommens vom 19. Juni 1990 zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen ([2]) (im Folgenden „Schengener Durchführungsübereinkommen“) errichtet. Mit der Entwicklung des SIS der zweiten Generation (im Folgenden „SIS II“) wurde gemäß der Verordnung (EG) Nr. 2424/2001 des Rates ([3]) und dem Beschluss 2001/886/JI des Rates ([4]) die Kommission betraut. Es wurde später durch die Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates ([5]) und den Beschluss 2007/533/JI des Rates ([6]) eingerichtet. Das SIS II ersetzte das mit dem Schengener Durchführungsübereinkommen geschaffene SIS.

(3) Drei Jahre nach Inbetriebnahme des SIS II führte die Kommission eine Bewertung des Systems gemäß der Verordnung (EG) Nr. 1987/2006 sowie dem Beschluss 2007/533/JI durch. Am 21. Dezember 2016 hat die Kommission dem Europäischen Parlament und dem Rat den Bericht über die Bewertung des Schengener Informationssystems der zweiten Generation (SIS II) gemäß Artikel 24 Absatz 5, Artikel 43 Absatz 3 und Artikel 50 Absatz 5 der Verordnung (EG) Nr. 1987/2006 und Artikel 59 Absatz 3 und Artikel 66 Absatz 5 des Beschlusses 2007/533/JI sowie eine dazugehörige Arbeitsunterlage vorgelegt. Die in diesen Dokumenten enthaltenen Empfehlungen sollten gegebenenfalls in diese Verordnung eingehen.

(4) Diese Verordnung bildet die Rechtsgrundlage für das SIS in Bezug auf die Angelegenheiten, die in den Anwendungsbereich von Teil 3 Titel V Kapitel 4 und 5 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) fallen. Die Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates ([7]) bildet die Rechtsgrundlage für das SIS in Bezug auf die Angelegenheiten, die in den Anwendungsbereich von Teil 3 Titel V Kapitel 2 des AEUV fallen.

([1]) Standpunkt des Europäischen Parlaments vom 24. Oktober 2018 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates 19. November 2018.

([2]) ABl. L 239 vom 22.9.2000, S. 19.

([3]) Verordnung (EG) Nr. 2424/2001 des Rates vom 6. Dezember 2001 über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L 328 vom 13.12.2001, S. 4.).

([4]) Beschluss 2001/886/JI des Rates vom 6. Dezember 2001 über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L 328 vom 13.12.2001, S. 1).

([5]) Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L 381 vom 28.12.2006, S. 4).

([6]) Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L 205 vom 7.8.2007, S. 63).

([7]) 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 (siehe Seite 14 dieses Amtsblatts).

(5) Dass verschiedene Instrumente als Rechtsgrundlage für das SIS vorgesehen sind, lässt den Grundsatz unberührt, dass das SIS ein einziges Informationssystem darstellt, das auch als solches betrieben werden sollte. Es sollte ein einziges Netz von nationalen Büros, SIRENE-Büros genannt, für den Austausch von Zusatzinformationen umfassen. Einige Bestimmungen dieser Rechtsinstrumente sollten daher identisch sein.

(6) Es ist notwendig, die Ziele des SIS, bestimmte Elemente seiner Systemarchitektur und die Finanzierung des SIS zu präzisieren, Vorschriften für den End-to-End-Betrieb und die End-to-End-Nutzung des Systems festzulegen und Zuständigkeiten zu definieren. Es ist ebenfalls notwendig, die in das System einzugebenden Datenkategorien, die Eingabe- und Verarbeitungszwecke sowie die Eingabekriterien festzulegen. Außerdem sind Vorschriften für die Löschung von Ausschreibungen, die zugriffsberechtigten Behörden und die Verwendung biometrischer Daten erforderlich, und es ist erforderlich, die Verpflichtungen im Hinblick auf den Datenschutz und die Datenverarbeitung genauer zu bestimmen.

(7) Ausschreibungen im SIS enthalten nur die für die Identifizierung einer Person oder einer Sache und die zu ergreifende Maßnahme erforderlichen Angaben. Die Mitgliedstaaten sollten daher erforderlichenfalls Zusatzinformationen zu den Ausschreibungen austauschen.

(8) Das SIS umfasst ein zentrales System (im Folgenden „zentrales SIS“) und nationale Systeme. Die nationalen Systeme können eine vollständige oder Teilkopie der SIS-Datenbank enthalten, die von zwei oder mehr Mitgliedstaaten gemeinsam genutzt werden kann. Da das SIS das wichtigste Instrument für den Informationsaustausch in Europa im Hinblick auf die Gewährleistung der Sicherheit und eines wirksamen Grenzmanagements ist, muss sein ununterbrochener Betrieb sowohl auf zentraler als auch auf nationaler Ebene gewährleistet sein. Die Verfügbarkeit des SIS sollte auf zentraler Ebene und auf Ebene der Mitgliedstaaten genau überwacht werden, und jeder Vorfall, der zur Nichtverfügbarkeit für die Endnutzer führt, sollte registriert und den Beteiligten auf nationaler Ebene und auf Unionsebene gemeldet werden. Jeder Mitgliedstaat sollte ein Backup für sein nationales System einrichten. Des Weiteren sollten die Mitgliedstaaten durch doppelte Verbindungspunkte, die physisch und geografisch voneinander getrennt sind, eine ununterbrochene Verbindung mit dem zentralen SIS gewährleisten. Das zentrale SIS und die Kommunikationsinfrastruktur sollten in einer Weise betrieben werden, die deren Betriebsbereitschaft 24 Stunden pro Tag und 7 Tage die Woche gewährleistet. Die Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (im Folgenden „eu-LISA“), die durch die Verordnung (EU) 2018/1726 des Europäischen Parlaments und des Rates [1] eingerichtet wurde, sollte daher technische Lösungen anwenden, um vorbehaltlich einer unabhängigen Folgenabschätzung und Kosten-Nutzen-Analyse die ununterbrochene Verfügbarkeit des SIS zu stärken.

(9) Es ist notwendig, ein Handbuch zu führen, das die ausführlichen Vorschriften für den Austausch von Zusatzinformationen im Hinblick auf die aufgrund der Ausschreibung erforderlichen Maßnahmen enthält (im Folgenden „SIRENE-Handbuch“). Die SIRENE-Büros sollten den schnellen und effizienten Austausch solcher Informationen gewährleisten.

(10) Damit der effiziente Austausch von Zusatzinformationen, einschließlich über die in der Ausschreibung angegebenen zu treffenden Maßnahmen, weiterhin garantiert ist, sollte die Arbeitsweise der SIRENE-Büros durch die Präzisierung der Anforderungen bezüglich der verfügbaren Ressourcen und der Schulung der Nutzer sowie der Frist für die Antwort auf die aus anderen SIRENE-Büros eingegangenen Anfragen verbessert werden.

(11) Die Mitgliedstaaten sollten sicherstellen, dass das Personal ihrer SIRENE-Büros die für die Wahrnehmung seiner Aufgaben erforderlichen Sprachkenntnisse und Kenntnisse des einschlägigen Recht und der einschlägigen Verfahrensvorschriften hat.

(12) Damit die Funktionen des SIS uneingeschränkt genutzt werden können, sollten die Mitgliedstaaten dafür sorgen, dass die Endnutzer und die Mitarbeiter der SIRENE-Büros regelmäßig geschult werden, auch was Datensicherheit, Datenschutz und die Datenqualität betrifft. Die SIRENE-Büros sollten an der Entwicklung von Schulungsprogrammen mitwirken. Soweit möglich, sollten auch mindestens einmal im Jahr Mitarbeiter mit anderen SIRENE-Büros ausgetauscht werden. Die Mitgliedstaaten sollten geeignete Maßnahmen treffen, um Kompetenz- und Erfahrungsverluste infolge von Personalfluktuation zu vermeiden.

(13) Das Betriebsmanagement der zentralen Komponenten des SIS wird von eu-LISA wahrgenommen. Damit eu-LISA die notwendigen finanziellen und personellen Ressourcen für alle Aspekte des Betriebsmanagements des zentralen SIS und der Kommunikationsinfrastruktur aufwenden kann, sollten ihre Aufgaben in dieser Verordnung ausführlich dargelegt werden, insbesondere hinsichtlich der technischen Aspekte des Austauschs von Zusatzinformationen.

(14) Unbeschadet der Verantwortung der Mitgliedstaaten für die Richtigkeit der in das SIS eingegebenen Daten und der Rolle der SIRENE-Büros als Qualitätskoordinatoren sollte eu-LISA für die Verbesserung der Datenqualität durch Einführung eines zentralen Instruments für die Überwachung der Datenqualität zuständig sein und regelmäßig Berichte an die Kommission und die Mitgliedstaaten übermitteln. Die Kommission sollte dem Europäischen

[1] 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).

Parlament und dem Rat über die aufgetretenen Probleme im Zusammenhang mit der Datenqualität berichten. Um die Qualität der Daten im SIS zusätzlich zu verbessern, sollte eu-LISA auch Schulungen zur Nutzung des SIS für nationale Schulungsstellen und, sofern möglich, für die SIRENE-Büros und Endnutzer anbieten.

(15) Um eine bessere Überwachung der Nutzung des SIS und die Analyse von Trends im Zusammenhang mit Straftaten zu ermöglichen, sollte eu-LISA in der Lage sein, ein dem neuesten Stand der Technik entsprechendes System für die statistische Berichterstattung an die Mitgliedstaaten, das Europäische Parlament, den Rat, die Kommission, Europol, Eurojust und die Europäische Agentur für die Grenz- und Küstenwache zu entwickeln, bei dem die Integrität der Daten nicht beeinträchtigt wird. Daher sollte ein zentrales Register eingerichtet werden. Statistiken, die in diesem Register erfasst oder von diesem Register erhalten werden, sollten keine personenbezogenen Daten enthalten. Die Mitgliedstaaten sollten im Rahmen eines Mechanismus zur Zusammenarbeit zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten nach dieser Verordnung Statistiken über die Ausübung des Rechts auf Auskunft, auf Berichtigung unrichtiger Daten und auf Löschung unrechtmäßig gespeicherter Daten übermitteln.

(16) Es sollten neue Datenkategorien in das SIS aufgenommen werden, um es den Endnutzern zu ermöglichen, ohne Zeitverlust fundierte Entscheidungen auf der Grundlage einer Ausschreibung zu treffen. Zur Erleichterung der Identifizierung und zur Aufdeckung von Mehrfachidentitäten sollte die Ausschreibung daher, sofern solche Informationen zur Verfügung stehen, eine Bezugnahme auf das persönliche Identifizierungsdokument der betreffenden Person oder dessen Nummer und, eine Kopie dieses Papiers, wenn möglich in Farbe, umfassen.

(17) Die zuständigen Behörden sollten, wenn unbedingt erforderlich, in der Lage sein, bestimmte Informationen in das SIS einzugeben, die sich auf unveränderliche besondere, objektive, physische Eigenschaften einer Person wie Tätowierungen, Male oder Narben beziehen.

(18) Soweit vorhanden, sollten alle relevanten Daten, insbesondere der Vorname der betreffenden Person, bei der Erstellung einer Ausschreibung eingegeben werden, um die Gefahr falscher Treffer und unnötiger operativer Maßnahmen so gering wie möglich zu halten.

(19) Im SIS sollten keine für die Durchführung von Abfragen verwendeten Daten gespeichert werden; hiervon ausgenommen ist die Führung von Protokollen zur Überprüfung der Rechtmäßigkeit der Abfrage, zur Überwachung der Rechtmäßigkeit der Datenverarbeitung, zur Eigenkontrolle und zur Gewährleistung des einwandfreien Funktionierens der nationalen Systeme sowie für die Zwecke der Integrität und Sicherheit der Daten.

(20) Das SIS sollte die Verarbeitung biometrischer Daten ermöglichen, damit die betroffenen Personen zuverlässiger identifiziert werden können. Jede Aufnahme von Lichtbildern, Gesichtsbildern und daktyloskopischen Daten in das SIS und jede Nutzung solcher Daten sollte auf das Maß beschränkt sein, das erforderlich ist, um die verfolgten Ziele zu erreichen; sie sollte nach dem Recht der Union und unter Achtung der Grundrechte, einschließlich des Kindeswohls, erfolgen und dem Unionsrechtentsprechen, einschließlich der einschlägigen Bestimmungen zum Datenschutz, die in dieser Verordnung festgelegt sind. Ebenso sollte das SIS, um Unannehmlichkeiten aufgrund einer falschen Identifizierung zu vermeiden, die Verarbeitung von Daten über Personen ermöglichen, deren Identität missbraucht wurde; eine solche Datenverarbeitung sollte an angemessene Garantien, einschließlich der Zustimmung der betroffenen Personen für jede Datenkategorie, insbesondere Handflächenabdrücke, und eine strikte Beschränkung der Zwecke, zu denen diese personenbezogenen Daten rechtmäßig verarbeitet werden dürfen, geknüpft sein.

(21) Die Mitgliedstaaten sollten die erforderlichen technischen Vorkehrungen dafür treffen, dass die Endnutzer jedes Mal, wenn sie zur Durchführung einer Abfrage in einer nationalen Polizei- oder Einwanderungsdatenbank berechtigt sind, parallel dazu auch eine Abfrage im SIS durchführen, vorbehaltlich der Grundsätze gemäß Artikel 4 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates ([1]) und Artikel 5 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([2]). Dadurch sollte sichergestellt werden, dass das SIS seine Funktion als wichtigste Ausgleichsmaßnahme im Raum ohne Kontrollen an den Binnengrenzen erfüllt und besser gegen die grenzüberschreitende Dimension der Kriminalität und die Mobilität von Straftätern vorgegangen werden kann.

(22) In dieser Verordnung sollten die Voraussetzungen für die Verwendung von daktyloskopischen Daten, Lichtbildern und Gesichtsbildern zu Identifizierungs- und Überprüfungszwecken festgelegt werden. Gesichtsbilder und Lichtbilder sollten für Identifizierungszwecke zunächst nur an regulären Grenzübergangsstellen verwendet werden. Eine solche Verwendung sollte vorbehaltlich eines Berichts der Kommission erfolgen, in dem die Verfügbarkeit, Zuverlässigkeit und Einsatzbereitschaft dieser Technologie bestätigt wird.

([1]) 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).

([2]) 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).

(23) Durch die Einführung einer Funktion zur automatisierten Fingerabdruck-Identifizierung im SIS wird das bestehende Prüm-Verfahren über den gegenseitigen grenzüberschreitenden Online-Zugriff auf spezielle nationale DNA-Datenbanken und automatisierte daktyloskopische Identifizierungssysteme gemäß den Beschlüssen 2008/615/JI [1] und 2008/616/JI [2] des Rates ergänzt. Mit der Abfrage anhand daktyloskopischer Daten im SIS kann aktiv nach dem Täter gesucht werden. Es sollte daher möglich sein, daktyloskopische Daten eines unbekannten Täters in das SIS einzugeben, sofern diese Daten mit einer sehr hohen Wahrscheinlichkeit dem Täter einer schweren oder terroristischen Straftat zugeordnet werden können. Dies gilt insbesondere, wenn daktyloskopische Daten auf einer Waffe oder einem Gegenstand vorgefunden werden, die bzw. der für die Straftat verwendet wurde. Das bloße Vorfinden daktyloskopischer Daten am Tatort sollte jedoch nicht als Indiz dafür gelten, dass es sich mit sehr hoher Wahrscheinlichkeit um die daktyloskopischen Daten des Täters handelt. Eine weitere Voraussetzung für das Erstellen einer entsprechenden Ausschreibung sollte sein, dass die Identität der verdächtigen Person nicht auf der Grundlage von Daten aus einer anderen einschlägigen nationalen, Unions- oder internationalen Datenbank festgestellt werden kann. Falls die daktyloskopischen Daten zu einer möglichen Übereinstimmung führen, sollte der Mitgliedstaat unter Hinzuziehung von Experten weitere Überprüfungen durchführen, um zu ermitteln, ob es sich beim Verdächtigen um die Person handelt, deren Abdrücke im SIS gespeichert sind, sowie die Identität der Person feststellen. Die Verfahren sollten dem nationalen Recht unterliegen. Diese Identifizierung könnte wesentlich zu den Ermittlungen beitragen und zu einer Festnahme führen, sofern alle Bedingungen für eine Festnahme erfüllt sind.

(24) Es sollte zulässig sein, die im SIS gespeicherten daktyloskopischen Daten mit an einem Tatort gefundenen vollständigen oder unvollständigen Sätzen von Finger- oder Handflächenabdrücken abzugleichen, wenn sie mit hoher Wahrscheinlichkeit dem Täter zuzuordnen sind, der die schwere oder terroristische Straftat begangen hat, sofern ein Abgleich zugleich in den einschlägigen nationalen Fingerabdruck-Datenbanken durchgeführt wird. Besondere Aufmerksamkeit sollte der Schaffung von Qualitätsstandards für die Speicherung biometrischer Daten, einschließlich latenter daktyloskopischer Daten, gewidmet werden.

(25) Lässt sich die Identität einer Person nicht mit anderen Mitteln feststellen, so sollte versucht werden, die Identität mithilfe daktyloskopischer Daten festzustellen. Es sollte in allen Fällen zulässig sein, eine Person mithilfe daktyloskopischer Daten zu identifizieren.

(26) Falls keine daktyloskopischen Daten verfügbar sind, sollte es in klar definierten Fällen möglich sein, der Ausschreibung ein DNA-Profil hinzuzufügen. Dieses DNA-Profil sollte ausschließlich befugten Benutzern zugänglich sein. Mithilfe von DNA-Profilen sollte die Identifizierung von vermissten schutzbedürftigen Personen und insbesondere von Kindern erleichtert werden, indem es unter anderem gestattet wird, DNA-Profile der Verwandten in gerader aufsteigender oder absteigender Linie oder von Geschwistern zur Identifizierung zu verwenden. Die DNA-Daten sollten nur die Mindestinformationen enthalten, die zur Identifizierung der vermissten Person erforderlich sind.

(27) DNA-Profile sollten nur aus dem SIS abgerufen werden, wenn eine Identifizierung für die in dieser Verordnung dargelegten Zwecke erforderlich und verhältnismäßig ist. DNA-Profile sollten für keine anderen Zwecke als diejenigen, für die sie in das SIS eingegeben wurden, abgerufen oder verarbeitet werden. Die in dieser Verordnung festgelegten Datenschutz- und Sicherheitsbestimmungen sollten Anwendung finden. Erforderlichenfalls sollten zusätzliche Garantien für die Nutzung von DNA-Profilen vorgesehen werden, um jede Gefahr von falschen Übereinstimmungen, Hacking und unbefugter Weitergabe an Dritte zu verhindern.

(28) Das SIS sollte Personenausschreibungen zum Zwecke der Übergabe- oder Auslieferungshaft enthalten. Zusätzlich zu den Ausschreibungen sollte der Austausch von Zusatzinformationen, die für die Übergabe- und Auslieferungsverfahren erforderlich sind, über die SIRENE-Büros vorgesehen werden. Insbesondere sollten Daten im Sinne von Artikel 8 des Rahmenbeschlusses 2002/584/JI des Rates [3] im SIS verarbeitet werden. Aus operativen Gründen ist es angemessen, dass der ausschreibende Mitgliedstaat eine bestehende Ausschreibung zur Festnahme nach Ermächtigung der Justizbehörden vorübergehend nicht verfügbar macht, wenn nach einer Person, gegen die ein Europäischer Haftbefehl erlassen wurde, intensiv und aktiv gefahndet wird und nicht an der konkreten Fahndung beteiligte Endnutzer den Erfolg der Fahndung gefährden könnten. Diese vorübergehende Nichtverfügbarkeit solcher Ausschreibungen sollte grundsätzlich nicht länger als 48 Stunden dauern.

(29) Auch sollte eine Übersetzung der ergänzenden Daten, die zum Zwecke der Übergabe auf der Grundlage des Europäischen Haftbefehls und zum Zwecke der Auslieferung eingegeben wurden, in das SIS aufgenommen werden können.

---

[1] 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).

[2] 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).

[3] Rahmenbeschluss 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (ABl. L 190 vom 18.7.2002, S. 1).

(30) Das SIS sollte Ausschreibungen von vermissten Personen oder schutzbedürftigen Personen, die am Reisen gehindert werden müssen, enthalten, damit diese geschützt und etwaige Gefahren für die öffentliche Sicherheit oder die öffentliche Ordnung abgewehrt werden können. Ausschreibungen von Kindern und die entsprechenden Verfahren sollten dem Wohl des Kindes gemäß Artikel 24 der Charta der Grundrechte der Europäischen Union und Artikel 3 des Übereinkommens der Vereinten Nationen vom 20. November 1989 über die Rechte des Kindes dienen. Maßnahmen und Entscheidungen der zuständigen Behörden, einschließlich der Justizbehörden, im Anschluss an die Ausschreibung eines Kindes sollten in Zusammenarbeit mit den Kinderschutzbehörden getroffen werden. Die nationale Hotline für vermisste Kinder sollte gegebenenfalls unterrichtet werden.

(31) Ausschreibungen von vermissten Personen, die unter Schutz gestellt werden müssen, sollten auf Antrag der zuständigen Behörde eingegeben werden. Alle Kinder, die aus Aufnahmeeinrichtungen der Mitgliedstaaten abgängig sind, sollten Gegenstand von Ausschreibungen von vermissten Personen im SIS sein.

(32) Ausschreibungen von Kindern, die dem Risiko einer Kindesentführung durch einen Elternteil ausgesetzt sind, sollten auf Ersuchen der zuständigen Behörden, einschließlich der nach nationalem Recht für Fragen der elterlichen Verantwortung zuständigen Justizbehörden, in das SIS eingegeben werden. Ausschreibungen von Kindern, die dem Risiko einer Kindesentführung durch einen Elternteil ausgesetzt sind, sollten nur in das SIS eingegeben werden können, wenn das Risiko konkret und offensichtlich ist, sowie unter abgegrenzten Umständen. Es ist daher erforderlich, dass strenge und angemessene Regelungsschranken zur Verfügung stehen. Die zuständige Behörde sollte bei der Bewertung, ob ein konkretes und offensichtliches Risiko besteht, dass ein Kind in Kürze widerrechtlich aus einem Mitgliedstaat verbracht wird, die persönliche Situation des Kindes und das Umfeld berücksichtigen, dem das Kind ausgesetzt ist.

(33) Mit dieser Verordnung sollte eine neue Kategorie von Ausschreibungen für bestimmte Kategorien schutzbedürftiger Personen, die am Reisen gehindert werden müssen, eingeführt werden. Personen, die aufgrund ihres Alters, einer Behinderung oder ihrer familiären Umstände Schutz benötigen, sollten als schutzbedürftig gelten.

(34) Ausschreibungen von Kindern, die zu ihrem eigenen Schutz am Reisen gehindert werden müssen, sollten in das SIS eingegeben werden, wenn ein konkretes und offensichtliches Risiko besteht, dass sie aus dem Hoheitsgebiet eines Mitgliedstaats gebracht werden oder dieses verlassen. Solche Ausschreibungen sollten eingegeben werden, wenn durch die Reise die Gefahr bestünde, dass sie Opfer von Menschenhandel oder einer erzwungenen Eheschließung, von Genitalverstümmelung bei Frauen oder sonstiger Formen geschlechtsspezifischer Gewalt werden, dass sie Opfer terroristischer Straftaten werden oder darin verwickelt werden oder dass sie in bewaffnete Gruppen eingezogen oder rekrutiert werden oder zur aktiven Teilnahme an Feindseligkeiten gezwungen werden.

(35) Ausschreibungen von schutzbedürftigen Erwachsenen, die zu ihrem eigenen Schutz am Reisen gehindert werden müssen, sollten eingegeben werden, wenn durch eine Reise die Gefahr bestünde, dass sie Opfer von Menschenhandel oder geschlechtsspezifischer Gewalt werden.

(36) Damit strenge und angemessene Regelungsschranken garantiert werden, sollten — soweit dies nach nationalem Recht vorgesehen ist — Ausschreibungen von Kindern oder sonstigen schutzbedürftigen Personen, die am Reisen gehindert werden müssen, in das SIS eingegeben werden, nachdem eine Entscheidung einer Justizbehörde oder eine Entscheidung einer zuständigen Behörde, die durch eine Justizbehörde bestätigt wurde, ergangen ist.

(37) Es sollte eine neue zu ergreifende Maßnahme eingeführt werden, damit eine Person angehalten und befragt werden kann, damit der ausschreibende Mitgliedstaat möglichst detaillierte Informationen erhält. Diese Maßnahme sollte für Fälle gelten, in denen eine Person aufgrund eindeutiger Anhaltspunkte verdächtigt wird, eine der in Artikel 2 Absätze 1 und 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten zu planen oder zu begehen, in denen weitere Informationen für die Vollstreckung einer Freiheitsstrafe oder Haftanordnung gegen eine wegen einer der in Artikel 2 Absätze 1 und 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten verurteilte Person erforderlich sind, oder in denen Grund zu der Annahme besteht, dass sie eine dieser Straftaten begehen wird,. Diese zu ergreifende Maßnahme sollte zudem bestehende Rechtshilfeverfahren unberührt lassen. Sie sollte ausreichende Informationen liefern, damit über weitere Maßnahmen entschieden werden kann. Diese neue Maßnahme sollte nicht dazu führen, dass die Person durchsucht oder festgenommen wird. Die Verfahrensrechte von Verdächtigen und beschuldigten Personen nach Unions- und nationalem Recht sollten gewahrt werden, einschließlich ihres Rechts auf Rechtsbeistand gemäß der Richtlinie 2013/48/EU des Europäischen Parlaments und des Rates ([1]).

(38) Bei Sachfahndungsausschreibungen zur Sicherstellung oder Beweissicherung in Strafverfahren sollten die Sachen gemäß dem nationalen Recht sichergestellt werden, durch das bestimmt wird, ob und unter welchen Bedingungen eine Sache sicherzustellen ist, insbesondere, wenn sie sich im Besitz ihres rechtmäßigen Eigentümers befindet.

(39) Das SIS sollte neue Kategorien für Sachen von hohem Wert — wie Gegenstände der Informationstechnik — enthalten, die mithilfe einer eindeutigen Kennnummer ermittelt und gesucht werden können.

([1]) Richtlinie 2013/48/EU des Europäischen Parlaments und des Rates vom 22. Oktober 2013 über das Recht auf Zugang zu einem Rechtsbeistand in Strafverfahren und in Verfahren zur Vollstreckung des Europäischen Haftbefehls sowie über das Recht auf Benachrichtigung eines Dritten bei Freiheitsentzug und das Recht auf Kommunikation mit Dritten und mit Konsularbehörden während des Freiheitsentzugs (ABl. L 294 vom 6.11.2013, S. 1).

(40) Was Ausschreibungen angeht, die im Hinblick auf Dokumente zur Sicherstellung oder Beweissicherung in Strafverfahren in das SIS eingegeben werden, ist der Begriff „gefälscht“ so auszulegen, dass sowohl verfälschte als auch totalgefälschte Dokumente erfasst sind.

(41) Jeder Mitgliedstaat sollte die Möglichkeit haben, einer Ausschreibung einen Vermerk, Kennzeichnung genannt, hinzuzufügen, um deutlich zu machen, dass die gemäß der Ausschreibung zu ergreifende Maßnahme in seinem Hoheitsgebiet nicht vollzogen wird. Bei Ausschreibungen zum Zwecke der Übergabehaft sollte keine Bestimmung dieser Verordnung dahin gehend ausgelegt werden, dass hiermit von der Anwendung der im Rahmenbeschluss 2002/584/JI enthaltenen Bestimmungen abgewichen oder deren Anwendung verhindert wird. Die Entscheidung, eine Kennzeichnung im Hinblick auf die Nichtvollstreckung eines Europäischen Haftbefehls hinzuzufügen, sollte nur auf die im Rahmenbeschluss angegebenen Ablehnungsgründe gestützt sein.

(42) Wurde eine Kennzeichnung hinzugefügt und konnte der Aufenthaltsort der zum Zwecke der Übergabehaft gesuchten Person ermittelt werden, so sollte der Aufenthaltsort der Person immer der ausschreibenden Justizbehörde mitgeteilt werden, die daraufhin beschließen kann, der zuständigen Justizbehörde gemäß den Bestimmungen des Rahmenbeschlusses 2002/584/JI einen Europäischen Haftbefehl zu übermitteln.

(43) Die Mitgliedstaaten sollten die Möglichkeit haben, Ausschreibungen im SIS miteinander zu verknüpfen. Das Verknüpfen von zwei oder mehr Ausschreibungen sollte sich nicht auf die zu ergreifende Maßnahme, die Prüffrist für Ausschreibungen oder die Rechte des Zugriffs auf die Ausschreibungen auswirken.

(44) Ausschreibungen sollten nicht länger als für den spezifischen Zweck, zu dem die Eingabe erfolgte, erforderlich im SIS gespeichert werden. Die Prüffristen für die verschiedenen Ausschreibungskategorien sollten dem Zweck der jeweiligen Ausschreibungen angemessen sein. Sachfahndungsausschreibungen, die mit einer Personenausschreibung verknüpft sind, sollten nur so lange wie die Personenausschreibung beibehalten werden. Die Entscheidung, Personenausschreibungen beizubehalten, sollte sich auf eine umfassende individuelle Bewertung stützen. Die Mitgliedstaaten sollten Personen- und Sachfahndungsausschreibungen innerhalb der vorgeschriebenen Prüffristen überprüfen und Statistiken über die Zahl der Ausschreibungen führen, deren Erfassungsdauer verlängert worden ist.

(45) Die Eingabe einer Ausschreibung in das SIS und die Verlängerung der Ablauffrist sollte einer Verhältnismäßigkeitsprüfung unterliegen, bei der auch geprüft wird, ob Angemessenheit, Relevanz und Bedeutung des konkreten Falles die Eingabe einer Ausschreibung in das SIS hinreichend rechtfertigen. Bei terroristischen Straftaten sollte davon ausgegangen werden, dass Angemessenheit, Relevanz und Bedeutung des Falles eine Ausschreibung im SIS hinreichend rechtfertigen. Aus Gründen der öffentlichen oder der nationalen Sicherheit sollten die Mitgliedstaaten ausnahmsweise von der Eingabe einer Ausschreibung in das SIS absehen können, wenn davon auszugehen ist, dass dadurch behördliche oder rechtliche Untersuchungen, Ermittlungen oder Verfahren behindert würden.

(46) Für die Löschung von Ausschreibungen müssen Regeln festgelegt werden. Eine Ausschreibung sollte nur so lange im SIS gespeichert werden, bis der Zweck, für den sie eingegeben wurde, erfüllt ist. Wegen der unterschiedlichen Handhabung durch die Mitgliedstaaten bei der Festlegung des Zeitpunkts, zu dem eine Ausschreibung ihren Zweck erfüllt hat, sollten für jede Ausschreibungskategorie genaue Kriterien dafür festgelegt werden, wann eine Ausschreibung zu löschen ist.

(47) Die Integrität der SIS-Daten ist von größter Bedeutung. Daher sollten für die Verarbeitung von SIS-Daten sowohl auf zentraler als auch auf nationaler Ebene angemessene Schutzmaßnahmen vorgesehen werden, die die durchgängige Sicherheit der Daten gewährleisten. Für die an der Datenverarbeitung beteiligten Behörden sollten die Sicherheitsanforderungen dieser Verordnung verbindlich sein und sollten einem einheitlichen Meldeverfahren für Zwischenfälle unterliegen. Ihr Personal sollte in geeigneter Weise geschult sein, und es sollte über alle diesbezüglichen Straftatbestände und Sanktionen unterrichtet werden.

(48) Im SIS verarbeitete Daten sowie damit verbundene Zusatzinformationen, die gemäß dieser Verordnung ausgetauscht werden, sollten Drittländern oder internationalen Organisationen nicht übermittelt oder zur Verfügung gestellt werden.

(49) Es ist angezeigt, den für die Zulassung von Kraft-, Wasser- und Luftfahrzeugen zuständigen Dienststellen Zugriff auf das SIS zu gewähren, damit diese prüfen können, ob das betreffende Fahrzeug bereits in einem Mitgliedstaat zur Sicherstellung ausgeschrieben ist. Es ist ferner angezeigt, den für die Zulassung von Schusswaffen zuständigen Dienststellen Zugriff auf das SIS zu gewähren, damit diese prüfen können, ob die betreffende Schusswaffe bereits in einem Mitgliedstaat zur Sicherstellung ausgeschrieben ist oder ob die Person, die den Antrag auf Registrierung gestellt hat, ausgeschrieben ist.

(50) Ein direkter Zugriff auf das SIS sollte nur zuständigen staatlichen Stellen gewährt werden. Dabei sollte sich der Zugriff auf Ausschreibungen der entsprechenden Fahrzeuge und Zulassungsbescheinigungen oder Kennzeichen bzw. auf Ausschreibungen von Schusswaffen und Personen, die die Zulassung beantragen, beschränken. Solche Stellen sollten den Polizeibehörden jeden Treffer im SIS melden, die dann die weiteren Maßnahmen entsprechend der betreffenden SIS-Ausschreibung ergreifen und den Treffer über die SIRENE-Büros dem ausschreibenden Mitgliedstaat melden sollten.

(51) Unbeschadet spezifischerer Vorschriften in der vorliegenden Verordnung sollten die nach der Richtlinie (EU) 2016/680 erlassenen nationalen Rechts- und Verwaltungsvorschriften Anwendung auf die Verarbeitung — einschließlich der Erhebung und Übermittlung — personenbezogener Daten nach Maßgabe der vorliegenden Verordnung durch die nationalen zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung terroristischer oder sonstiger schwerer Straftaten oder der Strafvollstreckung finden. Der Zugriff auf die in das SIS eingegebenen Daten und das Recht auf Abfrage dieser Daten durch zuständige nationale Behörden, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung terroristischer oder sonstiger schwerer Straftaten oder die Strafvollstreckung verantwortlich sind, unterliegen sämtlichen einschlägigen Bestimmungen der vorliegenden Verordnung und der in nationales Recht umgesetzten Richtlinie (EU) 2016/680, und insbesondere der Überwachung durch die in der Richtlinie (EU) 2016/680 genannten Aufsichtsbehörden.

(52) Unbeschadet spezifischerer Vorschriften in der vorliegenden Verordnung für die Verarbeitung personenbezogener Daten sollte die Verordnung (EU) 2016/679 Anwendung auf die nach Maßgabe dieser Verordnung durchgeführte Verarbeitung personenbezogener Daten durch die Mitgliedstaaten finden, es sei denn, diese Verarbeitung erfolgt durch die nationalen zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung terroristischer oder sonstiger schwerer Straftaten.

(53) Für die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Union bei der Wahrnehmung ihrer Aufgaben aufgrund der vorliegenden Verordnung sollte die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([1]) gelten.

(54) Für die Verarbeitung personenbezogener Daten gemäß der vorliegenden Verordnung durch Europol sollte die Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates ([2]) gelten.

(55) Stellt sich bei von nationalen Mitgliedern von Eurojust und den sie unterstützenden Personen im SIS durchgeführten Abfragen heraus, dass eine von einem Mitgliedstaat eingegebene Ausschreibung vorliegt, kann Eurojust die beantragten Maßnahmen nicht ergreifen. Daher sollte Eurojust den betreffenden Mitgliedstaat unterrichten, damit dieser den Fall weiterverfolgen kann.

(56) Die zuständigen Behörden sollten bei der Nutzung des SIS sicherstellen, dass die Würde und die Integrität der Person, deren Daten verarbeitet werden, geachtet werden. Bei der Verarbeitung personenbezogener Daten für die Zwecke dieser Verordnung sollten keine Personen aufgrund des Geschlechts, der Rasse oder der ethnischen Herkunft, der Religion oder der Weltanschauung, einer Behinderung, des Alters oder der sexuellen Ausrichtung diskriminiert werden.

(57) Was die Geheimhaltung anbelangt, so sollten die Beamten und sonstigen Bediensteten, die in Verbindung mit dem SIS eingesetzt oder tätig werden, den einschlägigen Bestimmungen des Statuts der Beamten der Europäischen Union und den Beschäftigungsbedingungen für die sonstigen Bediensteten der Union unterliegen, die in der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates ([3]) (im Folgenden „Statut“) niedergelegt sind.

(58) Sowohl die Mitgliedstaaten als auch eu-LISA sollten über Sicherheitspläne verfügen, um die Erfüllung der Sicherheitsanforderungen zu erleichtern; ferner sollten sie zusammenarbeiten, um Sicherheitsfragen von einem gemeinsamen Blickwinkel aus anzugehen.

(59) Die unabhängigen nationalen Aufsichtsbehörden, die in der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 genannt werden (im Folgenden „Aufsichtsbehörden“), sollten die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten gemäß der vorliegenden Verordnung überwachen, einschließlich des Austauschs von Zusatzinformationen. Den Aufsichtsbehörden sollten ausreichende Mittel zur Erfüllung dieser Aufgabe zur Verfügung gestellt werden. Die Rechte der betroffenen Person auf Auskunft, Berichtigung und Löschung ihrer im SIS gespeicherten personenbezogenen Daten und etwaige Rechtsbehelfe vor nationalen Gerichten sowie die gegenseitige Anerkennung von Entscheidungen sollten geregelt werden. Außerdem sollten die Mitgliedstaaten zur Vorlage jährlicher Statistiken verpflichtet werden.

(60) Die Aufsichtsbehörden sollten gewährleisten, dass die Datenverarbeitungsvorgänge in den nationalen Systemen ihres jeweiligen Mitgliedstaats mindestens alle vier Jahre nach internationalen Prüfstandards überprüft werden. Die Prüfung sollte entweder von den Aufsichtsbehörden durchgeführt werden, oder die Aufsichtsbehörden sollten einen unabhängigen Datenschutzprüfer direkt damit beauftragen. Der unabhängige Prüfer sollte kontinuierlich unter der Kontrolle und der Verantwortung der betreffenden Aufsichtsbehörden arbeiten, die deshalb den Prüfer selbst anweisen und Zweck, Tragweite und Methodik der Prüfung klar vorgeben, Leitlinien festlegen sowie die Prüfung und ihre endgültigen Ergebnisse beaufsichtigen sollten.

([1]) 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).

([2]) 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]) ABl. L 56 vom 4.3.1968, S. 1.

(61) Der Europäische Datenschutzbeauftragte sollte die Tätigkeiten der Organe und Einrichtungen der Union im Zusammenhang mit der Verarbeitung personenbezogener Daten gemäß dieser Verordnung überwachen. Der Europäische Datenschutzbeauftragte und die Aufsichtsbehörden sollten bei der Überwachung des SIS zusammenarbeiten.

(62) Dem Europäischen Datenschutzbeauftragten sollten ausreichende Mittel zur Erfüllung der ihm nach dieser Verordnung übertragenen Aufgaben zur Verfügung gestellt werden, einschließlich der Unterstützung durch Sachverständige für biometrische Daten.

(63) Nach der Verordnung (EU) 2016/794 hat Europol die Tätigkeit der nationalen zuständigen Behörden sowie deren Zusammenarbeit bei der Bekämpfung von Terrorismus und schwerer Kriminalität zu unterstützen und zu verstärken sowie Bedrohungs- und andere Analysen zu erstellen. Die Möglichkeiten von Europol, nationalen Strafverfolgungsbehörden umfassende operative und analytische Produkte zu liefern, die den Menschenhandel und die sexuelle Ausbeutung von Kindern, einschließlich im Internet, betreffen, sollten durch die Ausweitung der Zugriffsrechte von Europol auf Ausschreibungen von Vermissten weiter verbessert werden. Dies würde dazu beitragen, dass diese Straftaten besser verhütet, die möglichen Opfer geschützt und die Täter ermittelt werden können. Das bei Europol eingerichtete Europäische Zentrum zur Bekämpfung der Cyberkriminalität würde ebenfalls von dem Europol eingeräumten Zugriff auf Ausschreibungen von Vermissten profitieren, insbesondere in Fällen von reisenden Sexualstraftätern und des sexuellen Missbrauchs von Kindern im Internet, in denen Straftäter oftmals angeben, dass sie Kontakt zu Kindern haben oder aufnehmen können, die möglicherweise als vermisst gemeldet wurden.

(64) Um die Lücke beim Informationsaustausch über Terrorismus, insbesondere über ausländische terroristische Kämpfer — bei denen die Überwachung der Bewegungen von entscheidender Bedeutung ist — zu schließen, werden die Mitgliedstaaten ermutigt, Informationen über Aktivitäten mit Terrorismusbezug an Europol weiterzugeben. Dieser Informationsaustausch sollte im Wege des Austauschs von Zusatzinformationen mit Europol über die betreffenden Ausschreibungen erfolgen. Zu diesem Zweck sollte Europol eine Verbindung zur Kommunikationsinfrastruktur herstellen.

(65) Ferner müssen für Europol klare Regeln für die Verarbeitung und das Herunterladen von SIS-Daten festgelegt werden, damit Europol das SIS — unter Einhaltung der Datenschutzstandards gemäß der vorliegenden Verordnung und der Verordnung (EU) 2016/794 — umfassend nutzen kann. Stellt sich bei von Europol im SIS durchgeführten Abfragen heraus, dass eine von einem Mitgliedstaat eingegebene Ausschreibung vorliegt, kann Europol nicht die erforderlichen Maßnahmen ergreifen. Daher sollte Europol den betreffenden Mitgliedstaat im Wege des Austauschs von Zusatzinformationen mit dem jeweiligen SIRENE-Büro unterrichten, damit dieser Mitgliedstaat den Fall weiterverfolgen kann.

(66) In der Verordnung (EU) 2016/1624 des Europäischen Parlaments und des Rates [1] ist für die Zwecke jener Verordnung vorgesehen, dass der Einsatzmitgliedstaat die von der Europäischen Agentur für die Grenz- und Küstenwache entsandten Mitglieder von Teams gemäß Artikel 2 Nummer 8 der jener Verordnung ermächtigt, Datenbanken der Union abzufragen, wenn dies für die Erfüllung der im Einsatzplan für Grenzübertrittskontrollen, Grenzüberwachung und Rückkehr jeweils festgelegten Ziele erforderlich ist. Andere einschlägige Agenturen der Union, insbesondere das Europäische Unterstützungsbüro für Asylfragen und Europol, können als Teil der Teams zur Unterstützung der Migrationssteuerung auch Sachverständige entsenden, die nicht dem Personal dieser Agenturen der Union angehören. Ziel des Einsatzes der Teams gemäß Artikel 2 Nummern 8 und 9 der jener Verordnung ist eine technische und operative Verstärkung für die ersuchenden Mitgliedstaaten — vor allem diejenigen, die einem unverhältnismäßigen Migrationsdruck ausgesetzt sind. Damit die in Artikel 2 Nummern 8 und 9 jener Verordnung genannten Teams ihre Aufgaben erfüllen können, ist der Zugriff auf das SIS über eine technische Schnittstelle erforderlich, die die Europäische Agentur für die Grenz- und Küstenwache mit dem zentralen SIS verbindet. Stellt sich bei von den Teams gemäß Artikel 2 Nummern 8 und 9 der Verordnung (EU) 2016/1624 oder bei von den Personalteams durchgeführten Abfragen heraus, dass eine von einem Mitgliedstaat eingegebene Ausschreibung vorliegt, so kann das Teammitglied oder das Personal die erforderliche Maßnahme nur treffen, wenn es vom Einsatzmitgliedstaat dazu ermächtigt wird. Daher sollte der Einsatzmitgliedstaat unterrichtet werden, damit dieser den Fall weiterverfolgen kann. Der Einsatzmitgliedstaat sollte den ausschreibenden Mitgliedstaat im Wege des Austauschs von Zusatzinformationen von dem Treffer in Kenntnis setzen.

(67) Bestimmte Aspekte des SIS 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 zählen beispielsweise technische Vorschriften für die Eingabe, Aktualisierung, Löschung und Abfrage von Daten und die Datenqualität, sowie Regeln im Zusammenhang mit biometrischen Daten, Regeln über die

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

Vereinbarkeit und die Rangfolge von Ausschreibungen, über Verknüpfungen zwischen Ausschreibungen, über die Festlegung des Ablaufzeitpunkts von Ausschreibungen innerhalb der maximalen Frist und über den Austausch von Zusatzinformationen. Daher sollten der Kommission Durchführungsbefugnisse für diese Aspekte übertragen werden. Bei den technischen Vorschriften über die Abfrage von Ausschreibungen sollte auf ein reibungsloses Funktionieren der nationalen Anwendungen geachtet werden.

(68) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([1]) ausgeübt werden. Die Verfahren für die Annahme von Durchführungsrechtsakten gemäß dieser Verordnung und der Verordnung (EU) 2018/1861sollten identisch sein.

(69) Zur Gewährleistung der Transparenz sollte eu-LISA zwei Jahre nach Inbetriebnahme des SIS gemäß dieser Verordnung einen Bericht über die technische Funktionsweise des zentralen SIS und der Kommunikationsinfrastruktur, einschließlich ihrer Sicherheit, und über den bilateralen und multilateralen Austausch von Zusatzinformationen vorlegen. Die Kommission sollte alle vier Jahre eine Gesamtbewertung vornehmen.

(70) Um das reibungslose Funktionieren des SIS sicherzustellen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte im Hinblick auf neue Unterkategorien von Sachen, die im Rahmen von Sachfahndungsausschreibungen zur Sicherstellung oder Beweissicherung in Strafverfahren gesucht werden, und die Bestimmung der Umstände, unter denen Lichtbilder und Gesichtsbilder in einem anderen Kontext als an regulären Grenzübergangsstellen zur Identifizierung von Personen genutzt werden dürfen, zu erlassen. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung ([2]) niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung der delegierten Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(71) Da die Ziele dieser Verordnung, nämlich die Einrichtung eines Informationssystems der Union und die diesbezügliche Regelung sowie der Austausch damit verbundener Zusatzinformationen, von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr aufgrund ihrer Beschaffenheit 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.

(72) Diese Verordnung steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden. Diese Verordnung wahrt insbesondere den Schutz personenbezogener Daten gemäß Artikel 8 der Charta der Grundrechte der Europäischen Union in vollem Umfang und zielt dabei darauf ab, ein sicheres Umfeld für alle Personen, die sich im Gebiet der Union aufhalten, und den besonderen Schutz von Kindern vor Menschenhandel und Entführung zu gewährleisten. In Fällen, in denen auch Kinder betroffen sind, sollte das Wohl des Kindes vorrangig berücksichtigt werden.

(73) 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. Da diese Verordnung den Schengen-Besitzstand ergänzt, beschließt Dänemark gemäß Artikel 4 des genannten Protokolls innerhalb von sechs Monaten, nachdem der Rat diese Verordnung angenommen hat, ob es sie in nationales Recht umsetzt.

(74) Das Vereinigte Königreich beteiligt sich an dieser Verordnung im Einklang mit Artikel 5 Absatz 1 des dem EUV und dem AEUV beigefügten Protokolls Nr. 19 über den in den Rahmen der Europäischen Union einbezogenen Schengen-Besitzstand sowie Artikel 8 Absatz 2 des Beschlusses 2000/365/EG des Rates ([3]).

(75) Irland beteiligt sich an dieser Verordnung im Einklang mit Artikel 5 Absatz 1 des dem EUV und AEUV beigefügten Protokolls Nr. 19 sowie Artikel 6 Absatz 2 des Beschlusses 2002/192/EG des Rates ([4]).

([1]) 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).

([2]) ABl. L 123 vom 12.5.2016, S. 1.

([3]) Beschluss 2000/365/EG des Rates vom 29. Mai 2000 zum Antrag des Vereinigten Königreichs Großbritannien und Nordirland, einzelne Bestimmungen des Schengen-Besitzstands auf es anzuwenden (ABl. L 131 vom 1.6.2000, S. 43).

([4]) Beschluss 2002/192/EG des Rates vom 28. Februar 2002 zum Antrag Irlands auf Anwendung einzelner Bestimmungen des Schengen-Besitzstands auf Irland (ABl. L 64 vom 7.3.2002, S. 20).

(76) Für Island und Norwegen stellt diese Verordnung eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands im Sinne des Übereinkommens zwischen dem Rat der Europäischen Union sowie der Republik Island und dem Königreich Norwegen über die Assoziierung der beiden letztgenannten Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands ([1]) dar, die zu dem in Artikel 1 Buchstabe G des Beschlusses 1999/437/EG des Rates ([2]) genannten Bereich gehören.

(77) Für die Schweiz stellt diese Verordnung eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands im Sinne des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands ([3]) dar, die zu dem in Artikel 1 Buchstabe G des Beschlusses 1999/437/EG in Verbindung mit Artikel 3 des Beschlusses 2008/149/JI des Rates ([4]) genannten Bereich gehören.

(78) Für Liechtenstein stellt diese Verordnung eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands im Sinne des Protokolls zwischen der Europäischen Union, der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zu dem Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands ([5]) dar, die zu dem in Artikel 1 Buchstabe G des Beschlusses 1999/437/EG in Verbindung mit Artikel 3 des Beschlusses 2011/349/EU des Rates ([6]) genannten Bereich gehören.

(79) Für Bulgarien und Rumänien stellt diese Verordnung einen auf dem Schengen-Besitzstand aufbauenden oder anderweitig damit zusammenhängenden Rechtsakt im Sinne des Artikels 4 Absatz 2 der Beitrittsakte von 2005 dar und sollte in Verbindung mit den Beschlüssen 2010/365/EU ([7]) und (EU) 2018/934 ([8]) des Rates gelesen werden.

(80) Für Kroatien stellt diese Verordnung einen auf dem Schengen-Besitzstand aufbauenden oder anderweitig damit zusammenhängenden Rechtsakt im Sinne des Artikels 4 Absatz 2 der Beitrittsakte von 2011 dar und sollte in Verbindung mit dem Beschluss (EU) 2017/733 des Rates ([9]) gelesen werden.

(81) Für Zypern stellt diese Verordnung einen auf dem Schengen-Besitzstand aufbauenden oder anderweitig damit zusammenhängenden Rechtsakt im Sinne des Artikels 3 Absatz 2 der Beitrittsakte von 2003 dar.

(82) Diese Verordnung sollte auf Irland zu einem Zeitpunkt Anwendung finden, der nach den Verfahren in den einschlägigen Rechtsinstrumenten betreffend die Anwendung des Schengen-Besitzstands auf diesen Staat festgelegt wird.

(83) Mit dieser Verordnung wird eine Reihe von Verbesserungen des SIS eingeführt, die seine Wirksamkeit steigern, den Datenschutz verstärken und die Zugriffsrechte ausweiten. Einige dieser Verbesserungen erfordern keine komplexen technischen Entwicklungen, während für andere technische Änderungen in unterschiedlichem Ausmaß vonnöten sind. Damit die Verbesserungen des Systems den Endnutzern so bald wie möglich zur Verfügung stehen können, werden mit dieser Verordnung Änderungen des Beschlusses 2007/533/JI in mehreren Phasen eingeführt. Einige Verbesserungen des Systems sollten sofort nach Inkrafttreten dieser Verordnung gelten, während andere entweder ein Jahr oder zwei Jahre nach ihrem Inkrafttreten gelten sollten. Diese Verordnung sollte innerhalb von drei Jahren nach ihrem Inkrafttreten in ihrer Gesamtheit gelten. Damit Verzögerungen bei der Anwendung dieser Verordnung vermieden werden, sollte ihre in mehreren Schritten erfolgende Umsetzung genau überwacht werden.

([1]) ABl. L 176 vom 10.7.1999, S. 36.

([2]) Beschluss 1999/437/EG des Rates vom 17. Mai 1999 zum Erlass bestimmter Durchführungsvorschriften zu dem Übereinkommen zwischen dem Rat der Europäischen Union und der Republik Island und dem Königreich Norwegen über die Assoziierung dieser beiden Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands (ABl. L 176 vom 10.7.1999, S. 31).

([3]) ABl. L 53 vom 27.2.2008, S. 52.

([4]) Beschluss 2008/149/JI des Rates vom 28. Januar 2008 über den Abschluss — im Namen der Europäischen Union — des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands (ABl. L 53 vom 27.2.2008, S. 50).

([5]) ABl. L 160 vom 18.6.2011, S. 21.

([6]) Beschluss 2011/349/EU des Rates vom 7. März 2011 über den Abschluss — im Namen der Europäischen Union — des Protokolls zwischen der Europäischen Union, der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zum Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, insbesondere in Bezug auf die justizielle Zusammenarbeit in Strafsachen und die polizeiliche Zusammenarbeit (ABl. L 160 vom 18.6.2011, S. 1).

([7]) Beschluss 2010/365/EU des Rates vom 29. Juni 2010 über die Anwendung der Bestimmungen des Schengen-Besitzstands über das Schengener Informationssystem in der Republik Bulgarien und Rumänien (ABl. L 166 vom 1.7.2010, S. 17).

([8]) Beschluss (EU) 2018/934 des Rates vom 25. Juni 2018 über das Inkraftsetzen der übrigen Bestimmungen des Schengen-Besitzstands über das Schengener Informationssystem in der Republik Bulgarien und in Rumänien (ABl. L 165 vom 2.7.2018, S. 37).

([9]) Beschluss (EU) 2017/733 des Rates vom 25. April 2017 über die Anwendung der Bestimmungen des Schengen-Besitzstands über das Schengener Informationssystem in der Republik Kroatien (ABl. L 108 vom 26.4.2017, S. 31).

(84) Die Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates ([1]), der Beschluss 2007/533/JI und der Beschluss 2010/261/EU der Kommission ([2]) sollten mit Wirkung ab dem Zeitpunkt der vollständigen Geltung der vorliegenden Verordnung aufgehoben werden.

(85) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates ([3]) angehört und hat am 3. Mai 2017 eine Stellungnahme abgegeben —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Allgemeines Ziel des SIS

Das SIS hat zum Ziel, anhand der über dieses System mitgeteilten Informationen ein hohes Maß an Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts der Union, einschließlich der Wahrung der öffentlichen Sicherheit und Ordnung sowie des Schutzes der Sicherheit im Hoheitsgebiet der Mitgliedstaaten, zu gewährleisten und die Anwendung der Bestimmungen des von Teil 3 Titel V Kapitel 4 und 5 des AEUV im Bereich des Personenverkehrs in ihrem Hoheitsgebiet sicherzustellen.

Artikel 2

Gegenstand

(1) In dieser Verordnung werden die Voraussetzungen und Verfahren für die Eingabe von Personen- und Sachfahndungsausschreibungen in das SIS und deren Verarbeitung sowie für den Austausch von Zusatzinformationen und ergänzenden Daten zum Zwecke der polizeilichen und justiziellen Zusammenarbeit in Strafsachen festgelegt.

(2) Diese Verordnung enthält außerdem Bestimmungen über die Systemarchitektur des SIS, über die Zuständigkeiten der Mitgliedstaaten und der Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (im Folgenden „eu-LISA"), über die Datenverarbeitung, über die Rechte der betroffenen Personen und über die Haftung.

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Ausschreibung" einen in das SIS eingegebenen Datensatz, der den zuständigen Behörden die Identifizierung einer Person oder Sache im Hinblick auf die Ergreifung spezifischer Maßnahmen ermöglicht;
2. „Zusatzinformationen" Informationen, die nicht zu den im SIS gespeicherten Ausschreibungsdaten gehören, aber mit SIS-Ausschreibungen verknüpft sind und in folgenden Fällen über die SIRENE-Büros ausgetauscht werden:
   a) bei Eingabe einer Ausschreibung, damit die Mitgliedstaaten einander konsultieren oder unterrichten können;
   b) nach einem Treffer, damit die erforderlichen Maßnahmen ergriffen werden können;
   c) in Fällen, in denen die ersuchten Maßnahmen nicht ergriffen werden können;
   d) bei Fragen der Qualität der SIS-Daten;
   e) bei Fragen der Vereinbarkeit und Rangfolge von Ausschreibungen;
   f) bei Fragen des Auskunftsrechts;
3. „ergänzende Daten" im SIS gespeicherte und mit SIS-Ausschreibungen verknüpfte Daten, die den zuständigen Behörden unmittelbar zur Verfügung stehen müssen, wenn eine Person, zu der Daten in das SIS eingegeben wurden, als Ergebnis einer Abfrage im SIS aufgefunden wird;

([1]) Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über den Zugang von für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständigen Dienststellen der Mitgliedstaaten zum Schengener Informationssystem der zweiten Generation (SIS II) (ABl. L 381 vom 28.12.2006, S. 1).

([2]) Beschluss 2010/261/EU der Kommission vom 4. Mai 2010 über den Sicherheitsplan für das zentrale SIS II und die Kommunikationsinfrastruktur (ABl. L 112 vom 5.5.2010, S. 31).

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

4. „personenbezogene Daten“ personenbezogene Daten im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) 2016/679;

5. „Verarbeitung personenbezogener Daten“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, das Protokollieren, die Organisation, das Ordnen, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, die Löschung oder die Vernichtung;

6. „Übereinstimmung“ das Eintreten folgender Schritte:

   a) Eine Abfrage wurde durch einen Endnutzer im SIS durchgeführt;

   b) diese Abfrage hat ergeben, dass ein anderer Mitgliedstaat eine Ausschreibung in das SIS eingegeben hat; und

   c) die Daten der Ausschreibung im SIS stimmen mit den für die Abfrage verwendeten Daten überein;

7. „Treffer“ eine Übereinstimmung, die folgende Kriterien erfüllt:

   a) Sie wurde bestätigt, und zwar

      i) vom Endnutzer oder

      ii) von der zuständigen Behörde im Einklang mit den nationalen Verfahren für den Fall, dass die betreffende Übereinstimmung auf der Grundlage eines Abgleichs von biometrischen Daten erzielt wurde,

      und

   b) es wurde um weitere Maßnahmen ersucht;

8. „Kennzeichnung“ die Aussetzung der Gültigkeit einer Ausschreibung auf nationaler Ebene, die Ausschreibungen zwecks Festnahme, Ausschreibungen von vermissten und schutzbedürftigen Personen und Ausschreibungen zu verdeckten Kontrollen, Ermittlungsanfragen und gezielten Kontrollen hinzugefügt werden kann;

9. „ausschreibender Mitgliedstaat“ den Mitgliedstaat, der die Ausschreibung in das SIS eingegeben hat;

10. „vollziehender Mitgliedstaat“ den Mitgliedstaat, der nach einem Treffer die erforderlichen Maßnahmen ergreift oder ergriffen hat;

11. „Endnutzer“ ein Mitglied des Personals einer zuständigen Behörde, das berechtigt ist, direkt Abfragen in der CS-SIS, dem N.SIS oder einer technischen Kopie davon durchführen;

12. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen oder physiologischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, d. h. Lichtbilder, Gesichtsbilder, daktyloskopische Daten und DNA-Profil;

13. „daktyloskopische Daten“ Daten zu Fingerabdrücken und Handflächenabdrücken, die aufgrund ihrer Einzigartigkeit und der darin enthaltenen Bezugspunkte präzise und schlüssige Abgleiche zur Identität einer Person ermöglichen;

14. „Gesichtsbild“ eine digitale Aufnahme des Gesichts, in ausreichender Bildauflösung und Qualität für den automatisierten biometrischen Abgleich;

15. „DNA-Profil“ einen Buchstaben- beziehungsweise Zahlencode, der eine Reihe von Identifikationsmerkmalen des nichtcodierenden Teils einer analysierten menschlichen DNA-Probe, d. h. der speziellen Molekularstruktur an den verschiedenen DNA-Loci, abbildet;

16. „terroristische Straftat“ eine Straftat nach nationalem Recht, die in den Artikeln 3 bis 14 der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates ([1]) aufgeführt ist oder die für die Mitgliedstaaten, die nicht durch die genannte Richtlinie gebunden sind, einer dieser Straftaten gleichwertig ist;

17. „Gefahr für die öffentliche Gesundheit“ eine Gefahr für die öffentliche Gesundheit im Sinne von Artikel 2 Nummer 21 der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates ([2]).

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

([2]) Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex) (ABl. L 77 vom 23.3.2016, S. 1).

Artikel 4

Systemarchitektur und Betrieb des SIS

(1) Das SIS besteht aus

a) einem zentralen System (im Folgenden „zentrales SIS“), zu dem folgende Elemente gehören:

i) eine technische Unterstützungseinheit (im Folgenden „CS-SIS“), die eine Datenbank (im Folgenden „SIS-Datenbank“) enthält, einschließlich eines Back-up-CS-SIS;

ii) eine einheitliche nationale Schnittstelle (im Folgenden „NI-SIS“);

b) einem nationalen System (im Folgenden „N.SIS“) in jedem einzelnen Mitgliedstaat, das aus den nationalen, mit dem zentralen SIS kommunizierenden Datensystemen besteht, einschließlich mindestens einem nationalen oder gemeinsamen Back-up-N.SIS; und

c) einer Kommunikationsinfrastruktur zwischen der CS-SIS, der Back-up-CS-SIS und der NI-SIS (im Folgenden „Kommunikationsinfrastruktur“), die ein verschlüsseltes virtuelles Netz speziell für SIS-Daten und den Austausch von Daten zwischen SIRENE-Büros nach Artikel 7 Absatz 2 zur Verfügung stellt.

Ein N.SIS gemäß Buchstabe b kann einen Datenbestand (im Folgenden „nationale Kopie“) umfassen, der eine vollständige oder Teilkopie der SIS-Datenbank enthält. Zwei oder mehr Mitgliedstaaten können in einem ihrer N.SIS eine gemeinsame Kopie erstellen, die von diesen Mitgliedstaaten gemeinsam genutzt werden kann. Eine derartige gemeinsame Kopie gilt als die nationale Kopie jedes dieser Mitgliedstaaten.

Ein gemeinsames Back-up-N.SIS gemäß Buchstabe b kann gemeinsam von zwei oder mehr Mitgliedstaaten genutzt werden. In diesen Fällen gilt das gemeinsame Back-up-N.SIS als Back-up-N.SIS jedes dieser Mitgliedstaaten. Das N.SIS und sein Back-up können gleichzeitig verwendet werden, um die ununterbrochene Verfügbarkeit für die Endnutzer zu gewährleisten.

Mitgliedstaaten, die eine gemeinsame Kopie oder ein gemeinsames Back-up-N.SIS zur gemeinsamen Nutzung erstellen möchten, vereinbaren ihre jeweiligen Zuständigkeiten schriftlich. Die Mitgliedstaaten unterrichten die Kommission über ihre Vereinbarung.

Die Kommunikationsinfrastruktur muss die ununterbrochene Verfügbarkeit des SIS unterstützen und dazu beitragen, diese zu gewährleisten. Sie muss redundante und getrennte Wege für die Verbindungen zwischen der CS-SIS und der Back-up-CS-SIS sowie für die Verbindungen zwischen jedem nationalen SIS-Netzzugangspunkt und der CS-SIS und der Back-up-CS-SIS umfassen.

(2) Die Mitgliedstaaten nehmen die Eingabe, Aktualisierung, Löschung und Abfrage von SIS-Daten jeweils über ihr eigenes N.SIS vor. Mitgliedstaaten, die eine nationale Teilkopie oder eine vollständige nationale Kopie bzw. eine gemeinsame Teilkopie oder eine gemeinsame vollständige Kopie verwenden, stellen diese Kopie innerhalb des Hoheitsgebiets jedes dieser Mitgliedstaaten zur Abfrage im automatisierten Verfahren zur Verfügung. Die nationale oder gemeinsame Teilkopie enthält mindestens die in Artikel 20 Absatz 3 Buchstaben a bis v aufgeführten Daten. Es darf nicht möglich sein, die Datensätze der N.SIS anderer Mitgliedstaaten abzufragen, außer im Fall gemeinsamer Kopien.

(3) Die CS-SIS ist für die technische Aufsicht und die Verwaltung zuständig und verfügt über eine Back-up-CS-SIS, die bei einem Ausfall der Haupt-CS-SIS alle Funktionen dieses Systems übernehmen kann. Die CS-SIS und die Back-up-CS-SIS befinden sich an den beiden technischen Standorten von eu-LISA.

(4) eu-LISA wendet technische Lösungen an, um die ununterbrochene Verfügbarkeit des SIS entweder dadurch zu stärken, dass ein gleichzeitiger Betrieb der CS-SIS und der Back-up-CS-SIS erfolgt, sofern die Back-up-CS-SIS weiterhin in der Lage ist, bei einem Ausfall der CS-SIS den Betrieb des SIS sicherzustellen, oder dadurch, dass das System oder dessen Bestandteile dupliziert werden. Ungeachtet der in Artikel 10 der Verordnung (EU) 2018/1726. festgelegten Verfahrenserfordernisse erstellt eu-LISA spätestens am 28. Dezember 2019 eine Studie zu den Optionen für technische Lösungen, die eine unabhängige Folgenabschätzung und eine unabhängige Kosten-Nutzen-Analyse enthält.

(5) Falls dies unter außergewöhnlichen Umständen erforderlich ist, kann eu-LISA vorübergehend eine zusätzliche Kopie der SIS-Datenbank erstellen.

(6) Die CS-SIS leistet die erforderlichen Dienste für die Eingabe und Verarbeitung der SIS-Daten, einschließlich der Abfrage der SIS-Datenbank. Für die Mitgliedstaaten, die eine nationale oder gemeinsame Kopie verwenden, übernimmt die CS-SIS Folgendes:

a) Bereitstellung der Online-Aktualisierungen für die nationalen Kopien;

b) Gewährleistung der Synchronisierung und Kohärenz zwischen den nationalen Kopien und der SIS-Datenbank; und

c) Bereitstellung der Vorgänge für die Initialisierung und Wiederherstellung der nationalen Kopien.

(7) Die CS-SIS gewährleistet eine ununterbrochene Verfügbarkeit.

Artikel 5

Kosten

(1) Die Kosten für den Betrieb, die Wartung und die Weiterentwicklung des zentralen SIS und der Kommunikationsinfrastruktur werden aus dem Gesamthaushaltsplan der Union finanziert. Diese Kosten beinhalten in Bezug auf die CS-SIS ausgeführten Arbeiten zur Gewährleistung der in Artikel 4 Absatz 6 genannten Dienste.

(2) Die Kosten für die Einrichtung, den Betrieb, die Wartung und die Weiterentwicklung der einzelnen N.SIS werden von dem jeweiligen Mitgliedstaat getragen.

KAPITEL II

Zuständigkeiten der Mitgliedstaaten

Artikel 6

Nationale Systeme

Jeder Mitgliedstaat ist dafür zuständig, dass sein N.SIS errichtet, betrieben, gewartet sowie weiterentwickelt und an die NI-SIS angeschlossen wird.

Jeder Mitgliedstaat ist dafür zuständig, die ununterbrochene Verfügbarkeit der SIS-Daten für die Endnutzer zu gewährleisten.

Jeder Mitgliedstaat übermittelt seine Ausschreibungen über sein N.SIS.

Artikel 7

N.SIS-Stelle und SIRENE-Büro

(1) Jeder Mitgliedstaat bestimmt eine Behörde (im Folgenden „N.SIS-Stelle"), die die zentrale Zuständigkeit für sein N.SIS hat.

Diese Behörde ist für das reibungslose Funktionieren und die Sicherheit des N.SIS verantwortlich, gewährleistet den Zugriff der zuständigen Behörden auf das SIS und trifft die erforderlichen Maßnahmen zur Gewährleistung der Einhaltung dieser Verordnung. Sie ist dafür zuständig, dass sämtliche Funktionen des SIS den Endnutzern in geeigneter Weise zur Verfügung gestellt werden.

(2) Jeder Mitgliedstaat bestimmt eine nationale Behörde (im Folgenden „SIRENE-Büro"), die 24 Stunden pro Tag und 7 Tage die Woche einsatzfähig sein muss und den Austausch und die Verfügbarkeit aller Zusatzinformationen im Einklang mit dem SIRENE-Handbuch gewährleistet. Jedes SIRENE-Büro dient seinem Mitgliedstaat als einzige Kontaktstelle für den Austausch von Zusatzinformationen zu den Ausschreibungen und für die Einleitung der geforderten Maßnahmen, wenn Ausschreibungen zu Personen oder Sachen in das SIS aufgenommen wurden und diese Personen oder Sachen infolge eines Treffers aufgefunden werden.

Jedes SIRENE-Büro muss — im Einklang mit nationalem Recht — über einen leichten direkten oder indirekten Zugang zu allen einschlägigen nationalen Informationen, einschließlich nationalen Datenbanken und allen Informationen zu den Ausschreibungen seines Mitgliedstaats, und zur Beratung durch Experten verfügen, damit es in der Lage ist, rasch und innerhalb der in Artikel 8 vorgesehenen Fristen auf Ersuchen um Zusatzinformationen zu reagieren.

Die SIRENE-Büros koordinieren die Überprüfung der Qualität der in das SIS eingegebenen Daten. Für diese Zwecke haben sie Zugriff auf die im SIS verarbeiteten Daten.

(3) Die Mitgliedstaaten legen der eu-LISA Angaben über ihre N.SIS-Stelle und ihr SIRENE-Büro vor. eu-LISA veröffentlicht die Liste der N.SIS-Stellen und der SIRENE Büros zusammen mit der in Artikel 56 Absatz 7 genannten Liste.

Artikel 8

Austausch von Zusatzinformationen

(1) Der Austausch von Zusatzinformationen erfolgt über die Kommunikationsinfrastruktur im Einklang mit den Bestimmungen des SIRENE-Handbuchs. Die Mitgliedstaaten stellen die erforderlichen technischen und personellen Ressourcen bereit, um die fortlaufende Verfügbarkeit und den fristgerechten und wirksamen Austausch von Zusatzinformationen sicherzustellen. Sollte die Kommunikationsinfrastruktur nicht zur Verfügung stehen, so greifen die Mitgliedstaaten auf andere in geeigneter Weise gesicherte technische Mittel für den Austausch von Zusatzinformationen zurück. Eine Liste von in geeigneter Weise gesicherten technischen Mitteln wird im SIRENE-Handbuch festgelegt.

(2) Zusatzinformationen dürfen nur für die Zwecke verwendet werden, für die sie gemäß Artikel 64 übermittelt wurden, es sei denn, der ausschreibende Mitgliedstaat hat vorher seine Zustimmung zu einer anderweitigen Verwendung erteilt.

(3) Die SIRENE-Büros erfüllen ihre Aufgaben schnell und effizient, insbesondere indem sie so schnell wie möglich, jedoch spätestens zwölf Stunden nach Eingang, auf ein Ersuchen um Zusatzinformationen antworten. Im Falle von Ausschreibungen wegen terroristischer Straftaten, von Ausschreibungen von Personen zum Zwecke der Übergabe- oder Auslieferungshaft und von Ausschreibungen von Kindern gemäß Artikel 32 Absatz 1 Buchstabe c, handeln die SIRENE-Büros umgehend.

Ersuchen um Zusatzinformationen mit höchster Priorität werden in den SIRENE-Formularen als „URGENT" (dringend) gekennzeichnet, und der Grund für die Dringlichkeit wird angegeben.

(4) Die Kommission erlässt Durchführungsrechtsakte mit genauen Vorschriften für die Aufgaben der SIRENE-Büros gemäß dieser Verordnung und für den Austausch von Zusatzinformationen in Form eines Handbuchs mit der Bezeichnung „SIRENE-Handbuch". Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 9

Technische und funktionelle Konformität

(1) Bei der Einrichtung seines N.SIS hält jeder Mitgliedstaat die gemeinsamen Standards, Protokolle und technischen Verfahren ein, die festgelegt wurden, um die Kompatibilität des N.SIS mit dem zentralen SIS für die zügige und wirksame Übermittlung von Daten zu gewährleisten.

(2) Verwendet ein Mitgliedstaat eine nationale Kopie, so stellt er über die Dienste der CS-SIS und über die automatischen Aktualisierungen nach Artikel 4 Absatz 6 sicher, dass die in der nationalen Kopie gespeicherten Daten mit den Daten in der SIS-Datenbank identisch und kohärent sind und dass eine Abfrage in seiner nationalen Kopie ein mit einer Abfrage in der SIS-Datenbank gleichwertiges Ergebnis liefert.

(3) Endnutzer erhalten die zur Erfüllung ihrer Aufgaben erforderlichen Daten, insbesondere und soweit erforderlich alle verfügbaren Daten, die die Identifizierung der betroffenen Person und das Ergreifen der beantragten Maßnahmen ermöglichen.

(4) Die Mitgliedstaaten und eu-LISA führen regelmäßig Tests durch, um die technische Konformität der in Absatz 2 genannten nationalen Kopien zu überprüfen. Die Ergebnisse dieser Tests werden als Teil des mit der Verordnung (EU) Nr. 1053/2013 des Rates [1] eingeführten Mechanismus berücksichtigt.

(5) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung und Weiterentwicklung der gemeinsamen Standards, Protokolle und technischen Verfahren gemäß Absatz 1 dieses Artikels. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 10

Sicherheit — Mitgliedstaaten

(1) Jeder Mitgliedstaat trifft für sein N.SIS die erforderlichen Maßnahmen, einschließlich der Annahme eines Sicherheitsplans sowie von Notfallplänen zur Aufrechterhaltung und Wiederherstellung des Betriebs, um

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

b) Unbefugten den Zugang zu Datenverarbeitungsanlagen, in denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle);

c) zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden (Datenträgerkontrolle);

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

e) zu verhindern, dass automatisierte Datenverarbeitungssysteme mithilfe von Datenübertragungseinrichtungen von Unbefugten genutzt werden können (Benutzerkontrolle);

f) die unbefugte Verarbeitung von Daten im SIS und die unbefugte Änderung oder Löschung von Daten, die im SIS verarbeitet werden, zu verhindern (Kontrolle der Dateneingabe);

g) sicherzustellen, dass die zur Benutzung eines automatisierten Datenverarbeitungssystems Berechtigten nur mittels einer persönlichen und eindeutigen Nutzerkennung und vertraulicher Zugriffsverfahren ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle);

[1] Verordnung (EU) Nr. 1053/2013 des Rates vom 7. Oktober 2013 zur Einführung eines Evaluierungs- und Überwachungsmechanismus für die Überprüfung der Anwendung des Schengen-Besitzstands und zur Aufhebung des Beschlusses des Exekutivausschusses vom 16. September 1998 bezüglich der Errichtung des Ständigen Ausschusses Schengener Durchführungsübereinkommen (ABl. L 295 vom 6.11.2013, S. 27).

h) sicherzustellen, dass alle Behörden mit Zugriffsrecht auf das SIS oder mit Zugangsberechtigung zu den Datenverarbeitungsanlagen Profile mit einer Beschreibung der Aufgaben und Zuständigkeiten der Personen erstellen, die zum Zugriff auf die Daten sowie zu ihrer Eingabe, Aktualisierung, Löschung und Abfrage berechtigt sind, und diese Profile den Aufsichtsbehörden nach Artikel 69 Absatz 1 auf deren Anfrage unverzüglich zur Verfügung stellen (Personalprofile);

i) sicherzustellen, dass überprüft und festgestellt werden kann, welchen Stellen personenbezogene Daten mithilfe von Datenübertragungseinrichtungen übermittelt werden können (Übermittlungskontrolle);

j) sicherzustellen, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten wann, von wem und zu welchem Zweck in automatisierte Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle);

k) das unbefugte Lesen, Kopieren, Ändern oder Löschen von personenbezogenen Daten während der Übermittlung von personenbezogenen Daten oder während des Transports von Datenträgern zu verhindern, insbesondere durch geeignete Verschlüsselungstechniken (Transportkontrolle);

l) die Wirksamkeit der in diesem Absatz genannten Sicherheitsmaßnahmen zu überwachen und die erforderlichen organisatorischen Maßnahmen bezüglich der internen Überwachung zu treffen, um die Einhaltung dieser Verordnung sicherzustellen (Eigenkontrolle);

m) sicherzustellen, dass die eingesetzten Systeme im Störungsfall für den Normalbetrieb wiederhergestellt werden können (Wiederherstellung); und

n) sicherzustellen, dass das SIS ordnungsgemäß funktioniert, dass Fehler gemeldet werden (Zuverlässigkeit) und dass im SIS gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beeinträchtigt werden können (Integrität).

(2) Die Mitgliedstaaten treffen für die Verarbeitung und den Austausch von Zusatzinformationen einschließlich der Sicherung der Räumlichkeiten der SIRENE-Büros Sicherheitsmaßnahmen, die den in Absatz 1 genannten gleichwertig sind.

(3) Die Mitgliedstaaten treffen für die Verarbeitung von SIS-Daten durch die in Artikel 44 genannten Behörden Sicherheitsmaßnahmen, die den in Absatz 1 des vorliegenden Artikels genannten gleichwertig sind.

(4) Die in den Absätzen 1, 2 und 3 beschriebenen Maßnahmen können Teil eines allgemeinen Sicherheitskonzepts und -plans auf nationaler Ebene sein, der mehrere IT-Systeme umfasst. In diesen Fällen müssen die Anforderung gemäß diesem Artikel und ihre Anwendbarkeit auf das SIS in diesem Plan deutlich erkennbar sein und durch ihn gewährleistet werden.

Artikel 11

Geheimhaltung — Mitgliedstaaten

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

(2) Arbeitet ein Mitgliedstaat bei Aufgaben im Zusammenhang mit dem SIS mit externen Auftragnehmern zusammen, so überwacht er die Tätigkeiten des Auftragnehmers genau, um sicherzustellen, dass alle Vorschriften dieser Verordnung, insbesondere betreffend Sicherheit, Geheimhaltung und Datenschutz, eingehalten werden.

(3) Das Betriebsmanagement des N.SIS oder etwaiger technischer Kopien wird nicht an private Unternehmen oder private Organisationen übertragen.

Artikel 12

Führen von Protokollen auf nationaler Ebene

(1) Die Mitgliedstaaten stellen sicher, dass jeder Zugriff auf personenbezogene Daten und jeder Austausch solcher Daten innerhalb der CS-SIS in ihrem N.SIS protokolliert werden, damit die Rechtmäßigkeit der Abfrage und der Datenverarbeitung kontrolliert, eine Eigenkontrolle durchgeführt und das einwandfreie Funktionieren des N.SIS gewährleistet werden können, sowie für die Zwecke der Datenintegrität und -sicherheit. Diese Anforderung gilt nicht für die in Artikel 4 Absatz 6 Buchstaben a, b und c genannten automatisierten Prozesse.

(2) Die Protokolle müssen insbesondere Folgendes enthalten: die Historie der Ausschreibung, das Datum und die Uhrzeit der Datenverarbeitung, die für die Abfrage verwendeten Daten, eine Angabe zu den verarbeiteten Daten sowie die persönliche und eindeutige Nutzerkennung der zuständigen Behörde und der Person, die die Daten verarbeitet.

(3) Abweichend von Absatz 2 dieses Artikels müssen die Protokolle bei Abfragen anhand von daktyloskopischen Daten oder eines Gesichtsbilds gemäß Artikel 43 die Art der für die Abfrage verwendeten Daten anstelle der tatsächlichen Daten enthalten.

(4) Die Protokolle dürfen nur für den in Absatz 1 genannten Zweck verwendet werden und werden drei Jahre, nachdem sie angelegt wurden, gelöscht. Die Protokolle, die die Historie von Ausschreibungen beinhalten, werden drei Jahre nach Löschung der betreffenden Ausschreibung gelöscht.

(5) Die Protokolle können länger als für die in Absatz 4 genannten Zeiträume gespeichert werden, wenn sie für ein bereits laufendes Kontrollverfahren benötigt werden.

(6) Die nationalen zuständigen Behörden, die die Rechtmäßigkeit der Abfrage kontrollieren, die Rechtmäßigkeit der Datenverarbeitung überwachen, eine Eigenkontrolle durchführen und das einwandfreie Funktionieren des N.SIS sowie die Datenintegrität und -sicherheit gewährleisten, haben im Rahmen ihrer Zuständigkeiten auf Anfrage Zugang zu den Protokollen, damit sie ihre Aufgaben wahrnehmen können.

(7) Führen Mitgliedstaaten nach Maßgabe ihres nationalen Rechts eine Abfrage von Kraftfahrzeugen im automatisierten Verfahren mittels eines Systems zur automatischen Nummernschilderkennung durch, so bewahren sie ein Protokoll der Abfrage nach Maßgabe ihres nationalen Rechts auf. Erforderlichenfalls kann eine vollständige Abfrage im SIS durchgeführt werden, um zu überprüfen, ob ein Treffer erzielt wurde. Für jede vollständige Abfrage gelten die Absätze 1 bis 6.

(8) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung des Inhalts der Protokolle gemäß Absatz 7 dieses Artikels. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 13

Eigenkontrolle

Die Mitgliedstaaten stellen sicher, dass jede zum Zugriff auf SIS-Daten berechtigte Behörde die erforderlichen Maßnahmen zur Einhaltung der Bestimmungen dieser Verordnung trifft und erforderlichenfalls mit der Aufsichtsbehörde zusammenarbeitet.

Artikel 14

Schulung des Personals

(1) Das Personal der zum Zugriff auf das SIS berechtigten Behörden erhält, bevor es ermächtigt wird, im SIS gespeicherte Daten zu verarbeiten, und in regelmäßigen Abständen, nachdem der Zugriff auf das SIS gewährt wurde, eine angemessene Schulung in Fragen der Datensicherheit, der Grundrechte, einschließlich des Datenschutzes, und der Vorschriften und Verfahren für die Datenverarbeitung gemäß dem SIRENE-Handbuch. Das Personal wird über alle einschlägigen Bestimmungen zu Straftatbeständen und Strafen informiert, einschließlich jener, die in Artikel 73 festgelegt sind.

(2) Die Mitgliedstaaten müssen über ein nationales SIS-Schulungsprogramm verfügen, das Schulungen für die Endnutzer wie auch für das Personal der SIRENE-Büros umfasst.

Dieses Schulungsprogramm kann Teil eines allgemeinen Schulungsprogramms auf nationaler Ebene sein, das Schulungen in anderen einschlägigen Bereichen umfasst.

(3) Gemeinsame Schulungskurse werden mindestens einmal jährlich auf Unionsebene veranstaltet, um die Zusammenarbeit zwischen den SIRENE-Büros zu fördern.

KAPITEL III

Zuständigkeiten von eu-LISA

Artikel 15

Betriebsmanagement

(1) Für das Betriebsmanagement des zentralen SIS ist eu-LISA zuständig. eu-LISA gewährleistet in Zusammenarbeit mit den Mitgliedstaaten, dass vorbehaltlich einer Kosten-Nutzen-Analyse jederzeit die beste verfügbare Technologie für das zentrale SIS zum Einsatz kommt.

(2) eu-LISA ist ferner für folgende Aufgaben im Zusammenhang mit der Kommunikationsinfrastruktur zuständig:

a) Aufsicht;

b) Sicherheit;

c) Koordinierung der Beziehungen zwischen den Mitgliedstaaten und dem Betreiber;

d) Aufgaben im Zusammenhang mit dem Haushaltsvollzug;

e) Anschaffung und Erneuerung; und

f) vertragliche Fragen.

(3) eu-LISA ist ferner für folgende Aufgaben im Zusammenhang mit den SIRENE-Büros und der Kommunikation zwischen den SIRENE-Büros zuständig:

a) Koordinierung, Verwaltung und Unterstützung von Tests;

b) Pflege und Aktualisierung der technischen Spezifikationen für den Austausch von Zusatzinformationen zwischen den SIRENE-Büros und der Kommunikationsinfrastruktur; und

c) Bewältigung der Auswirkungen technischer Änderungen, wenn diese sowohl das SIS als auch den Austausch von Zusatzinformationen zwischen SIRENE-Büros betreffen.

(4) eu-LISA entwickelt und pflegt einen Mechanismus und Verfahren für die Durchführung von Qualitätskontrollen der Daten in der CS-SIS. Sie erstattet den Mitgliedstaaten in diesem Zusammenhang regelmäßig Bericht.

eu-LISA legt der Kommission regelmäßig Berichte über die aufgetretenen Probleme und die betroffenen Mitgliedstaaten vor.

Die Kommission legt dem Europäischen Parlament und dem Rat regelmäßig einen Bericht über die aufgetretenen Probleme im Zusammenhang mit der Datenqualität vor.

(5) eu-LISA führt zudem Aufgaben im Zusammenhang mit Schulungen zur technischen Nutzung des SIS und zu Maßnahmen zur Verbesserung der Qualität der SIS-Daten durch.

(6) Das Betriebsmanagement des zentralen SIS umfasst alle Aufgaben, die erforderlich sind, um das zentrale SIS im Einklang mit dieser Verordnung 24 Stunden pro Tag und 7 Tage die Woche betriebsbereit zu halten; dazu gehören insbesondere die für den einwandfreien Betrieb des Systems erforderlichen Wartungsarbeiten und technischen Anpassungen. Zu diesen Aufgaben gehören auch die Koordinierung, die Verwaltung und die Unterstützung von Tests für das zentrale SIS und das N.SIS, die sicherstellen, dass das zentrale SIS und das N.SIS gemäß den in Artikel 9 dargelegten Anforderungen an die technische und funktionelle Konformität funktionieren.

(7) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der technischen Anforderungen an die Kommunikationsinfrastruktur. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 16

Sicherheit — eu-LISA

(1) eu-LISA trifft die erforderlichen Maßnahmen, einschließlich der Annahme eines Sicherheitsplans sowie von Notfallplänen zur Aufrechterhaltung und Wiederherstellung des Betriebs für das zentrale SIS und die Kommunikationsinfrastruktur, um

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

b) Unbefugten den Zugang zu Datenverarbeitungsanlagen, in denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle);

c) zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden (Datenträgerkontrolle);

d) die unbefugte Dateneingabe sowie die unbefugte Kenntnisnahme, Änderung oder Löschung von gespeicherten personenbezogenen Daten zu verhindern (Speicherkontrolle);

e) zu verhindern, dass automatisierte Datenverarbeitungssysteme mithilfe von Datenübertragungseinrichtungen von Unbefugten genutzt werden (Benutzerkontrolle);

f) die unbefugte Verarbeitung von Daten im SIS und die unbefugte Änderung oder Löschung von Daten, die im SIS verarbeitet werden, zu verhindern (Kontrolle der Dateneingabe);

g) sicherzustellen, dass die zur Benutzung eines automatisierten Datenverarbeitungssystems Berechtigten nur mittels einer persönlichen und eindeutigen Nutzerkennung und vertraulicher Zugriffsverfahren ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle);

h) Profile mit einer Beschreibung der Aufgaben und Zuständigkeiten der zum Zugriff auf die Daten oder zum Zugang zu den Datenverarbeitungsanlagen berechtigten Personen zu erstellen und diese Profile dem Europäischen Datenschutzbeauftragten auf dessen Anfrage unverzüglich zur Verfügung zu stellen (Personalprofile);

i) sicherzustellen, dass überprüft und festgestellt werden kann, welchen Stellen personenbezogene Daten mithilfe von Datenübertragungseinrichtungen übermittelt werden können (Übermittlungskontrolle);

j) sicherzustellen, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten wann und von wem in automatisierte Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle);

k) das unbefugte Lesen, Kopieren, Ändern oder Löschen von personenbezogenen Daten während der Übermittlung von personenbezogenen Daten oder während des Transports von Datenträgern zu verhindern, insbesondere durch geeignete Verschlüsselungstechniken (Transportkontrolle);

l) die Wirksamkeit der in diesem Absatz genannten Sicherheitsmaßnahmen zu überwachen und die erforderlichen organisatorischen Maßnahmen bezüglich der internen Überwachung zu treffen, um die Einhaltung der Bestimmungen dieser Verordnung sicherzustellen (Eigenkontrolle);

m) sicherzustellen, dass die eingesetzten Systeme im Störungsfall für den Normalbetrieb wiederhergestellt werden können (Wiederherstellung);

n) sicherzustellen, dass das SIS ordnungsgemäß funktioniert, dass Fehler gemeldet werden (Zuverlässigkeit) und dass im SIS gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beeinträchtigt werden können (Integrität); und

o) die Sicherheit ihrer technischen Standorte sicherzustellen.

(2) eu-LISA trifft für die Verarbeitung und den Austausch von Zusatzinformationen über die Kommunikationsinfrastruktur Sicherheitsmaßnahmen, die den in Absatz 1 genannten gleichwertig sind.

Artikel 17

Geheimhaltung — eu-LISA

(1) Unbeschadet des Artikels 17 des Statuts wendet eu-LISA geeignete Regeln für die berufliche Schweigepflicht beziehungsweise eine andere vergleichbare Geheimhaltungspflicht auf alle Mitarbeiter an, die mit SIS-Daten arbeiten müssen, wobei mit Artikel 11 dieser Verordnung ein vergleichbarer Standard einzuhalten ist. Diese Pflicht besteht auch nach dem Ausscheiden dieser Personen aus dem Amt oder Dienstverhältnis oder nach der Beendigung ihrer Tätigkeit weiter.

(2) eu-LISA trifft für den Austausch von Zusatzinformationen über die Kommunikationsinfrastruktur Geheimhaltungsmaßnahmen, die den in Absatz 1 genannten gleichwertig sind.

(3) Arbeitet eu-LISA bei Aufgaben im Zusammenhang mit dem SIS mit externen Auftragnehmern zusammen, so überwacht sie die Tätigkeiten des Auftragnehmers genau, um sicherzustellen, dass alle Vorschriften dieser Verordnung, insbesondere betreffend Sicherheit, Geheimhaltung und Datenschutz, eingehalten werden.

(4) Das Betriebsmanagement der CS-SIS wird nicht an private Unternehmen oder private Organisationen übertragen.

Artikel 18

Führen von Protokollen auf zentraler Ebene

(1) eu-LISA stellt sicher, dass jeder Zugriff auf personenbezogene Daten und jeder Austausch solcher Daten innerhalb der CS-SIS für die in Artikel 12 Absatz 1 genannten Zwecke protokolliert werden.

(2) Die Protokolle müssen insbesondere Folgendes enthalten: die Historie der Ausschreibung, das Datum und die Uhrzeit der Datenverarbeitung, die für die Abfrage verwendeten Daten, eine Angabe zu den verarbeiteten Daten sowie die persönliche und eindeutige Nutzerkennung der zuständigen Behörde, die die Daten verarbeitet.

(3) Abweichend von Absatz 2 dieses Artikels müssen die Protokolle bei Abfragen anhand von daktyloskopischen Daten oder von Gesichtsbildern gemäß Artikel 43 die Art der für die Abfrage verwendeten Daten anstelle der tatsächlichen Daten enthalten.

(4) Die Protokolle dürfen nur für die in Absatz 1 genannten Zwecke verwendet werden und werden drei Jahre, nachdem sie angelegt wurden, gelöscht. Die Protokolle, die die Historie von Ausschreibungen beinhalten, werden drei Jahre nach Löschung der betreffenden Ausschreibung gelöscht.

(5) Die Protokolle können länger als für die in Absatz 4 genannten Zeiträume gespeichert werden, wenn sie für ein bereits laufendes Kontrollverfahren benötigt werden.

(6) eu-LISA hat im Rahmen ihrer Zuständigkeiten Zugang zu den Protokollen, damit sie eine Eigenkontrolle durchführen und das einwandfreie Funktionieren der CS-SIS sowie die Datenintegrität und -sicherheit gewährleisten kann.

Der Europäische Datenschutzbeauftragte hat im Rahmen seiner Zuständigkeiten auf Anfrage Zugang zu diesen Protokollen, damit er seine Aufgaben wahrnehmen kann.

KAPITEL IV

Information der Öffentlichkeit

Artikel 19

Aufklärungskampagnen über das SIS

Zu Beginn der Anwendung dieser Verordnung führt die Kommission in Zusammenarbeit mit den Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten eine Aufklärungskampagne zur Unterrichtung der Öffentlichkeit über die Ziele des SIS, die im SIS gespeicherten Daten, die zum Zugang zum SIS berechtigten Behörden und die Rechte der betroffenen Personen durch. Die Kommission wiederholt derartige Kampagnen in Zusammenarbeit mit den Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten regelmäßig. Die Kommission betreibt eine für die Öffentlichkeit zugängliche Website mit allen einschlägigen Informationen zum SIS. Die Mitgliedstaaten entwickeln in Zusammenarbeit mit ihren Aufsichtsbehörden die erforderlichen Maßnahmen zur allgemeinen Unterrichtung ihrer Bürger und Einwohner über das SIS und setzen diese um.

KAPITEL V

Kategorien von Daten und Kennzeichnung

Artikel 20

Kategorien von Daten

(1) Unbeschadet des Artikels 8 Absatz 1 oder der Bestimmungen dieser Verordnung über die Speicherung von ergänzenden Daten enthält das SIS nur die Kategorien von Daten, die von jedem Mitgliedstaat zur Verfügung gestellt werden und die für die in den Artikeln 26, 32, 34, 36, 38 und 40 festgelegten Zwecke erforderlich sind.

(2) Die Datenkategorien sind:

a) Informationen über Personen, zu denen eine Ausschreibung eingegeben wurde;

b) Informationen über die in den Artikeln 26, 32, 34, 36 und 38 aufgeführten Sachen.

(3) Alle Ausschreibungen im SIS mit Angaben zu Personen dürfen nur folgende Daten enthalten:

a) Nachnamen;

b) Vornamen;

c) Geburtsnamen;

d) frühere Namen und Aliasnamen;

e) besondere, objektive, unveränderliche körperliche Merkmale;

f) Geburtsort;

g) Geburtsdatum;

h) Geschlecht;

i) sämtliche Staatsangehörigkeiten;

j) Angabe, ob die betreffende Person

   i) bewaffnet ist,

   ii) gewalttätig ist,

   iii) flüchtig oder entflohen ist,

   iv) selbstmordgefährdet ist;

   v) eine Gefahr für die öffentliche Gesundheit darstellt oder

   vi) an einer Aktivität im Sinne der Artikel 3 bis 14 der Richtlinie (EU) 2017/541 beteiligt ist;

k) den Ausschreibungsgrund;

l) die Behörde, die die Ausschreibung erstellt hat;

m) eine Bezugnahme auf die Entscheidung, die der Ausschreibung zugrunde liegt;

n) die im Falle eines Treffers zu ergreifende Maßnahme;

o) Verknüpfungen mit anderen Ausschreibungen nach Artikel 63;

p) die Art der Straftat;

q) die Eintragungsnummer der Person in einem nationalen Register;

r) bei Ausschreibungen nach Artikel 32 Absatz 1 eine Kategorisierung der Art des Falls;

s) die Art der Identifizierungsdokumente der Person;

t) das Ausstellungsland der Identifizierungsdokumente der Person;

u) die Nummer(n) der Identifizierungsdokumente der Person;

v) das Ausstellungsdatum der Identifizierungsdokumente der Person;

w) Lichtbilder und Gesichtsbilder;

x) nach Maßgabe von Artikel 42 Absatz 3 einschlägige DNA-Profile;

y) daktyloskopische Daten;

z) eine Kopie der Identifizierungsdokumente, möglichst in Farbe.

(4) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung und Weiterentwicklung der notwendigen technischen Vorschriften für die Eingabe, Aktualisierung, Löschung und Abfrage der Daten nach den Absätzen 2 und 3 dieses Artikels und der gemeinsamen Standards nach Absatz 5 dieses Artikels. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

(5) Die technischen Vorschriften müssen für Abfragen in der CS-SIS, in nationalen oder gemeinsamen Kopien und in technischen Kopien nach Artikel 56 Absatz 2 ähnlich sein. Sie müssen auf gemeinsamen Standards beruhen.

Artikel 21

Verhältnismäßigkeit

(1) Vor der Eingabe einer Ausschreibung und bei der Verlängerung der Gültigkeitsdauer einer Ausschreibung stellen die Mitgliedstaaten fest, ob Angemessenheit, Relevanz und Bedeutung des Falles eine Ausschreibung im SIS hinreichend rechtfertigen.

(2) Falls eine Person oder eine Sache im Rahmen einer Ausschreibung im Zusammenhang mit einer terroristischen Straftat gesucht wird, so wird davon ausgegangen, dass Angemessenheit, Relevanz und Bedeutung des Falles eine Ausschreibung im SIS rechtfertigen. Aus Gründen der öffentlichen oder der nationalen Sicherheit können die Mitgliedstaaten ausnahmsweise von der Eingabe einer Ausschreibung absehen, wenn davon auszugehen ist, dass sie behördliche oder rechtliche Untersuchungen, Ermittlungen oder Verfahren behindert.

Artikel 22

Anforderungen an die Eingabe einer Ausschreibung

(1) Mit Ausnahme der in Artikel 40 genannten Situationen besteht der zur Eingabe einer Ausschreibung in das SIS erforderliche Mindestdatensatz aus den Daten nach Artikel 20 Absatz 3 Buchstaben a, g, k und n. Die übrigen Daten nach dem genannten Absatz werden ebenfalls in das SIS eingegeben, sofern sie verfügbar sind.

(2) Die Daten nach Artikel 20 Absatz 3 Buchstabe e dieser Verordnung werden nur eingegeben, wenn dies zur Identifizierung der betreffenden Person unbedingt erforderlich ist. Die Mitgliedstaaten sorgen dafür, dass bei der Eingabe dieser Daten Artikels 10 der Richtlinie (EU) 2016/680 eingehalten wird.

Artikel 23

Vereinbarkeit von Ausschreibungen

(1) Vor der Eingabe einer Ausschreibung prüft der Mitgliedstaat, ob die betreffende Person oder die Sache bereits Gegenstand einer SIS-Ausschreibung ist. Zur Prüfung, ob eine Person bereits Gegenstand einer Ausschreibung ist, wird auch eine Prüfung anhand daktyloskopischer Daten durchgeführt, sofern diese Daten verfügbar sind.

(2) Für jede Person oder Sache wird nur eine Ausschreibung je Mitgliedstaat in das SIS eingegeben. Falls erforderlich, können von anderen Mitgliedstaaten neue Ausschreibungen für dieselbe Person oder dieselbe Sache gemäß Absatz 3 eingegeben werden.

(3) Ist eine Person oder eine Sache bereits Gegenstand einer SIS-Ausschreibung, so prüft der Mitgliedstaat, der eine neue Ausschreibung eingeben möchte, ob die Ausschreibungen miteinander vereinbar sind. Liegt keine Unvereinbarkeit vor, so kann der Mitgliedstaat die neue Ausschreibung eingeben. Sind die Ausschreibungen nicht miteinander vereinbar, so konsultieren die SIRENE-Büros der Mitgliedstaaten einander, indem sie Zusatzinformationen austauschen, um eine Einigung zu erzielen. Die Vorschriften für die Vereinbarkeit von Ausschreibungen werden im SIRENE-Handbuch festgelegt. Nach Konsultationen zwischen den Mitgliedstaaten kann wegen wesentlicher nationaler Belange von diesen Vorschriften für die Vereinbarkeit abgewichen werden.

(4) Bei Treffern zu Mehrfachausschreibungen zu derselben Person oder derselben Sache beachtet der vollziehende Mitgliedstaat die im SIRENE-Handbuch dargelegten Vorschriften für die Rangfolge der Ausschreibungen.

Ist eine Person Gegenstand von Mehrfachausschreibungen von verschiedenen Mitgliedstaaten, so werden nach Artikel 26 eingegebene Fahndungsausschreibungen nach Maßgabe von Artikel 25 vorrangig vollzogen.

Artikel 24

Allgemeine Bestimmungen über die Kennzeichnung

(1) Ist ein Mitgliedstaat der Auffassung, dass die Durchführung einer nach Artikel 26, 32 oder 36 eingegebenen Ausschreibung mit seinem nationalen Recht, seinen internationalen Verpflichtungen oder wesentlichen nationalen Interessen nicht vereinbar ist, so kann er verlangen, die Ausschreibung so mit einer Kennzeichnung zu versehen, dass die Maßnahme aufgrund der Ausschreibung nicht in seinem Hoheitsgebiet vollzogen wird. Die Kennzeichnung wird vom SIRENE-Büro des ausschreibenden Mitgliedstaats hinzugefügt.

(2) Damit die Mitgliedstaaten die Möglichkeit haben, die Kennzeichnung einer nach Artikel 26 eingegebenen Ausschreibung zu verlangen, werden sämtliche Mitgliedstaaten im Wege des Austausches von Zusatzinformationen automatisch über neue Ausschreibungen dieser Kategorie informiert.

(3) Verlangt ein ausschreibender Mitgliedstaat in besonders dringenden und schwerwiegenden Fällen den Vollzug der Maßnahme, so prüft der vollziehende Mitgliedstaat, ob er gestatten kann, die auf sein Verlangen hinzugefügte Kennzeichnung zurückzuziehen. Wenn dies möglich ist, trifft der vollziehende Mitgliedstaat die nötigen Vorkehrungen, damit die Maßnahme unverzüglich ausgeführt werden kann.

Artikel 25

Kennzeichnung von Ausschreibungen zum Zwecke der Übergabehaft

(1) Findet der Rahmenbeschluss 2002/584/JI Anwendung, so ersucht ein Mitgliedstaat den ausschreibenden Mitgliedstaat darum, als Folgemaßnahme eine die Festnahme verhindernde Kennzeichnung einer Ausschreibung zum Zwecke der Übergabehaft hinzuzufügen, wenn die nach nationalem Recht für die Vollstreckung eines Europäischen Haftbefehls zuständige Justizbehörde die Vollstreckung des Haftbefehls wegen Vorliegens eines Grundes für die Nichtvollstreckung verweigert hat und die Kennzeichnung verlangt worden ist.

Ein Mitgliedstaat kann ferner verlangen, dass einer Ausschreibung eine Kennzeichnung hinzugefügt wird, wenn seine zuständige Justizbehörde die ausgeschriebene Person während des Übergabeverfahrens freilässt.

(2) Auf Anordnung einer nach nationalem Recht zuständigen Justizbehörde kann jedoch entweder aufgrund einer allgemeinen Anweisung oder in einem besonderen Fall ein Mitgliedstaat vom ausschreibenden Mitgliedstaat die Kennzeichnung einer Ausschreibung zum Zwecke der Übergabehaft verlangen, wenn offensichtlich ist, dass die Vollstreckung des Europäischen Haftbefehls abzulehnen sein wird.

KAPITEL VI

Ausschreibungen von Personen zum Zwecke der Übergabe-oder Auslieferungshaft

Artikel 26

Ausschreibungsziele und -bedingungen

(1) Ausschreibungen betreffend Personen, nach denen zum Zwecke der Übergabehaft mit Europäischem Haftbefehl gesucht wird, oder Ausschreibungen von Personen, nach denen zum Zwecke der Auslieferungshaft gesucht wird, werden auf Antrag der Justizbehörde des ausschreibenden Mitgliedstaats eingegeben.

(2) Ausschreibungen zum Zwecke der Übergabehaft werden auch auf der Grundlage eines Haftbefehls eingegeben, der gemäß Übereinkünften zwischen der Union und Drittländern auf der Grundlage der Verträge zum Zwecke der Übergabe von Personen aufgrund eines Haftbefehls ausgestellt wurde, wenn diese die Übermittlung eines solchen Haftbefehls über das SIS vorsehen.

(3) In dieser Verordnung sind Bezugnahmen auf Bestimmungen des Rahmenbeschlusses 2002/584/JI dahin gehend auszulegen, dass sie die entsprechenden Bestimmungen von Übereinkünften zwischen der Union und Drittländern auf der Grundlage der Verträge zum Zwecke der Übergabe von Personen aufgrund eines Haftbefehls, die die Übermittlung eines solchen Haftbefehls über das SIS vorsehen, mit einschließen.

(4) Der ausschreibende Mitgliedstaat kann im Fall einer laufenden operativen Maßnahme eine gemäß diesem Artikel eingegebene bestehende Ausschreibung zur Festnahme vorübergehend für die Abfrage durch die an der operativen Maßnahme beteiligten Endnutzer in den Mitgliedstaaten nicht verfügbar machen. In solchen Fällen können nur die SIRENE-Büros auf die Ausschreibung zugreifen. Die Mitgliedstaaten machen eine Ausschreibung nur dann nicht verfügbar, wenn

a) der Zweck der operativen Maßnahme nicht durch andere Maßnahmen erreicht werden kann;

b) zuvor eine entsprechende Bewilligung durch die zuständige Justizbehörde des ausschreibenden Mitgliedstaats erteilt wurde, und

c) alle an der operativen Maßnahme beteiligten Mitgliedstaaten im Wege des Austauschs von Zusatzinformationen informiert wurden.

Die technische Möglichkeit nach Unterabsatz 1 darf nur für maximal 48 Stunden verwendet werden. Wenn es jedoch für operative Zwecke erforderlich ist, kann dieser Zeitraum um weitere Zeiträume von jeweils 48 Stunden verlängert werden. Die Mitgliedstaaten führen Statistiken über die Zahl der Ausschreibungen, bei denen von dieser technischen Möglichkeit Gebrauch gemacht wurde.

(5) Besteht ein eindeutiger Hinweis darauf, dass die in Artikel 38 Absatz 2 Buchstaben a, b, c, e, g, h, j und k genannten Sachen mit einer Person verbunden sind, die Gegenstand einer Ausschreibung gemäß den Absätzen 1 und 2 dieses Artikels ist, so können Ausschreibungen zu diesen Sachen eingegeben werden, um die Person ausfindig zu machen. In solchen Fällen werden die Personen- und die Sachfahndungsausschreibung im Einklang mit Artikel 63 miteinander verknüpft.

(6) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung und Weiterentwicklung der notwendigen Vorschriften für die Eingabe, Aktualisierung, Löschung und Abfrage der Daten gemäß Absatz 5 dieses Artikels. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 27

Ergänzende Daten zu zum Zwecke der Übergabehaft gesuchten Personen

(1) Wird eine Person zum Zwecke der Übergabehaft mit Europäischem Haftbefehl gesucht, so gibt der ausschreibende Mitgliedstaat eine Kopie des Originals des Europäischen Haftbefehls in das SIS ein.

Ein Mitgliedstaat kann Kopien von mehr als einem Europäischen Haftbefehl für eine Ausschreibung zum Zweck der Übergabehaft eingeben.

(2) Der ausschreibende Mitgliedstaat kann eine Kopie einer Übersetzung des Europäischen Haftbefehls in einer oder mehreren anderen Amtssprachen der Organe der Union eingeben.

Artikel 28

Zusatzinformationen zu zum Zwecke der Übergabehaft gesuchten Personen

Der Mitgliedstaat, der eine Ausschreibung zum Zwecke der Übergabehaft eingegeben hat, übermittelt die Informationen nach Artikel 8 Absatz 1 des Rahmenbeschlusses 2002/584/JI im Wege des Austauschs von Zusatzinformationen an die anderen Mitgliedstaaten.

Artikel 29

Zusatzinformationen zu zum Zwecke der Auslieferungshaft gesuchten Personen

(1) Der Mitgliedstaat, der eine Ausschreibung zum Zwecke der Auslieferungshaft eingegeben hat, übermittelt allen anderen Mitgliedstaaten die folgenden Informationen im Wege des Austauschs von Zusatzinformationen:

a) um die Festnahme ersuchende Behörde;

b) etwaiges Bestehen eines Haftbefehls oder einer Urkunde mit gleicher Rechtswirkung oder eines rechtskräftigen Urteils;

c) Art und rechtliche Würdigung der Straftat;

d) Beschreibung der Umstände, unter denen die Straftat begangen wurde; einschließlich der Zeit, des Orts und der Art der Täterschaft der ausgeschriebenen Person;

e) soweit möglich die Folgen der Straftat;

f) alle sonstigen Informationen, die für die Vollstreckung der Ausschreibung von Nutzen oder erforderlich sind.

(2) Die Daten nach Absatz 1 dieses Artikels werden nicht übermittelt, wenn die in den Artikeln 27 bzw. 28 genannten Daten bereits mitgeteilt wurden und vom vollstreckenden Mitgliedstaat für die Durchführung einer Ausschreibung als ausreichend erachtet werden.

Artikel 30

Umwandlung einer Maßnahme im Hinblick auf Ausschreibungen zum Zwecke der Übergabe- oder Auslieferungshaft

Ist eine Festnahme nicht möglich, entweder weil der darum ersuchte Mitgliedstaat die Vornahme nach den in den Artikeln 24 oder 25 festgelegten Verfahren für die Kennzeichnung ablehnt, oder weil im Falle einer Ausschreibung zum Zwecke der Auslieferungshaft eine Untersuchung noch nicht abgeschlossen ist, so geht der zur Festnahme ersuchte Mitgliedstaat in Bezug auf die Ausschreibung vor, indem er den Aufenthaltsort der betreffenden Person mitteilt.

Artikel 31

Durchführung von Maßnahmen aufgrund einer Ausschreibung zum Zwecke der Übergabe- oder Auslieferungshaft

(1) Eine in das SIS eingegebene Ausschreibung nach Artikel 26 und die ergänzenden Daten nach Artikel 27 stellen zusammen einen Europäischen Haftbefehl gemäß dem Rahmenbeschluss 2002/584/JI dar und haben die gleiche Wirkung wie dieser, sofern jener Rahmenbeschluss Anwendung findet.

(2) Findet der Rahmenbeschluss 2002/584/JI keine Anwendung, so ist eine nach den Artikeln 26 und 29 in das SIS eingegebene Ausschreibung einem Ersuchen um vorläufige Festnahme im Sinne des Artikels 16 des Europäischen Auslieferungsübereinkommens vom 13. Dezember 1957 oder des Artikels 15 des Benelux-Übereinkommens über Auslieferung und Rechtshilfe in Strafsachen vom 27. Juni 1962 rechtlich gleichgestellt.

KAPITEL VII

Ausschreibungen von vermissten Personen oder von schutzbedürftigen Personen, die am Reisen gehindert werden müssen

Artikel 32

Ausschreibungsziele und -bedingungen

(1) Ausschreibungen zu folgenden Kategorien von Personen werden auf Ersuchen der zuständigen Behörde des ausschreibenden Mitgliedstaats in das SIS eingegeben:

a) Vermisste, die in Gewahrsam genommen werden müssen, und zwar

   i) zu ihrem eigenen Schutz oder

   ii) um eine Gefahr für die öffentliche Ordnung oder die öffentliche Sicherheit zu verhindern;

b) Vermisste, die nicht in Gewahrsam genommen werden müssen;

c) von Entführung durch einen Elternteil, ein Familienmitglied oder einen Vormund bedrohte Kinder, die am Reisen gehindert werden müssen;

d) Kinder, die am Reisen gehindert werden müssen, weil ein konkretes und offensichtliches Risiko besteht, dass sie aus dem Hoheitsgebiet eines Mitgliedstaats gebracht werden oder dieses verlassen und

   i) Opfer von Menschenhandel, einer erzwungenen Eheschließung, der Genitalverstümmelung bei Frauen oder sonstiger Formen geschlechtsspezifischer Gewalt werden;

   ii) Opfer von terroristischen Straftaten werden oder darin verwickelt werden; oder

   iii) in bewaffnete Gruppen eingezogen oder rekrutiert werden oder zur aktiven Teilnahme an Feindseligkeiten gezwungen werden;

e) schutzbedürftige Personen, die volljährig sind und die zu ihrem eigenen Schutz am Reisen gehindert werden müssen, weil ein konkretes und offensichtliches Risiko besteht, dass sie aus dem Hoheitsgebiet eines Mitgliedstaats gebracht werden oder dieses verlassen und Opfer von Menschenhandel oder geschlechtsspezifischer Gewalt werden.

(2) Absatz 1 Buchstabe a findet insbesondere auf Kinder und Personen Anwendung, die aufgrund einer Anordnung einer zuständigen Stelle in eine Einrichtung eingewiesen werden müssen.

(3) In Fällen, in denen das konkrete und offensichtliche Risiko besteht, dass ein Kind im Sinne von Absatz 1 Buchstabe c in Kürze aus dem Mitgliedstaat, in dem die zuständigen Behörden gelegen sind, entführt wird, wird aufgrund einer Entscheidung der zuständigen Behörden, einschließlich der Justizbehörden des Mitgliedstaats, der die Zuständigkeit in Fragen der elterlichen Verantwortung hat, eine Ausschreibung zu dem betreffenden Kind eingegeben.

(4) Eine Ausschreibung von Personen gemäß Absatz 1 Buchstaben d und e wird aufgrund einer Entscheidung der zuständigen Behörden, einschließlich der Justizbehörden, eingegeben.

(5) Der ausschreibende Mitgliedstaat überprüft regelmäßig gemäß Artikel 53 Absatz 4, ob die Ausschreibungen nach Absatz 1 Buchstaben c, d und e dieses Artikels aufrechterhalten werden müssen.

(6) Der ausschreibende Mitgliedstaat sorgt dafür, dass alle der folgenden Voraussetzungen erfüllt sind:

a) aus den Daten, die er in das SIS eingegeben hat, geht hervor, in welche der in Absatz 1 genannten Kategorien die von der Ausschreibung betroffene Person einzuordnen ist;

b) aus den Daten, die er in das SIS eingegeben habt, geht hervor, um welche Art von Fall es sich handelt, sofern die Art des Falls bekannt ist; und

c) sein SIRENE-Büro hat für die gemäß Absatz 1 Buchstaben c, d und e eingegebenen Ausschreibungen zum Zeitpunkt der Erstellung der Ausschreibung alle ihm zur Verfügung stehenden relevanten Informationen bereitgestellt.

(7) Vier Monate bevor ein Kind, das Gegenstand einer Ausschreibung nach diesem Artikel ist, gemäß dem nationalen Recht des ausschreibenden Mitgliedstaats volljährig wird, teilt die CS-SIS automatisch dem ausschreibenden Mitgliedstaat mit, dass der Grund des Ersuchens und die zu ergreifenden Maßnahmen entweder aktualisiert werden müssen oder die Ausschreibung gelöscht werden muss.

(8) Besteht ein eindeutiger Hinweis darauf, dass die in Artikel 38 Absatz 2 Buchstaben a, b, c, e, g, h und k genannten Sachen mit einer Person verbunden sind, die Gegenstand einer Ausschreibung gemäß Absatz 1 dieses Artikels ist, so können Ausschreibungen zu diesen Sachen eingegeben werden, um die Person ausfindig zu machen. In solchen Fällen werden die Personen- und die Sachfahndungsausschreibung im Einklang mit Artikel 63 miteinander verknüpft.

(9) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung und Weiterentwicklung der Vorschriften für die Kategorisierung der Arten von Fällen und die Eingabe der Daten gemäß Absatz 6. Die Arten von Fällen vermisster Personen, bei denen es sich um Kinder handelt, umfassen — unter anderem — Kinder, die von Zuhause weggelaufen sind, unbegleitete Kinder im Zusammenhang mit Migration und Kinder, die von Entführung durch einen Elternteil bedroht sind.

Die Kommission erlässt ferner Durchführungsrechtsakte zur Festlegung und Weiterentwicklung der notwendigen technischen Vorschriften für die Eingabe, Aktualisierung, Löschung und Abfrage der Daten gemäß Absatz 8.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 33

Maßnahmen aufgrund einer Ausschreibung

(1) Werden Personen nach Artikel 32 ausfindig gemacht, so teilen die zuständigen Behörden des vollziehenden Mitgliedstaats dem ausschreibenden Mitgliedstaat vorbehaltlich der Anforderungen des Absatzes 4 den Aufenthaltsort dieser Personen mit.

(2) Im Falle von Personen, die gemäß Artikel 32 Absatz 1 Buchstaben a, c, d und e unter Schutz gestellt werden müssen, konsultiert der vollziehende Mitgliedstaat sofort seine eigenen zuständigen Behörden sowie die zuständigen Behörden des ausschreibenden Mitgliedstaats im Wege des Austauschs von Zusatzinformationen, um unverzüglich die zu treffenden Maßnahmen zu vereinbaren. Die zuständigen Behörden im vollziehenden Mitgliedstaat können nach Maßgabe des nationalen Rechts diese Personen in Gewahrsam nehmen, um ihre Weiterreise zu verhindern.

(3) Im Falle von Kindern ist jede Entscheidung über zu ergreifende Maßnahmen oder jede Entscheidung gemäß Absatz 2, das Kind in Gewahrsam zu nehmen, im Einklang mit dem Wohl des Kindes zu treffen. Diese Entscheidungen werden sofort, spätestens aber zwölf Stunden, nachdem das Kind ausfindig gemacht wurde, gegebenenfalls in Abstimmung mit den entsprechenden Kinderschutzbehörden getroffen.

(4) Bei volljährigen vermissten Personen, die ausfindig gemacht wurden, bedarf die Mitteilung von Daten, ausgenommen die Mitteilung von Daten zwischen den zuständigen Behörden, der Einwilligung des Betroffenen. Die zuständigen Behörden können jedoch der Person, die den Betroffenen als vermisst gemeldet hat, mitteilen, dass die Ausschreibung gelöscht wurde, weil die Person ausfindig gemacht wurde.

KAPITEL VIII

Ausschreibungen von Personen, die im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesucht werden

Artikel 34

Ausschreibungsziele und -bedingungen

(1) Im Hinblick auf die Mitteilung des Wohnsitzes oder des Aufenthaltsorts der betreffenden Personen geben die Mitgliedstaaten auf Ersuchen der zuständigen Behörde in das SIS Ausschreibungen zu folgenden Personen ein:

a) Zeugen;

b) Personen, die im Rahmen eines Strafverfahrens wegen Taten, derentwegen sie verfolgt werden, vor Gericht geladen sind oder die zum Zwecke der Ladung gesucht werden;

c) Personen, denen ein Strafurteil oder andere Schriftstücke im Rahmen eines Strafverfahrens wegen Taten, derentwegen sie verfolgt werden, zugestellt werden müssen;

d) Personen, denen die Ladung zum Antritt eines Freiheitsentzugs zugestellt werden muss.

(2) Besteht ein eindeutiger Hinweis darauf, dass die in Artikel 38 Absatz 2 Buchstaben a, b, c, e, g, h und k genannten Sachen mit einer Person verbunden sind, die Gegenstand einer Ausschreibung gemäß Absatz 1 dieses Artikels ist, so können Ausschreibungen zu diesen Sachen eingegeben werden, um die Person ausfindig zu machen. In derartigen Fällen werden die Ausschreibung der Person und die Ausschreibung der Sache im Einklang mit Artikel 63 miteinander verknüpft.

(3) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung und Weiterentwicklung der notwendigen technischen Vorschriften für die Eingabe, Aktualisierung, Löschung und Abfrage der Daten gemäß Absatz 2 dieses Artikels. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 35

Maßnahmen aufgrund einer Ausschreibung

Die erbetenen Informationen werden dem ausschreibenden Mitgliedstaat im Wege des Austauschs von Zusatzinformationen mitgeteilt.

KAPITEL IX

Personen- und Sachfahndungsausschreibungen für verdeckte Kontrollen, Ermittlungsanfragen oder gezielte Kontrollen

Artikel 36

Ausschreibungsziele und -bedingungen

(1) Personenausschreibungen und Sachfahndungsausschreibungen in Bezug auf die in Artikel 38 Absatz 2 Buchstaben a, b, c, e, g, h, i, k und l genannten Sachen sowie auf bargeldlose Zahlungsmittel werden nach Maßgabe des nationalen Rechts des ausschreibenden Mitgliedstaats für verdeckte Kontrollen, für Ermittlungsanfragen oder für gezielte Kontrollen gemäß Artikel 37 Absätze 3, 4 und 5 eingegeben.

(2) Bei der Eingabe von Ausschreibungen für verdeckte Kontrollen, Ermittlungsanfragen oder gezielte Kontrollen und im Fall, dass die vom ausschreibenden Mitgliedstaat benötigten Informationen über die in Artikel 37 Absatz 1 Buchstaben a bis h genannten hinausgehen, führt der ausschreibende Mitgliedstaat in der Ausschreibung alle benötigten Informationen auf. Beziehen sich diese Informationen auf besondere Kategorien personenbezogener Daten gemäß Artikel 10 der Richtlinie (EU) 2016/680, so werden sie nur beantragt, wenn dies für den spezifischen Zweck der Ausschreibung und in Bezug auf die Straftat, wegen der die Ausschreibung eingegeben wurde, unbedingt erforderlich ist.

(3) Personenausschreibungen für verdeckte Kontrollen, Ermittlungsanfragen und gezielte Kontrollen sind zulässig zur Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten, zur Strafvollstreckung und zur Abwehr von Gefahren für die öffentliche Sicherheit, wenn eine oder mehrere der nachstehenden Voraussetzungen erfüllt sind:

a) eindeutige Anhaltspunkte dafür vorliegen, dass eine Person eine der in Artikel 2 Absätze 1 und 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten plant oder begeht,

b) die in Artikel 37 Absatz 1 genannten Informationen zur Vollstreckung einer Freiheitsstrafe oder einer Haftanordnung gegen eine wegen einer der in Artikel 2 Absätze 1 und 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten verurteilte Person erforderlich sind,

c) die Gesamtbeurteilung einer Person, insbesondere aufgrund der bisher von ihr begangenen Straftaten, erwarten lässt, dass sie auch eine der in Artikel 2 Absätze 1 und 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten künftig begehen wird.

(4) Personenausschreibungen für verdeckte Kontrollen, Ermittlungsanfragen und gezielte Kontrollen können ferner, soweit das nationale Recht es erlaubt, auf Veranlassung der für die Sicherheit des Staates zuständigen Stellen eingegeben werden, wenn konkrete Anhaltspunkte dafür vorliegen, dass die in Artikel 37 Absatz 1 genannten Informationen zur Abwehr einer von dem Betroffenen ausgehenden erheblichen Gefährdung oder anderer erheblicher Gefahren für die innere oder äußere Sicherheit des Staates erforderlich sind. Der Mitgliedstaat, der die Ausschreibung nach diesem Absatz eingegeben hat, unterrichtet die anderen Mitgliedstaaten über eine solche Ausschreibung. Jeder Mitgliedstaat bestimmt, an welche Behörden diese Informationen übermittelt werden. Diese Informationen werden über das SIRENE-Büro übermittelt.

(5) Besteht ein eindeutiger Hinweis darauf, dass die in Artikel 38 Absatz 2 Buchstaben a, b, c, e, g, h, j, k und l genannten Sachen oder bargeldlose Zahlungsmittel im Zusammenhang mit schweren Straftaten nach Absatz 3 dieses Artikels stehen oder mit den erheblichen Gefahren nach Absatz 4 dieses Artikels verbunden sind, können Ausschreibungen zu diesen Sachen eingegeben und mit den Ausschreibungen gemäß den Absätzen 3 und 4 dieses Artikels verknüpft werden.

(6) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung und Weiterentwicklung der notwendigen technischen Vorschriften für die Eingabe, Aktualisierung, Löschung und Abfrage der Daten gemäß Absatz 5 dieses Artikels sowie der Zusatzinformationen gemäß Absatz 2 dieses Artikels. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 37

Maßnahmen aufgrund einer Ausschreibung

(1) Für verdeckte Kontrollen, für Ermittlungsanfragen oder für gezielte Kontrollen sollte der vollziehende Mitgliedstaat die nachstehenden Informationen ganz oder teilweise einholen und dem ausschreibenden Mitgliedstaat übermitteln:

a) die Tatsache, dass die Person, die Gegenstand einer Ausschreibung ist, ausfindig gemacht wurde, oder dass Sachen gemäß Artikel 38 Absatz 2 Buchstaben a, b, c, e, g, h, j, k oder l oder bargeldlose Zahlungsmittel, die Gegenstand einer Ausschreibung sind, ausfindig gemacht wurden;

b) Ort, Zeit und Grund der Kontrolle bzw. Ermittlungsanfrage;

c) Route und Bestimmungsort;

d) Begleitpersonen der Person, die Gegenstand der Ausschreibung ist, oder die Insassen des Kraft-, Wasser- oder Luftfahrzeugs oder Begleitpersonen des Inhabers des amtlichen Blanko- oder Identitätsdokuments, bei denen nach Lage der Dinge davon ausgegangen werden kann, dass sie mit dem Gegenstand der Ausschreibung in Verbindung stehen;

e) jede offengelegte Identität nebst jeder Beschreibung der Person, die das ausgeschriebene amtliche Blanko- bzw. Identitätsdokument verwendet;

f) die Sachen gemäß Artikel 38 Absatz 2 Buchstaben a, b, c, e, g, h, j, k oder l oder die benutzten bargeldlosen Zahlungsmittel;

g) mitgeführte Sachen einschließlich Reisedokumente;

h) die Umstände, unter denen die Person, die Sachen gemäß Artikel 38 Absatz 2 Buchstaben a, b, c, e, g, h, j, k oder l oder die benutzten bargeldlosen Zahlungsmittel ausfindig gemacht wurde(n);

i) alle weiteren Informationen, die vom ausschreibenden Mitgliedstaat gemäß Artikel 36 Absatz 2 beantragt wurden.

Beziehen sich die Informationen nach Unterabsatz 1 Buchstabe i auf besondere Kategorien personenbezogener Daten gemäß Artikel 10 der Richtlinie (EU) 2016/680, so werden sie gemäß den in dem genannten Artikel dargelegten Bedingungen verarbeitet, sofern sie andere personenbezogene Daten, die zu demselben Zweck verarbeitet werden, ergänzen.

(2) Der vollziehende Mitgliedstaat übermittelt die Informationen nach Absatz 1 im Wege des Austauschs von Zusatzinformationen.

(3) Eine verdeckte Kontrolle umfasst die verdeckte Erhebung möglichst vieler der in Absatz 1 aufgeführten Informationen während der Routinetätigkeit der nationalen zuständigen Behörden des vollziehenden Mitgliedstaats. Die Erhebung dieser Informationen darf den verdeckten Charakter der Kontrollmaßnahmen nicht gefährden und die ausgeschriebene Person darf unter keinen Umständen auf das Vorhandensein der Ausschreibung hingewiesen werden.

(4) Eine Ermittlungsanfrage umfasst eine Befragung der Person, auch auf der Grundlage von Informationen oder spezifischen Fragen, die der ausschreibende Mitgliedstaat gemäß Artikel 36 Absatz 2 in die Ausschreibung aufgenommen hat. Die Befragung erfolgt im Einklang mit dem nationalen Recht des vollziehenden Mitgliedstaats.

(5) Bei der gezielten Kontrolle können die Person, das Kraft-, Wasser- oder Luftfahrzeug, der Container oder die mitgeführten Sachen zu den in Artikel 36 genannten Zwecken durchsucht werden. Durchsuchungen erfolgen nach Maßgabe des nationalen Rechts des vollziehenden Mitgliedstaats.

(6) Wenn nach dem nationalen Recht des vollziehenden Mitgliedstaats gezielte Kontrollen nicht zulässig sind, erfolgt für den betreffenden Mitgliedstaat stattdessen automatisch eine Ermittlungsanfrage. Wenn nach dem nationalen Recht des vollziehenden Mitgliedstaats Ermittlungsanfragen nicht zulässig sind, erfolgt für den betreffenden Mitgliedstaat stattdessen automatisch eine verdeckte Kontrolle. Wenn die Richtlinie 2013/48/EU Anwendung findet, gewährleisten die Mitgliedstaaten, dass das Recht von Verdächtigen und beschuldigten Personen auf Rechtsbeistand unter den in der genannten Richtlinie dargelegten Bedingungen geachtet wird.

(7) Absatz 6 berührt nicht die Pflicht der Mitgliedstaaten, den Endnutzern gemäß Artikel 36 Absatz 2 beantragte Informationen zur Verfügung zu stellen.

KAPITEL X

Sachfahndungsausschreibungen zur Sicherstellung oder Beweissicherung in Strafverfahren

Artikel 38

Ausschreibungsziele und -bedingungen

(1) Die Mitgliedstaaten geben in das SIS Ausschreibungen in Bezug auf Sachen, die zur Sicherstellung oder zur Beweissicherung in Strafverfahren gesucht werden, ein.

(2) Ausschreibungen sind in Bezug auf folgende Kategorien von leicht identifizierbaren Sachen einzugeben:

a) Kraftfahrzeuge unabhängig vom Antriebssystem;

b) Anhänger mit einem Leergewicht von mehr als 750 kg;

c) Wohnwagen;

d) industrielle Ausrüstung;

e) Wasserfahrzeuge;

f) Wasserfahrzeugmotoren;

g) Container;

h) Luftfahrzeuge;

i) Flugzeugmotoren;

j) Schusswaffen;

k) amtliche Blankodokumente, die gestohlen, unterschlagen auf sonstige Weise abhandengekommen sind oder gefälschte Blankodokumente;

l) gestohlene, unterschlagene, auf sonstige Weise abhandengekommene, für ungültig erklärte oder gefälschte ausgestellte Identitätsdokumente wie Pässe, Personalausweise, Aufenthaltstitel, Reisedokumente und Führerscheine;

m) gestohlene, unterschlagene, auf sonstige Weise abhandengekommene, für ungültig erklärte oder gefälschte Kfz-Zulassungsbescheinigungen und Kfz-Kennzeichen;

n) Banknoten (Registriergeld) und gefälschte Banknoten;

o) Gegenstände der Informationstechnik;

p) identifizierbare Teile von Kraftfahrzeugen;

q) identifizierbare Teile von industrieller Ausrüstung;

r) andere hochwertige identifizierbare Sachen im Sinne von Absatz 3.

Bei den unter den Buchstaben k, l und m genannten Dokumenten kann der ausschreibende Mitgliedstaat angeben, ob es sich um gestohlene, unterschlagene, auf sonstige Weise abhandengekommene, ungültige oder gefälschte Dokumente handelt.

(3) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 75 zur Änderung dieser Verordnung durch Festlegung neuer Unterkategorien von Sachen nach Absatz 2 Buchstaben o, p, q und r dieses Artikels zu erlassen.

(4) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung und Weiterentwicklung der technischen Vorschriften für die Eingabe, Aktualisierung, Löschung und Abfrage der Daten nach Absatz 2 dieses Artikels. Diese Durchführungsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren festgelegt und entwickelt.

Artikel 39

Maßnahmen aufgrund einer Ausschreibung

(1) Ergibt eine Abfrage, dass eine Sachfahndungsausschreibung besteht und die Sache gefunden wurde, so stellt die zuständige Stelle die betreffende Sache nach Maßgabe ihres nationalen Rechts sicher und setzt sich mit der Stelle des ausschreibenden Mitgliedstaats in Verbindung, um die erforderlichen Maßnahmen abzustimmen. Zu diesem Zweck können nach Maßgabe dieser Verordnung auch personenbezogene Daten übermittelt werden.

(2) Informationen nach Absatz 1 werden im Wege des Austauschs von Zusatzinformationen übermittelt.

(3) Der vollziehende Mitgliedstaat ergreift die erbetenen Maßnahmen nach Maßgabe seines nationalen Rechts.

KAPITEL XI

Ausschreibungen zu unbekannten gesuchten Personen zwecks Identifizierung nach Maßgabe des nationalen Rechts

Artikel 40

Ausschreibungen zu unbekannten gesuchten Personen zwecks Identifizierung nach Maßgabe des nationalen Rechts

Die Mitgliedstaaten können in das SIS Ausschreibungen eingeben, die ausschließlich daktyloskopische Daten enthalten. Bei diesen daktyloskopischen Daten handelt es sich um vollständige oder unvollständige Fingerabdruck- oder Handflächenabdrucksätze, die an Tatorten terroristischer oder sonstiger schwerer Straftaten, wegen derer ermittelt wird, vorgefunden wurden. Sie werden nur in das SIS eingegeben, wenn sie mit sehr hoher Wahrscheinlichkeit einem Täter zuzuordnen sind.

Kann die zuständige Behörde des ausschreibenden Mitgliedstaats die Identität der verdächtigen Person nicht auf der Grundlage von Daten aus einer anderen einschlägigen nationalen, Unions- oder internationalen Datenbank feststellen, dürfen die in Unterabsatz 1 genannten daktyloskopischen Daten nur in dieser Kategorie von Ausschreibungen als „unbekannte gesuchte Person“ zum Zweck der Identifizierung dieser Person eingegeben werden.

Artikel 41

Maßnahmen aufgrund einer Ausschreibung

Im Falle eines Treffers hinsichtlich der nach Artikel 40 eingegebenen Daten wird die Identität der Person nach Maßgabe des nationalen Rechts und durch fachmännische Überprüfung, ob die daktyloskopischen Daten im SIS zu der Person gehören, festgestellt. Die vollziehenden Mitgliedstaaten tauschen im Wege des Austauschs von Zusatzinformationen mit dem ausschreibenden Mitgliedstaat Angaben zur Identität und zum Aufenthaltsort der Person aus, um die zügige Untersuchung des Falles zu erleichtern.

KAPITEL XII

Besondere Vorschriften für biometrische Daten

Artikel 42

Besondere Vorschriften für die Eingabe von Lichtbildern, Gesichtsbildern, daktyloskopischen Daten und DNA-Profilen

(1) In das SIS werden nur Lichtbilder, Gesichtsbilder und daktyloskopische Daten nach Artikel 20 Absatz 3 Buchstaben w und y eingegeben, die den Mindestqualitätsstandards und technischen Spezifikationen entsprechen. Vor der Eingabe derartiger Daten wird eine Qualitätsprüfung durchgeführt, um festzustellen, ob sie den Mindestqualitätsstandards und technischen Spezifikationen entsprechen.

(2) Die in das SIS eingegebenen daktyloskopischen Daten können aus ein bis zehn gedrückten Fingerabdrücken und ein bis zehn gerollten Fingerabdrücken bestehen. Sie können ferner bis zu zwei Handflächenabdrücke umfassen.

(3) Ein DNA-Profil darf einer Ausschreibung nur in den in Artikel 32 Absatz 1 Buchstabe a vorgesehenen Fällen hinzugefügt werden, und erst nach einer Qualitätsprüfung, um festzustellen, ob die Mindestqualitätsstandards für die Daten und die technischen Spezifikationen eingehalten wurden und nur für den Fall, dass keine Lichtbilder, Gesichtsbilder oder daktyloskopischen Daten verfügbar sind oder diese nicht zur Identifizierung geeignet sind. Die DNA-Profile von Personen, die direkte Verwandte in gerader aufsteigender Linie, Verwandte in absteigender Linie oder Geschwister der ausgeschriebenen Person sind, können der Ausschreibung hinzugefügt werden, sofern diese Personen dem ausdrücklich zustimmen. Wird einer Ausschreibung ein DNA-Profil hinzugefügt, so enthält dieses Profil nur die Mindestinformationen, die zur Identifizierung der vermissten Person unbedingt erforderlich sind.

(4) Für die Speicherung der in den Absätzen 1 und 3 dieses Artikels genannten biometrischen Daten werden Mindestqualitätsstandards und technische Spezifikationen gemäß Absatz 5 dieses Artikels festgelegt. Diese Mindestqualitätsstandards und technischen Spezifikationen legen das Qualitätsniveau fest, das erforderlich ist, um die Daten zur Überprüfung der Identität einer Person gemäß Artikel 43 Absatz 1 sowie zur Identifizierung einer Person gemäß Artikel 43 Absätze 2 bis 4 verwenden zu können.

(5) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der Mindestqualitätsstandards und technischen Spezifikationen gemäß den Absätzen 1, 3 und 4 dieses Artikels. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 43

Besondere Vorschriften für die Überprüfung oder die Abfrage anhand von Lichtbildern, Gesichtsbildern, daktyloskopischen Daten und DNA-Profilen

(1) Wenn Lichtbilder, Gesichtsbilder, daktyloskopische Daten und DNA-Profile in einer Ausschreibung im SIS verfügbar sind, sind solche Lichtbilder, Gesichtsbilder, daktyloskopische Daten und DNA-Profile zu nutzen, um die Identität einer Person zu bestätigen, die durch eine alphanumerische Abfrage im SIS aufgefunden wurde.

(2) Daktyloskopische Daten können in allen Fällen abgefragt werden, um eine Person zu identifizieren. Daktyloskopische Daten sind abzufragen, um eine Person zu identifizieren, wenn die Identität der Person nicht durch andere Mittel festgestellt werden kann. Zu diesem Zweck enthält das zentrale SIS ein automatisiertes Fingerabdruck-Identifizierungssystem (AFIS).

(3) Daktyloskopische Daten im SIS im Zusammenhang mit gemäß den Artikeln 26, 32, 36 und 40 eingegebenen Ausschreibungen können auch anhand vollständiger oder unvollständiger Fingerabdruck- oder Handflächenabdrucksätze abgefragt werden, die an untersuchten Tatorten schwerer oder terroristischer Straftaten vorgefunden wurden, diese Abdrücke mit hoher Wahrscheinlichkeit einem Täter zuzuordnen sind und die Abfrage gleichzeitig in den einschlägigen nationalen Fingerabdruck-Datenbanken des Mitgliedstaats durchgeführt wird.

(4) Sobald die technische Möglichkeit dazu besteht, dürfen an regulären Grenzübergangsstellen Lichtbilder und Gesichtsbilder zur Identifizierung einer Person verwendet werden, wobei eine hochgradige Zuverlässigkeit der Identifizierung gewährleistet sein muss.

Vor der Implementierung dieser Funktionalität im SIS legt die Kommission einen Bericht über die Verfügbarkeit, Einsatzfähigkeit und Zuverlässigkeit der erforderlichen Technologie vor. Das Europäische Parlament wird zu diesem Bericht konsultiert.

Nach Beginn der Nutzung der Funktionalität an den regulären Grenzübergangsstellen wird der Kommission die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 75 zur Ergänzung dieser Verordnung zu erlassen, mit denen weitere Umstände bestimmt werden, in denen Lichtbilder und Gesichtsbilder zur Identifizierung von Personen genutzt werden dürfen.

KAPITEL XIII

Recht auf Zugriff und Überprüfung der Ausschreibungen

Artikel 44

Zum Zugriff auf Daten im SIS berechtigte nationale zuständige Behörden

(1) Die nationalen zuständigen Behörden erhalten Zugriff auf die in das SIS eingegebenen Daten mit dem Recht, diese unmittelbar oder in einer Kopie der SIS-Datenbank für folgende Zwecke abzufragen:

a) Grenzkontrollen gemäß der Verordnung (EU) 2016/399;

b) polizeiliche und zollrechtliche Überprüfungen in dem betreffenden Mitgliedstaat und deren Koordinierung durch hierfür bezeichnete Behörden;

c) Verhütung, Ermittlung, Aufdeckung oder Verfolgung terroristischer oder sonstiger schwerer Straftaten oder Strafvollstreckung in dem betreffenden Mitgliedstaat, sofern die Richtlinie (EU) 2016/680 Anwendung findet;

d) die Prüfung der Voraussetzungen für bzw. Entscheidungen über die Einreise und den Aufenthalt von Drittstaatsangehörigen im Hoheitsgebiet der Mitgliedstaaten — einschließlich im Hinblick auf Aufenthaltstitel und Visa für den längerfristigen Aufenthalt —, die Rückführung von Drittstaatsangehörigen sowie die Durchführung von Kontrollen von Drittstaatsangehörigen, die illegal in das Hoheitsgebiet der Mitgliedstaaten einreisen oder sich dort aufhalten;

e) Sicherheitskontrollen von Drittstaatsangehörigen, die internationalen Schutz beantragen, sofern die Behörden, die die Kontrollen ausführen, keine „Asylbehörden" im Sinne des Artikels 2 Buchstabe f der Richtlinie 2013/32/EU des Europäischen Parlaments und des Rates ([1]) darstellen, und gegebenenfalls für die beratende Unterstützung gemäß der Verordnung (EG) Nr. 377/2004 des Rates ([2]);

(2) Auch die für die Einbürgerung zuständigen nationalen Behörden können zur Prüfung eines Einbürgerungsantrags — wie in den nationalen Rechtsvorschriften vorgesehen — Zugriff auf die Daten im SIS mit dem Recht erhalten, diese unmittelbar abzufragen.

(3) Auch die nationalen Justizbehörden, einschließlich derjenigen, die für die Einleitung der staatsanwaltlichen Ermittlungen im Strafverfahren und justizielle Ermittlungen vor der Erhebung der Anklage gegen eine Person zuständig sind, sowie ihre Koordinierungsstellen können zur Ausführung ihrer Aufgaben — wie in den nationalen Rechtsvorschriften vorgesehen — Zugriff auf die in das SIS eingegebenen Daten mit dem Recht erhalten, diese unmittelbar abzufragen.

(4) Die in diesem Artikel genannten zuständigen Behörden werden in die Liste nach Artikel 56 Absatz 7 aufgenommen.

Artikel 45

Kfz-Zulassungsstellen

(1) Die für die Ausstellung von Fahrzeug-Zulassungsbescheinigungen im Sinne der Richtlinie 1999/37/EG des Rates ([3]) zuständigen Stellen der Mitgliedstaaten erhalten ausschließlich zur Überprüfung, ob die ihnen zur Zulassung vorgeführten Fahrzeuge und die dazugehörigen Fahrzeug-Zulassungsbescheinigungen und Kennzeichen gestohlen, unterschlagen oder auf sonstige Weise abhandengekommen, gefälscht sind, oder zur Beweissicherung in Strafverfahren gesucht werden, Zugang zu den gemäß Artikel 38 Absatz 2 Buchstaben a, b, c, m und p dieser Verordnung in das SIS eingegebene Daten.

Der Zugriff auf die Daten durch die in Unterabsatz 1 genannten Stellen erfolgt nach Maßgabe des nationalen Rechts des betreffenden Mitgliedstaats und wird auf die spezifische Zuständigkeit der betroffenen Dienststellen begrenzt.

(2) Stellen gemäß Absatz 1, bei denen es sich um staatliche Stellen handelt, dürfen Daten im SIS direkt abrufen.

([1]) Richtlinie 2013/32/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 zu gemeinsamen Verfahren für die Zuerkennung und Aberkennung des internationalen Schutzes (ABl. L 180 vom 29.6.2013, S. 60).

([2]) Verordnung (EG) Nr. 377/2004 des Rates vom 19. Februar 2004 zur Schaffung eines Netzes von Verbindungsbeamten für Einwanderungsfragen (ABl. L 64 vom 2.3.2004, S. 1).

([3]) Richtlinie 1999/37/EG des Rates vom 29. April 1999 über Zulassungsdokumente für Fahrzeuge (ABl. L 138 vom 1.6.1999, S. 57).

(3) Stellen gemäß Absatz 1 dieses Artikels, bei denen es sich um nichtstaatliche Stellen handelt, erhalten nur über eine Behörde nach Artikel 44 Zugang zu den Daten im SIS. Diese Behörde darf die Daten direkt abrufen und sie an die betreffende Stelle weiterleiten. Der jeweilige Mitgliedstaat sorgt dafür, dass die betreffende Stelle und ihre Mitarbeiter verpflichtet werden, etwaige Beschränkungen hinsichtlich der zulässigen Verwendung der ihnen von der Behörde übermittelten Daten einzuhalten.

(4) Artikel 39 gilt nicht für den gemäß dem vorliegenden Artikel erfolgenden Zugriff auf das SIS. Die Weitergabe von Informationen, die die Stellen gemäß Absatz 1 dieses Artikels durch den Zugriff auf das SIS erhalten haben, an die Polizei- oder Justizbehörden erfolgt nach Maßgabe des nationalen Rechts.

Artikel 46

Zulassungsstellen für Wasser- und Luftfahrzeuge

(1) Die für die Ausstellung von Zulassungsbescheinigungen für Wasserfahrzeuge, einschließlich Wasserfahrzeugmotoren, und Luftfahrzeuge, einschließlich Flugzeugmotoren, oder für das Verkehrsmanagement von Wasserfahrzeugen, einschließlich Wasserfahrzeugmotoren, und Luftfahrzeugen, einschließlich Flugzeugmotoren, zuständigen Stellen erhalten ausschließlich zur Überprüfung, ob die ihnen zur Zulassung vorgeführten Wasserfahrzeuge (einschließlich Wasserfahrzeugmotoren) und Luftfahrzeuge (einschließlich Flugzeugmotoren) beziehungsweise die ihrem Verkehrsmanagement unterliegenden Wasser- und Luftfahrzeuge gestohlen, unterschlagen, auf sonstige Weise abhandengekommen sind oder als Beweismittel in Strafverfahren gesucht werden, Zugang zu folgenden gemäß Artikel 38 Absatz 2 in das SIS eingegebene Daten:

a) Daten über Wasserfahrzeuge;

b) Daten über Wasserfahrzeugmotoren;

c) Daten über Luftfahrzeuge;

d) Daten über Flugzeugmotoren.

Der Zugang zu den Daten für die in Unterabsatz 1 genannten Stellen wird auf die spezifische Zuständigkeit der betroffenen Stellen begrenzt.

(2) Stellen gemäß Absatz 1, bei denen es sich um staatliche Stellen handelt, dürfen Daten im SIS direkt abrufen.

(3) Stellen gemäß Absatz 1 dieses Artikels, bei denen es sich um nichtstaatliche Stellen handelt, erhalten nur über eine Behörde nach Artikel 44 Zugang zu den Daten im SIS. Diese Behörde darf die Daten direkt abrufen und sie an die betreffende Stelle weiterleiten. Der jeweilige Mitgliedstaat sorgt dafür, dass die betreffende Stelle und deren Mitarbeiter verpflichtet werden, etwaige Beschränkungen hinsichtlich der zulässigen Verwendung der ihnen von der Behörde übermittelten Daten einzuhalten.

(4) Artikel 39 gilt nicht für den gemäß dem vorliegenden Artikel erfolgenden Datenabruf im SIS. Die Weitergabe von Informationen, die die Stellen gemäß Absatz 1 dieses Artikels durch den Zugang zum SIS erhalten haben, an die Polizei- oder Justizbehörden erfolgt nach Maßgabe des nationalen Rechts.

Artikel 47

Zulassungsstellen für Schusswaffen

(1) Die für die Ausstellung von Zulassungsbescheinigungen für Schusswaffen zuständigen Stellen in den Mitgliedstaaten erhalten Zugang zu den gemäß den Artikeln 26 und 36 in das SIS eingegebenen Daten in Bezug auf Personen und zu den gemäß Artikel 38 Absatz 2 in das SIS eingegebenen Daten in Bezug auf Schusswaffen. Der Zugang erfolgt zur Überprüfung, ob die Person, die eine Zulassung beantragt, zum Zwecke der Übergabe- oder Auslieferungshaft gesucht wird oder zum Zwecke verdeckter Kontrollen, Ermittlungsanfragen oder gezielter Kontrollen, oder zur Überprüfung, ob Schusswaffen, die zur Zulassung vorgelegt werden, zur Sicherstellung oder Beweissicherung in Strafverfahren gesucht werden.

(2) Der Zugang der in Absatz 1 genannten Stellen zu den Daten erfolgt nach Maßgabe des nationalen Rechts und wird auf die spezifische Zuständigkeit der betroffenen Dienststellen begrenzt.

(3) Stellen gemäß Absatz 1, bei denen es sich um staatliche Stellen handelt, dürfen die Daten im SIS direkt abrufen.

(4) Stellen gemäß Absatz 1, bei denen es sich um nichtstaatliche Stellen handelt, erhalten nur über eine Behörde nach Artikel 44 Zugang zu den Daten im SIS. Diese Behörde darf die Daten direkt abrufen und unterrichtet die betroffene Stelle davon, ob die Schusswaffe registriert werden kann. Der betreffende Mitgliedstaat sorgt dafür, dass die betreffende Stelle und deren Mitarbeiter verpflichtet werden, etwaige Beschränkungen hinsichtlich der zulässigen Verwendung der ihnen von der vermittelnden Behörde übermittelten Daten einzuhalten.

(5) Artikel 39 gilt nicht für den gemäß dem vorliegenden Artikel erfolgenden Datenabruf im SIS. Die Weitergabe von Informationen, die die Stellen gemäß Absatz 1 dieses Artikels durch den Zugang zum SIS erhalten haben, an die Polizei- oder Justizbehörden erfolgt nach Maßgabe des nationalen Rechts.

Artikel 48

Zugriff von Europol auf Daten im SIS

(1) Die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol), die durch die Verordnung (EU) 2016/794 errichtet wurde, hat, soweit dies zur Erfüllung ihres Mandats notwendig ist, das Recht, auf die Daten im SIS zuzugreifen und diese abzufragen. Europol kann auch Zusatzinformationen im Einklang mit den Bestimmungen des SIRENE-Handbuchs austauschen und zusätzlich anfragen.

(2) Stellt sich bei einer Abfrage durch Europol heraus, dass eine Ausschreibung im SIS gespeichert ist, setzt Europol den ausschreibenden Mitgliedstaat im Wege des Austauschs von Zusatzinformationen mithilfe der Kommunikationsinfrastruktur und gemäß den Bestimmungen des SIRENE-Handbuchs davon in Kenntnis. Bis Europol in der Lage ist, die für den Austausch von Zusatzinformationen vorgesehenen Funktionen zu verwenden, setzt es den ausschreibenden Mitgliedstaat über die in der Verordnung (EU) 2016/794 bestimmten Kanäle davon in Kenntnis.

(3) Europol kann die von den Mitgliedstaaten übermittelten Zusatzinformationen für die Zwecke ihres Abgleichs mit Europols Datenbanken und Projekten der operativen Analysen im Hinblick auf die Ermittlung etwaiger Zusammenhänge oder anderer relevanter Verbindungen sowie für die in Artikel 18 Absatz 2 Buchstaben a, b und c der Verordnung (EU) 2016/794 genannten strategischen, thematischen oder operativen Analysen verarbeiten. Jegliche Verarbeitung von Zusatzinformationen durch Europol für die Zwecke dieses Artikels erfolgt im Einklang mit jener Verordnung.

(4) Die Nutzung der durch eine Abfrage im SIS oder durch die Verarbeitung von Zusatzinformationen gewonnenen Informationen durch Europol unterliegt der Zustimmung des ausschreibenden Mitgliedstaats. Gestattet der Mitgliedstaat die Nutzung derartiger Informationen, so erfolgt deren Verarbeitung durch Europol nach Maßgabe der Verordnung (EU) 2016/794. Europol gibt derartige Informationen nur mit Zustimmung des ausschreibenden Mitgliedstaats und unter uneingeschränkter Wahrung der Vorschriften des Unionsrechts zum Datenschutz an Drittländer und -stellen weiter.

(5) Europol

a) unterlässt es unbeschadet der Absätze 4 und 6, Teile des SIS, zu denen sie Zugang hat, oder die darin gespeicherten Daten, auf die sie Zugriff hat, mit einem von oder bei Europol betriebenen System für die Datenerhebung und -verarbeitung zu verbinden bzw. in ein solches zu übernehmen oder einen bestimmten Teil des SIS herunterzuladen oder in anderer Weise zu vervielfältigen;

b) löscht ungeachtet des Artikels 31 Absatz 1 der Verordnung (EU) 2016/794 Zusatzinformationen, die personenbezogene Daten enthalten, spätestens ein Jahr nach der Löschung der entsprechenden Ausschreibung. Abweichend hiervon darf Europol, sofern diese Agentur in ihren Datenbanken oder Projekten für die operationelle Analyse über Informationen zu einem Fall verfügt, der mit den Zusatzinformationen in Verbindung steht, ausnahmsweise die Zusatzinformationen über diese Frist hinaus speichern, sofern dies zur Erfüllung ihrer Aufgaben erforderlich ist. Erforderlichenfalls unterrichtet Europol den ausschreibenden und den vollziehenden Mitgliedstaat über die weitere Speicherung derartiger Zusatzinformationen und legt eine Begründung dafür vor;

c) beschränkt den Zugriff auf die Daten im SIS, einschließlich der Zusatzinformationen, auf die eigens dazu ermächtigten Bediensteten von Europol, die diese Daten für die Erfüllung ihrer Aufgaben benötigen;

d) legt Maßnahmen zur Gewährleistung der Sicherheit, der Geheimhaltung und der Eigenkontrolle gemäß den Artikeln 10, 11 und 13 fest und wendet sie an;

e) stellt sicher, dass das zur Verarbeitung von SIS-Daten ermächtigte Personal eine angemessene Schulung und Unterrichtung nach Artikel 14 Absatz 1 erhält; und

f) gestattet dem Europäischen Datenschutzbeauftragten unbeschadet der Verordnung (EU) 2016/794, die Tätigkeiten Europols bei der Ausübung ihres Rechts auf Zugriff auf die Daten im SIS und deren Abfrage sowie beim Austausch und bei der Verarbeitung von Zusatzinformationen zu überwachen und zu überprüfen.

(6) Europol darf Daten aus dem SIS nur zu technischen Zwecken vervielfältigen, wenn dies zur direkten Abfrage durch die ordnungsgemäß ermächtigten Europol-Bediensteten erforderlich ist. Auf solche Vervielfältigungen findet diese Verordnung Anwendung. Die technische Kopie wird nur für die Zwecke der Speicherung von SIS-Daten verwendet, während diese Daten abgefragt werden. Sobald die Daten abgefragt wurden, werden sie gelöscht. Diese Verwendungen sind nicht als rechtswidriges Herunterladen oder Vervielfältigen von SIS-Daten anzusehen. Europol darf Ausschreibungsdaten oder ergänzende Daten, die von Mitgliedstaaten oder der CS-SIS übermittelt wurden, nicht in andere Europol-Systeme kopieren.

(7) Für die Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenkontrolle und der Sicherstellung der angemessenen Sicherheit und Integrität der Daten führt Europol gemäß den Bestimmungen des Artikels 12 über jeden Zugriff auf das SIS und jede Abfrage im SIS Protokolle. Diese Protokolle und Dokumentationen sind nicht als rechtswidriges Herunterladen oder Vervielfältigen eines Teils des SIS anzusehen.

(8) Die Mitgliedstaaten unterrichten Europol im Wege des Austauschs von Zusatzinformationen über jeden Treffer zu Ausschreibungen im Zusammenhang mit terroristischen Straftaten. Die Mitgliedstaaten können ausnahmsweise davon absehen, Europol zu unterrichten, wenn dies laufende Ermittlungen oder die Sicherheit einer Person gefährden oder wesentlichen Interessen der Sicherheit des ausschreibenden Mitgliedstaats zuwiderlaufen würde.

(9) Absatz 8 gilt ab dem Zeitpunkt, zu dem Europol Zusatzinformationen gemäß Absatz 1 erhalten kann.

Artikel 49

Zugriff von Eurojust auf Daten im SIS

(1) Nur die nationalen Mitglieder von Eurojust und die sie unterstützenden Personen haben — falls dies zur Erfüllung ihres Mandats erforderlich ist — Zugriff auf die nach den Artikeln 26, 32, 34, 38 und 40 Daten im SIS mit dem Recht, diese abzufragen.

(2) Stellt sich bei der Abfrage durch ein nationales Mitglied von Eurojust heraus, dass eine Ausschreibung im SIS gespeichert ist, setzt dieses nationale Mitglied den ausschreibenden Mitgliedstaat davon in Kenntnis. Eurojust darf die bei einer solchen Abfrage erlangten Informationen nur mit Zustimmung des ausschreibenden Mitgliedstaats und unter uneingeschränkter Wahrung der Vorschriften des Unionsrechts zum Datenschutz an Drittländer und -stellen weitergeben.

(3) Dieser Artikel gilt unbeschadet der Bestimmungen der Verordnung (EU) 2018/1727 des Europäischen Parlaments und des Rates ([1]) und der Verordnung (EU) 2018/1725 betreffend den Datenschutz und die Haftung wegen unbefugter oder unrichtiger Datenverarbeitung durch die nationalen Mitglieder von Eurojust oder die sie unterstützenden Personen sowie der Befugnisse des Europäischen Datenschutzbeauftragten gemäß diesen Verordnungen.

(4) Für die Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenkontrolle und der Sicherstellung der angemessenen Sicherheit und Integrität der Daten führt Eurojust gemäß den Bestimmungen des Artikels 12 über jeden Zugriff auf das SIS und jede Abfrage im SIS durch ein nationales Mitglied von Eurojust oder durch eine dieses Mitglied unterstützende Person Protokolle.

(5) Weder dürfen Teile des SIS mit einem der Erhebung und Verarbeitung von Daten dienenden, von oder bei Eurojust betriebenen System verbunden werden, noch dürfen Daten im SIS, auf die die nationalen Mitglieder oder die sie unterstützenden Personen Zugriff haben, an ein solches System übermittelt werden. Kein Teil des SIS darf heruntergeladen oder kopiert werden. Die Protokollierung von Zugriffen und Abfragen ist nicht als rechtswidriges Herunterladen oder Vervielfältigen von SIS-Daten anzusehen.

(6) Eurojust legt Maßnahmen zur Gewährleistung der Sicherheit, der Geheimhaltung und der Eigenkontrolle gemäß den Artikeln 10, 11 und 13 fest und wendet sie an.

Artikel 50

Zugriff von Mitgliedern der europäischen Grenz- und Küstenwacheteams, der Teams von mit rückkehrbezogenen Aufgaben betrautem Personal sowie der Teams zur Unterstützung der Migrationssteuerung auf Daten im SIS

(1) Gemäß Artikel 40 Absatz 8 der Verordnung (EU) 2016/1624 haben Mitglieder der Teams gemäß Artikel 2 Nummern 8 und 9 jener Verordnung im Rahmen ihres Mandats und insoweit dies zur Erfüllung ihrer Aufgaben erforderlich und im Einsatzplan für einen spezifischen Einsatz vorgesehen ist, das Recht auf Zugriff auf Daten im SIS und deren Abfrage, sofern sie zur Durchführung der Kontrollen gemäß Artikel 44 Absatz 1 der vorliegenden Verordnung ermächtigt sind und die in Artikel 14 Absatz 1 der vorliegenden Verordnung vorgeschriebene Schulung absolviert haben. Der Zugriff auf die Daten im SIS darf keinem anderen Teammitglied übertragen werden.

(2) Die Mitglieder der in Absatz 1 genannten Teams üben ihr Recht auf Zugriff auf Daten im SIS und deren Abfrage gemäß Absatz 1 unter Verwendung einer technischen Schnittstelle aus. Die technische Schnittstelle wird von der Europäischen Agentur für die Grenz- und Küstenwache eingerichtet und gewartet und ermöglicht eine direkte Verbindung mit dem zentralen SIS.

(3) Stellt sich bei der Abfrage durch ein Mitglied der Teams gemäß Absatz 1 dieses Artikels heraus, dass eine Ausschreibung im SIS vorliegt, wird der ausschreibende Mitgliedstaat hiervon unterrichtet. Nach Artikel 40 der Verordnung (EU) 2016/1624 handeln die Mitglieder der Teams in Reaktion auf eine Ausschreibung im SIS nur auf Anweisung und grundsätzlich nur in Gegenwart von Grenzschutzbeamten oder mit rückkehrbezogenen Aufgaben betrautem Personal des Einsatzmitgliedstaats, in dem sie tätig sind. Der Einsatzmitgliedstaat kann Teammitglieder ermächtigen, in seinem Namen zu handeln.

(4) Für die Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenkontrolle und der Sicherstellung der angemessenen Sicherheit und Integrität der Daten führt die Europäische Agentur für die Grenz- und Küstenwache gemäß den Bestimmungen des Artikels 12 über jeden Zugriff auf das SIS und jede Abfrage im SIS Protokolle.

(5) Die Europäische Agentur für die Grenz- und Küstenwache legt Maßnahmen zur Gewährleistung der Sicherheit, der Geheimhaltung und der Eigenkontrolle gemäß den Artikeln 10, 11 und 13 fest, wendet sie an und sorgt dafür, dass die in Absatz 1 dieses Artikels genannten Teams diese Maßnahmen anwenden.

(6) Dieser Artikel ist nicht so auszulegen, dass er sich auf die Bestimmungen der Verordnung (EU) 2016/1624 betreffend den Datenschutz oder die Haftung der Europäischen Agentur für die Grenz- und Küstenwache wegen unbefugter oder unrichtiger Datenverarbeitung durch diese auswirkt.

([1]) Verordnung (EU) 2018/1727 des Europäischen Parlaments und des Rates vom 14. November 2018 betreffend die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) und zur Ersetzung und Aufhebung des Beschlusses 2002/187/JI des Rates (ABl. L 295 vom 21.11.2018, S. 138).

(7) Unbeschadet des Absatzes 2 dürfen weder Teile des SIS mit einem der Erhebung und Verarbeitung von Daten dienenden System verbunden werden, das von den in Absatz 1 genannten Teams oder bei der Europäischen Agentur für die Grenz- und Küstenwache betrieben wird, noch dürfen die Daten im SIS, auf die diese Teams Zugriff haben, an ein solches System übermittelt werden. Kein Teil des SIS darf heruntergeladen oder kopiert werden. Die Protokollierung von Zugriffen und Abfragen ist nicht als Herunterladen oder Vervielfältigen von SIS-Daten anzusehen.

(8) Die Europäische Agentur für die Grenz- und Küstenwache gestattet dem Europäischen Datenschutzbeauftragten, die Tätigkeiten der Teams gemäß diesem Artikel bei der Ausübung ihres Rechts auf Zugriff auf die Daten im SIS und deren Abfrage zu überwachen und zu überprüfen. Dies gilt unbeschadet weiterer Bestimmungen der Verordnung (EU) 2018/1725.

Artikel 51

Evaluierung der Nutzung des SIS durch Europol, Eurojust und die Europäische Agentur für die Grenz- und Küstenwache

(1) Die Kommission evaluiert mindestens alle fünf Jahre den Betrieb und die Nutzung des SIS durch Europol, die nationalen Mitglieder von Eurojust und die sie unterstützenden Personen und die in Artikel 50 Absatz 1 genannten Teams.

(2) Europol, Eurojust und die Europäische Agentur für die Grenz- und Küstenwache stellen angemessene Folgemaßnahmen zu den Ergebnissen und Empfehlungen der Evaluierung sicher.

(3) Ein Bericht über die Ergebnisse der Evaluierung und die entsprechenden Folgemaßnahmen wird dem Europäischen Parlament und dem Rat übermittelt.

Artikel 52

Umfang des Zugriffs

Endnutzer einschließlich Europol, der nationalen Mitglieder von Eurojust und der sie unterstützenden Personen und der Mitglieder der Teams gemäß Artikel 2 Nummern 8 und 9 der Verordnung (EU) 2016/1624 greifen nur auf Daten zu, die zur Erfüllung ihrer Aufgaben erforderlich sind.

Artikel 53

Prüffrist für Personenausschreibungen

(1) Personenausschreibungen werden nicht länger gespeichert, als für den Zweck, für den sie eingegeben wurden, erforderlich ist.

(2) Ein Mitgliedstaat kann eine Personenausschreibung für die Zwecke des Artikels 26 und des Artikels 32 Absatz 1 Buchstaben a und b für einen Zeitraum von fünf Jahren eingeben. Der ausschreibende Mitgliedstaat prüft innerhalb dieser fünf Jahre die Erforderlichkeit, die Ausschreibung beizubehalten.

(3) Ein Mitgliedstaat kann eine Personenausschreibung für die Zwecke der Artikel 34 und 40 für einen Zeitraum von drei Jahren eingeben. Der ausschreibende Mitgliedstaat prüft innerhalb dieser drei Jahre die Erforderlichkeit, die Ausschreibung beizubehalten.

(4) Ein Mitgliedstaat kann eine Personenausschreibung für die Zwecke des Artikels 32 Absatz 1 Buchstaben c, d und e und des Artikels 36 für einen Zeitraum von einem Jahr eingeben. Der ausschreibende Mitgliedstaat prüft innerhalb dieses Jahres die Erforderlichkeit, die Ausschreibung beizubehalten.

(5) Jeder Mitgliedstaat bestimmt gegebenenfalls kürzere Prüffristen nach Maßgabe seines nationalen Rechts.

(6) Innerhalb der Prüffrist gemäß den Absätzen 2, 3 und 4 kann der ausschreibende Mitgliedstaat nach einer umfassenden individuellen Bewertung, die zu protokollieren ist, beschließen, die Personenausschreibung noch über die Prüffrist hinaus beizubehalten, wenn dies für den der Ausschreibung zugrunde liegenden Zweck erforderlich und verhältnismäßig ist. In diesen Fällen gelten die Absätze 2, 3 und 4 auch für die Verlängerung. Jede solche Verlängerung wird der CS-SIS mitgeteilt.

(7) Personenausschreibungen werden nach Ablauf der in den Absätzen 2, 3 und 4 genannten Prüffrist automatisch gelöscht, es sei denn, der ausschreibende Mitgliedstaat hat der CS-SIS eine Verlängerung nach Absatz 6 mitgeteilt. Die CS-SIS weist den ausschreibenden Mitgliedstaat mit einem Vorlauf von vier Monaten automatisch auf die programmierte Löschung hin.

(8) Die Mitgliedstaaten führen Statistiken über die Anzahl der Personenausschreibungen, deren Erfassungsdauer gemäß Absatz 6 dieses Artikels verlängert worden ist, und übermitteln sie auf Anfrage an die in Artikel 69 genannten Aufsichtsbehörden.

(9) Sobald ein SIRENE-Büro erkennt, dass eine Personenausschreibung ihren Zweck erfüllt hat und daher gelöscht werden sollte, teilt es dies umgehend der Behörde mit, die die Ausschreibung eingegeben hat. Die Behörde verfügt über eine Frist von 15 Kalendertagen ab Eingang dieser Mitteilung, um zu antworten, dass die Ausschreibung gelöscht wurde oder wird, oder Gründe für die Beibehaltung der Ausschreibung anzugeben. Geht bis Ende der Frist von 15 Tagen keine derartige Antwort ein, so sorgt das SIRENE-Büro dafür, dass die Ausschreibung gelöscht wird. Wenn dies nach nationalem Recht zulässig ist, wird die Ausschreibung vom SIRENE-Büro gelöscht. SIRENE-Büros melden wiederholt auftretende Probleme, auf die sie bei Tätigkeiten gemäß diesem Absatz stoßen, ihrer Aufsichtsbehörde.

Artikel 54

Prüffrist für Sachfahndungsausschreibungen

(1) Sachfahndungsausschreibungen werden nicht länger als für den Zweck, für den sie eingegeben wurden, erforderlich gespeichert.

(2) Ein Mitgliedstaat kann eine Sachfahndungsausschreibung für die Zwecke der Artikel 36 und 38 für einen Zeitraum von zehn Jahren eingeben. Der ausschreibende Mitgliedstaat prüft innerhalb dieser zehn Jahre die Erforderlichkeit, die Ausschreibung beizubehalten.

(3) Sachfahndungsausschreibungen gemäß den Artikeln 26, 32, 34 und 36 werden gemäß Artikel 53 geprüft, wenn sie im Zusammenhang mit einer Personenausschreibung stehen. Solche Ausschreibungen werden nur so lange wie die Personenausschreibung beibehalten.

(4) Innerhalb der Prüffrist gemäß den Absätzen 2 und 3 kann der ausschreibende Mitgliedstaat beschließen, die Sachfahndungsausschreibung noch über die Prüffrist hinaus beizubehalten, wenn dies für den der Ausschreibung zugrunde liegenden Zweck erforderlich ist. In diesen Fällen gilt Absatz 2 bzw. 3.

(5) Die Kommission kann Durchführungsrechtsakte erlassen, um für bestimmte Kategorien von Sachfahndungsausschreibungen kürzere Prüffristen festzulegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

(6) Die Mitgliedstaaten führen Statistiken über die Zahl der Sachfahndungsausschreibungen, deren Erfassungsdauer nach Absatz 4 verlängert worden ist.

KAPITEL XIV

Löschung von Ausschreibungen

Artikel 55

Löschung von Ausschreibungen

(1) Ausschreibungen von Personen zum Zwecke der Übergabe- oder Auslieferungshaft nach Artikel 26 werden gelöscht, wenn die betreffende Person an die zuständigen Behörden des ausschreibenden Mitgliedstaats übergeben oder ausgeliefert worden ist. Sie werden zudem gelöscht, wenn die richterliche Entscheidung, die der Ausschreibung zugrunde lag, von der zuständigen Justizbehörde nach nationalem Recht aufgehoben worden ist. Sie werden außerdem gelöscht, wenn die Ausschreibung gemäß Artikel 53 abgelaufen ist.

(2) Für die Löschung von Ausschreibungen von vermissten Personen oder schutzbedürftigen Personen gemäß Artikel 32, die am Reisen gehindert werden müssen, gelten folgende Bestimmungen:

a) Ausschreibungen von vermissten und von Entführung bedrohten Kindern werden gelöscht, sobald

   i) der betreffende Fall gelöst worden ist, beispielsweise wenn das betreffende Kind ausfindig gemacht oder rückgeführt wurde oder die zuständigen Behörden im vollziehenden Mitgliedstaat entschieden haben, in wessen Obhut das Kind gegeben wird;

   ii) die Ausschreibung nach Artikel 53 abgelaufen ist oder

   iii) die zuständige Behörde des ausschreibenden Mitgliedstaats die Löschung beschlossen hat.

b) Ausschreibungen von vermissten Erwachsenen, bei denen keine Schutzmaßnahmen ergriffen werden müssen, werden gelöscht, sobald

   i) die zu ergreifende Maßnahme ausgeführt wurde, wenn ihr Aufenthaltsort vom vollziehenden Mitgliedstaat festgestellt wurde;

   ii) die Ausschreibung nach Artikel 53 abgelaufen ist oder

   iii) die zuständige Behörde des ausschreibenden Mitgliedstaats die Löschung beschlossen hat.

c) Ausschreibungen von vermissten Erwachsenen, bei denen Schutzmaßnahmen ergriffen werden müssen, werden gelöscht, sobald

   i) die zu ergreifende Maßnahme ausgeführt wurde, wenn die Person unter Schutz gestellt wurde;

ii) die Ausschreibung nach Artikel 53 abgelaufen ist oder

iii) die zuständige Behörde des ausschreibenden Mitgliedstaats die Löschung beschlossen hat.

d) Ausschreibungen von volljährigen schutzbedürftigen Personen, die zu ihrem eigenen Schutz am Reisen gehindert werden müssen, und von Kindern, die am Reisen gehindert werden müssen, werden gelöscht, sobald

i) die zu ergreifende Maßnahme ausgeführt (beispielsweise die Person unter Schutz gestellt) wurde;

ii) die Ausschreibung nach Artikel 53 abgelaufen ist oder

iii) die zuständige Behörde des ausschreibenden Mitgliedstaats die Löschung beschlossen hat.

Wenn eine Person gemäß einer Entscheidung einer zuständigen Behörde in eine Einrichtung eingewiesen wurde, kann unbeschadet des nationalen Rechts eine Ausschreibung beibehalten werden, bis der Betreffende rückgeführt wurde.

(3) Ausschreibungen von im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesuchten Personen gemäß Artikel 34 werden gelöscht, sobald

a) der Aufenthaltsort der Person der zuständigen Behörde des ausschreibenden Mitgliedstaats mitgeteilt wurde;

b) die Ausschreibung nach Artikel 53 abgelaufen ist oder

c) die zuständige Behörde des ausschreibenden Mitgliedstaats die Löschung beschlossen hat.

Wenn ein Tätigwerden auf der Grundlage der Informationen gemäß Buchstabe a nicht möglich ist, informiert das SIRENE-Büro des ausschreibenden Mitgliedstaats das SIRENE-Büro des vollziehenden Mitgliedstaats, damit das Problem gelöst wird;

Wenn ein Treffer erzielt wurde und die Adressdaten an den ausschreibenden Mitgliedstaat weitergeleitet wurden und ein anschließender Treffer im gleichen vollziehenden Mitgliedstaat dieselben Adressdaten ergibt, wird der Treffer im vollziehenden Mitgliedstaat protokolliert, aber es werden weder die Adressdaten noch Zusatzinformationen erneut an den ausschreibenden Mitgliedstaat übermittelt. In einem solchen Fall informiert der vollziehende Mitgliedstaat den ausschreibenden Mitgliedstaat über die wiederholten Treffer, und der ausschreibende Mitgliedstaat nimmt eine umfassende individuelle Bewertung vor, ob die Ausschreibung beibehalten werden muss.

(4) Ausschreibungen für verdeckte Kontrollen, Ermittlungsanfragen oder gezielte Kontrollen gemäß Artikel 36 werden gelöscht, sobald

a) die Ausschreibung nach Artikel 53 abgelaufen ist oder

b) die zuständige Behörde des ausschreibenden Mitgliedstaats deren Löschung beschlossen hat.

(5) Sachfahndungsausschreibungen zur Sicherstellung oder Beweissicherung in Strafverfahren gemäß Artikel 38 werden gelöscht, sobald

a) die betreffende Sache sichergestellt oder eine entsprechende Maßnahme getroffen wurde und der erforderliche anschließende Austausch von Zusatzinformationen zwischen den betroffenen SIRENE-Büros stattgefunden hat oder die Sache einem anderen Gerichts- oder Verwaltungsverfahren unterworfen wird;

b) die Ausschreibung gemäß Artikel 53 abgelaufen ist oder

c) die zuständige Behörde des ausschreibenden Mitgliedstaats deren Löschung beschlossen hat.

(6) Ausschreibungen zu unbekannten gesuchten Personen gemäß Artikel 40 werden gelöscht, sobald

a) die betreffende Person identifiziert worden ist;

b) die Ausschreibung gemäß Artikel 53 abgelaufen ist oder

c) die zuständige Behörde des ausschreibenden Mitgliedstaats die Löschung beschlossen hat.

(7) Sachfahndungsausschreibungen, die gemäß den Artikeln 26, 32, 34 und 36 eingegeben wurden und die im Zusammenhang mit einer Personenausschreibung stehen, werden gelöscht, wenn die Personenausschreibung gemäß diesem Artikel gelöscht wird.

KAPITEL XV

Allgemeine Bestimmungen für die Datenverarbeitung

Artikel 56

Verarbeitung von SIS-Daten

(1) Die Mitgliedstaaten verarbeiten die in Artikel 20 genannten Daten nur für die Zwecke der in den Artikeln 26, 32, 34, 36, 38 und 40 genannten Ausschreibungskategorien.

(2) Die Daten werden nur zu technischen Zwecken vervielfältigt, wenn dies zur direkten Abfrage durch die in Artikel 44 genannten zuständigen Behörden erforderlich ist. Diese Verordnung findet auf solche Vervielfältigungen Anwendung. Ein Mitgliedstaat darf Ausschreibungsdaten oder ergänzende Daten, die von einem anderen Mitgliedstaat eingegeben wurden, nicht aus seinem N.SIS oder aus der CS-SIS in andere nationale Datenbestände kopieren.

(3) Technische Kopien nach Absatz 2, bei denen Offline-Datenbanken entstehen, dürfen für einen Zeitraum von höchstens 48 Stunden erfasst werden.

Die Mitgliedstaaten führen ein aktuelles Verzeichnis dieser Vervielfältigungen, stellen dieses Verzeichnis ihren Aufsichtsbehörden zur Verfügung und gewährleisten, dass diese Verordnung, insbesondere Artikel 10, auf diese Vervielfältigungen angewandt wird.

(4) Der Zugriff nationaler zuständiger Behörden nach Artikel 44 auf die Daten im SIS wird nur im Rahmen ihrer Zuständigkeiten und nur entsprechend bevollmächtigten Bediensteten gewährt.

(5) Jede Verarbeitung der in Ausschreibungen nach den Artikeln 26, 32, 34, 36, 38 und 40 dieser Verordnung enthaltenen Informationen zu anderen Zwecken als jenen, zu denen die Ausschreibung in das SIS eingegeben wurde, muss in Verbindung mit einem spezifischen Fall stehen und ist nur zulässig, soweit sie zur Abwehr einer unmittelbar bevorstehenden und schwerwiegenden Gefahr für die öffentliche Ordnung und Sicherheit, aus schwerwiegenden Gründen der nationalen Sicherheit oder zur Verhütung einer schweren Straftat erforderlich ist. Hierzu wird die vorherige Zustimmung des ausschreibenden Mitgliedstaats eingeholt.

(6) Jede Nutzung der SIS-Daten, die den Absätzen 1 bis 5 dieses Artikels nicht entspricht, wird nach dem nationalen Recht des jeweiligen Mitgliedstaats als Missbrauch bewertet und mit Sanktionen nach Maßgabe von Artikel 73 geahndet.

(7) Jeder Mitgliedstaat übermittelt eu-LISA eine Liste seiner zuständigen Behörden, die nach dieser Verordnung berechtigt sind, die Daten im SIS unmittelbar abzufragen, sowie alle Änderungen dieser Liste. In der Liste wird für jede Behörde angegeben, welche Daten sie für welche Aufgaben abfragen darf. eu-LISA sorgt dafür, dass die diese Liste jährlich im *Amtsblatt der Europäischen Union* veröffentlicht wird. eu-LISA führt auf ihrer Website eine laufend aktualisierte Liste der Änderungen, die von den Mitgliedstaaten im Zeitraum zwischen den jährlichen Veröffentlichungen übermittelt wurden.

(8) Soweit das Recht der Union keine besondere Regelung enthält, findet das nationale Recht des jeweiligen Mitgliedstaats auf die Daten in seinem N.SIS Anwendung.

Artikel 57

SIS-Daten und nationale Dateien

(1) Artikel 56 Absatz 2 berührt nicht das Recht eines Mitgliedstaats, SIS-Daten, in deren Zusammenhang Maßnahmen in seinem Hoheitsgebiet ergriffen wurden, in nationalen Dateien zu speichern. Diese Daten werden höchstens drei Jahre in nationalen Dateien gespeichert, es sei denn, in Sonderbestimmungen des nationalen Rechts ist eine längere Erfassungsdauer vorgesehen.

(2) Artikel 56 Absatz 2 berührt nicht das Recht eines Mitgliedstaats, Daten zu einer bestimmten Ausschreibung, die dieser Mitgliedstaat in das SIS eingegeben hat, in nationalen Dateien zu speichern.

Artikel 58

Information im Falle der Nichtausführung einer Ausschreibung

Kann die erbetene Maßnahme nicht durchgeführt werden, so unterrichtet der Mitgliedstaat, der um die Maßnahme ersucht wird, den ausschreibenden Mitgliedstaat im Wege des Austauschs von Zusatzinformationen umgehend hiervon.

Artikel 59

Qualität der Daten im SIS

(1) Der ausschreibende Mitgliedstaat ist für die Richtigkeit und Aktualität der Daten sowie die Rechtmäßigkeit der Eingabe in das und der Speicherung im SIS verantwortlich.

(2) Erhält ein ausschreibender Mitgliedstaat relevante ergänzende oder geänderte Daten nach Artikel 20 Absatz 3, so vervollständigt oder ändert er unverzüglich die betreffende Ausschreibung.

(3) Nur der ausschreibende Mitgliedstaat darf eine Änderung, Ergänzung, Berichtigung, Aktualisierung oder Löschung der von ihm in das SIS eingegebenen Daten vornehmen.

(4) Hat ein anderer als der ausschreibende Mitgliedstaat ergänzende oder geänderte Daten nach Artikel 20 Absatz 3, so übermittelt er sie dem ausschreibenden Mitgliedstaat unverzüglich im Wege des Austauschs von Zusatzinformationen, damit dieser die Ausschreibung vervollständigen oder ändern kann. Beziehen die ergänzenden oder geänderten Daten sich auf Personen, so werden sie nur übermittelt, wenn die Identität der Person festgestellt ist.

(5) Hat ein anderer als der ausschreibende Mitgliedstaat Anhaltspunkte dafür, dass Daten unrichtig sind oder unrechtmäßig gespeichert worden sind, so setzt er den ausschreibenden Mitgliedstaat so rasch wie möglich, spätestens aber zwei Arbeitstage, nachdem ihm diese Anhaltspunkte bekannt geworden sind, im Wege des Austauschs von Zusatzinformationen davon in Kenntnis. Der ausschreibende Mitgliedstaat prüft die Informationen und berichtigt oder löscht erforderlichenfalls die Daten unverzüglich.

(6) Können sich die Mitgliedstaaten nicht binnen zwei Monaten ab dem Zeitpunkt, zu dem die Anhaltspunkte nach Absatz 5 dieses Artikels erstmals bekannt geworden sind, einigen, so unterbreitet der Mitgliedstaat, der die Ausschreibung nicht eingegeben hat, die Angelegenheit den betreffenden Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten über die in Artikel 71 vorgesehene Zusammenarbeit zur Entscheidung.

(7) Die Mitgliedstaaten tauschen in den Fällen, in denen sich eine Person dahin gehend beschwert, dass sie nicht die in einer Ausschreibung gesuchte Person ist, Zusatzinformationen aus. Ergibt die Überprüfung, dass es sich bei der in der Ausschreibung gesuchten Person nicht um den Beschwerdeführer handelt, so wird der Beschwerdeführer über die Maßnahmen nach Artikel 62 und über das Recht auf Einlegung eines Rechtsbehelfs gemäß Artikel 68 Absatz 1 unterrichtet.

Artikel 60

Sicherheitsvorfälle

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

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

(3) Unbeschadet der Meldung und Mitteilung einer Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 der Verordnung (EU) 2016/679 oder Artikel 30 der Richtlinie (EU) 2016/680 setzen die Mitgliedstaaten, Europol, Eurojust und die Europäische Agentur für die Grenz- und Küstenwache unverzüglich die Kommission, eu-LISA, die zuständige Aufsichtsbehörde und den Europäischen Datenschutzbeauftragten von Sicherheitsvorfällen in Kenntnis. eu-LISA setzt die Kommission und den Europäischen Datenschutzbeauftragten unverzüglich von jedem das zentrale SIS betreffenden Sicherheitsvorfall in Kenntnis.

(4) Informationen über Sicherheitsvorfälle, die sich möglicherweise auf den Betrieb des SIS in einem Mitgliedstaat oder in eu-LISA, auf die Verfügbarkeit, die Integrität und die Vertraulichkeit der von anderen Mitgliedstaaten eingegebenen oder übermittelten Daten oder der ausgetauschten Zusatzinformationen auswirken, werden unverzüglich allen Mitgliedstaaten im Einklang mit dem von eu-LISA vorgelegten Plan für die Bewältigung von Sicherheitsvorfällen übermittelt.

(5) Die Mitgliedstaaten und eu-LISA arbeiten im Falle eines Sicherheitsvorfalls zusammen.

(6) Die Kommission meldet schwere Vorfälle umgehend dem Europäischen Parlament und dem Rat. Diese Berichte werden gemäß den geltenden Geheimschutzvorschriften als EU RESTRICTED/RESTREINT UE eingestuft.

(7) Wenn ein Sicherheitsvorfall durch einen Datenmissbrauch verursacht wird, müssen die Mitgliedstaaten, Europol, Eurojust und die Europäische Agentur für die Grenz- und Küstenwache dafür sorgen, dass Sanktionen gemäß Artikel 73 verhängt werden.

Artikel 61

Unterscheidung von Personen mit ähnlichen Merkmalen

(1) Wird bei der Eingabe einer neuen Ausschreibung festgestellt, dass im SIS bereits eine Ausschreibung einer Person mit denselben Identitätskriterien existiert, so kontaktiert das SIRENE-Büro den ausschreibenden Mitgliedstaat im Wege des Austauschs von Zusatzinformationen innerhalb von zwölf Stunden, um zu überprüfen, ob es sich um dieselbe Person handelt.

(2) Stellt sich bei der Überprüfung heraus, dass es sich bei der neuen Ausschreibung und der Person, die Gegenstand einer bereits in das SIS eingegebenen Ausschreibung ist, tatsächlich um die gleiche Person handelt, so wendet das SIRENE-Büro das Verfahren für die Eingabe einer Mehrfachausschreibung nach Artikel 23 an.

(3) Stellt sich bei der Überprüfung heraus, dass es sich hingegen um zwei verschiedene Personen handelt, so billigt das SIRENE-Büro das Ersuchen um eine zweite Ausschreibung und fügt die erforderlichen Daten zur Verhinderung einer falschen Identifizierung hinzu.

Artikel 62

Ergänzende Daten zur Behandlung von Fällen von Identitätsmissbrauch

(1) Könnte eine Person, die Gegenstand einer Ausschreibung sein soll, mit einer Person, deren Identität missbraucht wurde, verwechselt werden, so ergänzt der ausschreibende Mitgliedstaat vorbehaltlich der ausdrücklichen Genehmigung der Person, deren Identität missbraucht wurde, die Ausschreibung um Daten über diese Person, um negativen Auswirkungen einer falschen Identifizierung vorzubeugen. Personen, deren Identität missbraucht wurde, haben das Recht, ihre Zustimmung zur Verarbeitung der zugefügten personenbezogenen Daten zurückzuziehen.

(2) Daten über Personen, deren Identität missbraucht wurde, dürfen nur zu folgenden Zwecken verwendet werden:

a) um der zuständigen Behörde zu ermöglichen, zwischen der Person, deren Identität missbraucht wurde, und der Person, die Gegenstand der Ausschreibung sein soll, zu unterscheiden; und

b) um der Person, deren Identität missbraucht wurde, zu ermöglichen, ihre Identität zu beweisen und nachzuweisen, dass ihre Identität missbraucht wurde.

(3) Für die Zwecke dieses Artikels und vorbehaltlich der ausdrücklichen Zustimmung der Person, deren Identität missbraucht wurde, bezüglich jeder Datenkategorie dürfen nur die folgenden personenbezogenen Daten der Person, deren Identität missbraucht wurde, in das SIS eingegeben und dort weiterverarbeitet werden:

a) Nachnamen;

b) Vornamen;

c) Geburtsnamen;

d) frühere Namen und Aliasnamen, gegebenenfalls separat einzugeben;

e) besondere, objektive, unveränderliche körperliche Merkmale;

f) Geburtsort;

g) Geburtsdatum;

h) Geschlecht;

i) Lichtbilder und Gesichtsbilder;

j) Fingerabdrücke, Handflächenabdrücke oder beides;

k) sämtliche Staatsangehörigkeiten;

l) Art der Identifizierungsdokumente der Person;

m) Ausstellungsland der Identifizierungsdokumente der Person;

n) Nummer(n) der Identifizierungsdokumente der Person;

o) Ausstellungsdatum der Identifizierungsdokumente der Person;

p) Anschrift der Person;

q) Name des Vaters der Person;

r) Name der Mutter der Person.

(4) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung und Weiterentwicklung der notwendigen technischen Vorschriften für die Eingabe und Weiterverarbeitung der Daten gemäß Absatz 3 dieses Artikels. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

(5) Die Daten nach Absatz 3 werden zu demselben Zeitpunkt wie die entsprechende Ausschreibung oder auf Antrag der betreffenden Person bereits früher gelöscht.

(6) Nur die Behörden, die ein Zugriffsrecht für die entsprechende Ausschreibung haben, dürfen auf die Daten nach Absatz 3 zugreifen. Dieser Zugriff darf ausschließlich zur Verhinderung einer falschen Identifizierung erfolgen.

Artikel 63

Verknüpfungen zwischen Ausschreibungen

(1) Ein Mitgliedstaat kann von ihm im SIS vorgenommene Ausschreibungen miteinander verknüpfen. Durch eine solche Verknüpfung wird eine Verbindung zwischen zwei oder mehr Ausschreibungen hergestellt.

(2) Eine Verknüpfung wirkt sich nicht auf die jeweils zu ergreifende Maßnahme für jede verknüpfte Ausschreibung oder auf die Prüffrist für jede der verknüpften Ausschreibungen aus.

(3) Die Verknüpfung darf die in dieser Verordnung festgelegten Zugriffsrechte nicht beeinträchtigen. Behörden, die für bestimmte Ausschreibungskategorien kein Zugriffsrecht haben, dürfen nicht erkennen können, dass eine Verknüpfung mit einer Ausschreibung, auf die sie keinen Zugriff haben, besteht.

(4) Ein Mitgliedstaat verknüpft Ausschreibungen miteinander, wenn hierfür eine operationelle Notwendigkeit besteht.

(5) Ist ein Mitgliedstaat der Auffassung, dass eine von einem anderen Mitgliedstaat vorgenommene Verknüpfung zwischen Ausschreibungen nicht mit seinem nationalen Recht oder seinen internationalen Verpflichtungen vereinbar ist, so kann er die erforderlichen Maßnahmen ergreifen, um sicherzustellen, dass die Verknüpfung weder von seinem Hoheitsgebiet aus noch für außerhalb seines Hoheitsgebiets angesiedelte Behörden seines Landes zugänglich ist.

(6) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung und Weiterentwicklung von technischen Vorschriften für die Verknüpfung von Ausschreibungen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 64

Zweck und Erfassungsdauer von Zusatzinformationen

(1) Die Mitgliedstaaten bewahren Angaben über die einer Ausschreibung zugrunde liegenden Entscheidungen in ihrem SIRENE-Büro auf, um den Austausch von Zusatzinformationen zu erleichtern.

(2) Die von den SIRENE-Büros auf der Grundlage des Informationsaustauschs gespeicherten personenbezogenen Daten werden nicht länger als für den verfolgten Zweck erforderlich gespeichert. Sie werden auf jeden Fall spätestens ein Jahr nach der Löschung der entsprechenden Ausschreibung aus dem SIS gelöscht.

(3) Absatz 2 berührt nicht das Recht eines Mitgliedstaats, Daten zu einer bestimmten Ausschreibung, die dieser Mitgliedstaat eingegeben hat, oder zu einer Ausschreibung, in deren Zusammenhang Maßnahmen in seinem Hoheitsgebiet ergriffen wurden, in nationalen Dateien zu speichern. Die Frist für die Speicherung der Daten in diesen Dateien wird durch das nationale Recht geregelt.

Artikel 65

Übermittlung personenbezogener Daten an Dritte

Im SIS verarbeitete Daten sowie damit verbundene ausgetauschte Zusatzinformationen im Sinne dieser Verordnung dürfen Drittländern oder internationalen Organisationen nicht übermittelt oder zur Verfügung gestellt werden.

KAPITEL XVI

Datenschutz

Artikel 66

Anwendbare Gesetzgebung

(1) Für die Verarbeitung personenbezogener Daten durch eu-LISA, durch die Europäische Agentur für die Grenz- und Küstenwache und durch Eurojust im Rahmen der vorliegenden Verordnung gilt die Verordnung (EU) 2018/1725. Für die Verarbeitung personenbezogener Daten durch Europol im Rahmen dieser Verordnung gilt die Verordnung (EU) 2016/794.

(2) Für die Verarbeitung personenbezogener Daten im Rahmen der vorliegenden Verordnung durch die nationalen zuständigen Behörden und Stellen zum Zwecke der Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, gilt die Richtlinie (EU) 2016/680.

(3) Für die Verarbeitung personenbezogener Daten im Rahmen der vorliegenden Verordnung durch die nationalen zuständigen Behörden und Stellen gilt die Verordnung (EU) 2016/679, mit Ausnahme der Verarbeitung zum Zwecke der Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt.

Artikel 67

Recht auf Auskunft, Berichtigung unrichtiger Daten und Löschung unrechtmäßig gespeicherter Daten

(1) Die betroffenen Personen müssen in der Lage sein, die in den Artikeln 15 bis 17 der Verordnung (EU) 2016/679 und in Artikel 14 und Artikel 16 Absätze 1 und 2 der Richtlinie (EU) 2016/680 genannten Rechte auszuüben.

(2) Ein Mitgliedstaat, der nicht der ausschreibende Mitgliedstaat ist, darf der betroffenen Person Informationen über die personenbezogenen Daten der betroffenen Person, die verarbeitet werden, nur übermitteln, wenn er vorher dem ausschreibenden Mitgliedstaat Gelegenheit zur Stellungnahme gegeben hat. Die Kommunikation zwischen diesen Mitgliedstaaten erfolgt im Wege des Austauschs von Zusatzinformationen.

(3) Ein Mitgliedstaat trifft eine Entscheidung, der betroffenen Person keine Informationen — vollständig oder teilweise — zu übermitteln, nach Maßgabe seiner nationalen Rechtsvorschriften, soweit und solange diese teilweise oder vollständige Einschränkung in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und den Grundrechten und den berechtigten Interessen der betroffenen Person gebührend Rechnung getragen wird,

a) zur Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden,

b) zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,

c) zum Schutz der öffentlichen Sicherheit,

d) zum Schutz der nationalen Sicherheit oder

e) zum Schutz der Rechte und Freiheiten anderer.

In Fällen gemäß Unterabsatz 1 informiert der Mitgliedstaat die betroffenen Personen unverzüglich schriftlich über jede Verweigerung oder Einschränkung des Zugriffs und über die Gründe für die Verweigerung oder die Einschränkung. Dies kann unterlassen werden, wenn die Übermittlung dieser Information einem der in Unterabsatz 1 Buchstaben a bis e genannten Zwecke zuwiderliefe. Der Mitgliedstaat informiert die betroffene Person über die Möglichkeit, bei der Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

Der Mitgliedstaat gibt dokumentiert die sachlichen oder rechtlichen Gründe für die Entscheidung, der betroffenen Person keine Informationen zu übermitteln. Diese Angaben sind den Aufsichtsbehörden zur Verfügung zu stellen.

In solchen Fällen muss dafür gesorgt werden, dass die betroffene Person ihre Rechte auch durch die zuständigen Aufsichtsbehörden ausüben kann.

(4) Wenn eine betroffene Person einen Antrag auf Auskunft, Berichtigung oder Löschung gestellt hat, informiert der Mitgliedstaat die betroffene Person so schnell wie möglich, in jedem Fall jedoch innerhalb der in Artikel 12 Absatz 3 der Verordnung (EU) 2016/679 genannten Frist darüber, welche Maßnahmen zur Wahrung der Rechte gemäß diesem Artikel getroffen wurden.

Artikel 68

Rechtsbehelf

(1) Unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 über den Rechtsbehelf hat jeder das Recht, einen Rechtsbehelf wegen einer seine Person betreffenden Ausschreibung auf Auskunft, Berichtigung, Löschung, Information oder Schadenersatz bei jeder zuständigen Behörde, einschließlich eines Gerichts, einzulegen, die nach dem Recht eines Mitgliedstaats zuständig ist.

(2) Unbeschadet des Artikels 72 verpflichten sich die Mitgliedstaaten, rechtskräftige Entscheidungen der Gerichte oder Behörden nach Absatz 1 zu vollstrecken.

(3) Die Mitgliedstaaten erstatten dem Europäischen Datenschutzausschuss jährlich Bericht darüber,

a) wie viele Zugangsanträge dem für die Verarbeitung Verantwortlichen übermittelt wurden und in wie vielen Fällen Zugang zu den Daten gewährt wurde;

b) wie viele Zugangsanträge der Aufsichtsbehörde übermittelt wurden und in wie vielen Fällen Zugang zu den Daten gewährt wurde;

c) wie viele Anträge auf Berichtigung unrichtiger Daten und auf Löschung unrechtmäßig gespeicherter Daten dem für die Verarbeitung Verantwortlichen übermittelt wurden und in wie vielen Fällen die Daten berichtigt oder gelöscht wurden;

d) wie viele Anträge auf Berichtigung unrichtiger Daten und Löschung unrechtmäßig gespeicherter Daten der Aufsichtsbehörde übermittelt wurden;

e) wie viele Gerichtsverfahren eingeleitet wurden;

f) in wie vielen Fällen das Gericht zugunsten des Antragstellers entschieden hat;

g) Bemerkungen zu Fällen der gegenseitigen Anerkennung rechtskräftiger Entscheidungen der Gerichte oder Behörden anderer Mitgliedstaaten zu Ausschreibungen des ausschreibenden Mitgliedstaats.

Die Kommission entwickelt eine Vorlage für die Berichterstattung gemäß diesem Absatz.

(4) Die Berichte der Mitgliedstaaten werden in den gemeinsamen Bericht nach Artikel 71 Absatz 4 aufgenommen.

Artikel 69

Aufsicht über die N.SIS

(1) Die Mitgliedstaaten stellen sicher, dass die von ihnen benannten, mit den Befugnissen nach Kapitel VI der Verordnung (EU) 2016/679 oder Kapitel VI der Richtlinie (EU) 2016/680 ausgestatteten unabhängigen Aufsichtsbehörden die Rechtmäßigkeit der Verarbeitung personenbezogener Daten im SIS in ihrem Hoheitsgebiet, deren Übermittlung aus ihrem Hoheitsgebiet sowie des Austauschs und der Weiterverarbeitung von Zusatzinformationen in ihrem Hoheitsgebiet überwachen.

(2) Die Aufsichtsbehörden gewährleisten, dass die Datenverarbeitungsvorgänge in ihrem N.SIS mindestens alle vier Jahre nach internationalen Prüfungsstandards überprüft werden. Die Prüfung wird entweder von den Aufsichtsbehörden durchgeführt, oder die Aufsichtsbehörden geben die Prüfung unmittelbar bei einem unabhängigen Datenschutzprüfer in Auftrag. Der unabhängige Prüfer arbeitet jederzeit unter der Kontrolle und der Verantwortung der Aufsichtsbehörden.

(3) Die Mitgliedstaaten stellen sicher, dass die Aufsichtsbehörden über ausreichende Ressourcen zur Wahrnehmung der Aufgaben verfügen, die ihnen gemäß dieser Verordnung übertragen werden, und Zugang zur Beratung durch Personen mit ausreichendem Wissen über biometrische Daten haben.

Artikel 70

Aufsicht über eu-LISA

(1) Der Europäische Datenschutzbeauftragte ist für die Überwachung der Verarbeitung personenbezogener Daten durch eu-LISA verantwortlich und stellt sicher, dass diese Tätigkeiten im Einklang mit dieser Verordnung erfolgen. Die Aufgaben und Befugnisse nach den Artikeln 57 und 58 der Verordnung (EU) 2018/1725 finden entsprechend Anwendung.

(2) Der Europäische Datenschutzbeauftragte überprüft mindestens alle vier Jahre die Verarbeitung personenbezogener Daten durch eu-LISA nach internationalen Prüfungsstandards. Der Prüfbericht wird dem Europäischen Parlament, dem Rat, eu-LISA, der Kommission und den Aufsichtsbehörden übermittelt. eu-LISA erhält vor der Annahme des Berichts Gelegenheit zur Stellungnahme.

Artikel 71

Zusammenarbeit zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten

(1) Die Aufsichtsbehörden und der Europäische Datenschutzbeauftragte arbeiten im Rahmen ihrer jeweiligen Zuständigkeiten aktiv zusammen und gewährleisten eine koordinierte Beaufsichtigung des SIS.

(2) Im Rahmen ihrer jeweiligen Zuständigkeiten tauschen die Aufsichtsbehörden und der Europäische Datenschutzbeauftragte einschlägige Informationen aus, unterstützen sich gegenseitig bei Überprüfungen und Inspektionen, prüfen Schwierigkeiten bei der Auslegung oder Anwendung dieser Verordnung und anderer anwendbarer Unionsrechtsakte, gehen Problemen nach, die im Zuge der Wahrnehmung der unabhängigen Beaufsichtigung oder der Ausübung der Rechte betroffener Personen aufgetreten sind, arbeiten harmonisierte Vorschläge im Hinblick auf gemeinsame Lösungen für etwaige Probleme aus und fördern die Sensibilisierung für die Datenschutzrechte, soweit erforderlich.

(3) Für die Zwecke des Absatzes 2 kommen die Aufsichtsbehörden und der Europäische Datenschutzbeauftragte mindestens zweimal jährlich zu einer Sitzung im Rahmen des Europäischen Datenschutzausschusses zusammen. Die Kosten und die Ausrichtung dieser Sitzungen übernimmt der Europäische Datenschutzausschuss. In der ersten Sitzung wird eine Geschäftsordnung angenommen. Weitere Arbeitsverfahren werden je nach Bedarf gemeinsam festgelegt.

(4) Der Europäische Datenschutzausschuss übermittelt dem Europäischen Parlament, dem Rat und der Kommission jährlich einen gemeinsamen Tätigkeitsbericht über die koordinierte Aufsicht.

KAPITEL XVII

Haftung und Sanktionen

Artikel 72

Haftung

(1) Unbeschadet des Anspruchs auf Schadenersatz und jeglicher Haftungsregelung gemäß der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2018/1725.

a) hat jede Person oder jeder Mitgliedstaat, der/dem beim Betrieb des N.SIS durch eine rechtswidrige Verarbeitung personenbezogener Daten oder durch andere gegen diese Verordnung verstoßende Handlungen seitens eines Mitgliedstaats ein materieller oder immaterieller Schaden entsteht, das Recht, von diesem Mitgliedstaat Schadenersatz zu verlangen; und

b) hat jede Person oder jeder Mitgliedstaat, der/dem durch eine gegen diese Verordnung verstoßende Handlung seitens eu-LISA ein materieller oder immaterieller Schaden entsteht, das Recht, von eu-LISA Schadenersatz zu verlangen.

Ein Mitgliedstaat bzw. eu-LISA wird vollständig oder teilweise von seiner bzw. ihrer Haftung nach Unterabsatz 1 befreit, wenn er bzw. sie nachweist, dass er bzw. sie für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich ist.

(2) Verursacht eine Verletzung der in dieser Verordnung festgelegten Pflichten durch einen Mitgliedstaat einen Schaden am SIS, haftet dieser Mitgliedstaat für den entstandenen Schaden, es sei denn, eu-LISA oder ein anderer am SIS beteiligter Mitgliedstaat hat keine angemessenen Maßnahmen ergriffen, um den Schaden abzuwenden oder zu mindern.

(3) Die Geltendmachung von Schadenersatzansprüchen nach den Absätzen 1 und 2 gegen einen Mitgliedstaat unterliegt dem nationalen Recht dieses Mitgliedstaats. Die Geltendmachung von Schadenersatzansprüchen nach den Absätzen 1 und 2 gegen eu-LISA unterliegt den in den Verträgen vorgesehenen Voraussetzungen.

Artikel 73

Sanktionen

Die Mitgliedstaaten stellen sicher, dass jeder Missbrauch von SIS-Daten und jede Verarbeitung solcher Daten und jeder Austausch von Zusatzinformationen, die dieser Verordnung zuwiderlaufen, nach nationalem Recht geahndet werden kann.

Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

KAPITEL XVIII

Schlussbestimmungen

Artikel 74

Kontrolle und Statistiken

(1) eu-LISA stellt sicher, dass Verfahren vorhanden sind, mit denen der Betrieb des SIS anhand von Leistungs-, Kostenwirksamkeits-, Sicherheits- und Dienstqualitätszielen überwacht werden kann.

(2) Zum Zwecke der Wartung des Systems sowie zur Erstellung von Berichten, zur Berichterstattung über die Datenqualität und zur Ausarbeitung von Statistiken hat eu-LISA Zugang zu den erforderlichen Informationen über die Verarbeitungsvorgänge im zentralen SIS.

(3) eu-LISA erstellt tägliche, monatliche und jährliche Statistiken über die Zahl der Datensätze pro Ausschreibungskategorie, sowohl nach Mitgliedstaaten aufgeschlüsselt als auch insgesamt. Zudem erstellt eu-LISA jährliche Berichte über die Zahl der Treffer pro Ausschreibungskategorie und darüber, wie oft das SIS abgefragt und wie oft zwecks Eingabe, Aktualisierung oder Löschung einer Ausschreibung — sowohl nach Mitgliedstaaten aufgeschlüsselt als auch insgesamt — auf das System zugegriffen wurde. Die erstellten Statistiken dürfen keine personenbezogenen Daten enthalten. Der jährliche Statistikbericht wird veröffentlicht.

(4) Die Mitgliedstaaten, Europol, Eurojust und die Europäische Agentur für die Grenz- und Küstenwache stellen eu-LISA und der Kommission die Informationen zur Verfügung, die für die Erstellung der in den Absätzen 3, 6, 8 und 9 genannten Berichte erforderlich sind.

(5) Diese Informationen umfassen separate Statistiken über die Zahl der Abfragen durch die oder im Namen der Stellen, die in den Mitgliedstaaten für die Ausstellung von Kfz-Zulassungsbescheinigungen oder für die Ausstellung von Zulassungsbescheinigungen für Wasserfahrzeuge (einschließlich Wasserfahrzeugmotoren) und Luftfahrzeuge (einschließlich Flugzeugmotoren) oder deren Verkehrsmanagement sowie für die Zulassung von Schusswaffen zuständig sind. In diesen Statistiken wird auch die Zahl der Treffer pro Ausschreibungskategorie ausgewiesen.

(6) eu-LISA stellt dem Europäischen Parlament, dem Rat, den Mitgliedstaaten, der Kommission, Europol, Eurojust, der Europäischen Agentur für die Grenz- und Küstenwache sowie dem Europäischen Datenschutzbeauftragten alle von ihr erstellten Statistikberichte zur Verfügung.

Um die Umsetzung der Unionsrechtsakte, unter anderem für die Zwecke der Verordnung (EU) Nr. 1053/2013, zu überwachen, kann die Kommission eu-LISA ersuchen, regelmäßig oder ad hoc zusätzliche spezifische Statistikberichte über die Leistung des SIS, die Nutzung des SIS und den Austausch von Zusatzinformationen bereitzustellen.

Die Europäische Agentur für die Grenz- und Küstenwache kann eu-LISA ersuchen, regelmäßig oder ad hoc zusätzliche spezifische Statistikberichte zur Durchführung der in den Artikeln 11 und 13 der Verordnung (EU) 2016/1624 genannten Risikoanalysen und Schwachstellenbeurteilungen bereitzustellen.

(7) Für die Zwecke des Artikels 15 Absatz 4 und der Absätze 3, 4 und 6 des vorliegenden Artikels sorgt eu-LISA an ihren technischen Standorten für die Einrichtung, die Implementierung und das Hosting eines Zentralregisters, das die Daten nach Artikel 15 Absatz 4 und nach Absatz 3 des vorliegenden Artikels enthält, was eine Identifizierung einzelner Personen nicht ermöglicht und es der Kommission und den Agenturen nach Absatz 6 des vorliegenden Artikels gestattet, maßgeschneiderte Berichte und Statistiken zu erhalten. Auf Anfrage gewährt eu-LISA den Mitgliedstaaten und der Kommission sowie Europol, Eurojust und der Europäischen Agentur für die Grenz- und Küstenwache, soweit dies für die Erfüllung ihrer Aufgaben erforderlich ist, Zugang zum Zentralregister in Form eines gesicherten Zugangs über die Kommunikationsinfrastruktur. eu-LISA richtet Zugangskontrollen und spezifische Nutzerprofile ein, um sicherzustellen, dass auf das Zentralregister ausschließlich zu Berichterstattungs- und Statistikzwecken zugegriffen wird.

(8) Zwei Jahre nach dem Geltungsbeginn dieser Verordnung gemäß Artikel 79 Absatz 5 und danach alle zwei Jahre unterbreitet eu-LISA dem Europäischen Parlament und dem Rat einen Bericht über die technische Funktionsweise des zentralen SIS und der Kommunikationsinfrastruktur, einschließlich der ihrer Sicherheit, über das AFIS und über den bilateralen und multilateralen Austausch von Zusatzinformationen zwischen den Mitgliedstaaten. Dieser Bericht wird, sobald die entsprechende Technik eingesetzt wird, auch eine Bewertung der Nutzung von Gesichtsbildern zur Identifizierung von Personen enthalten.

(9) Drei Jahre nach dem Geltungsbeginn dieser Verordnung gemäß Artikel 79 Absatz 5 und danach alle vier Jahre nimmt die Kommission eine Gesamtbewertung des zentralen SIS und des bilateralen und multilateralen Austauschs von Zusatzinformationen zwischen den Mitgliedstaaten vor. Dabei misst sie die Ergebnisse an den Zielen, überprüft, ob die grundlegenden Prinzipien weiterhin Gültigkeit haben, bewertet die Anwendung dieser Verordnung in Bezug auf das zentrale SIS und die Sicherheit des zentralen SIS und zieht alle gebotenen Schlussfolgerungen für den künftigen Betrieb des Systems. Der Bewertungsbericht umfasst auch eine Beurteilung des AFIS und der Aufklärungskampagnen über das SIS, die gemäß Artikel 19 von der Kommission durchgeführt werden.

Die Kommission übermittelt den Bewertungsbericht dem Europäischen Parlament und dem Rat.

(10) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung detaillierter Bestimmungen über den Betrieb des Zentralregisters nach Absatz 7 dieses Artikels und die für dieses Register geltenden Datenschutz- und Sicherheitsvorschriften. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 76 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 75

Ausübung der Befugnisübertragung

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

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 38 Absatz 3 und Artikel 43 Absatz 4 wird der Kommission auf unbestimmte Zeit ab dem 27. Dezember 2018 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 38 Absatz 3 und Artikel 43 Absatz 4 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

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

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

(6) Ein delegierter Rechtsakt, der gemäß Artikel 38 Absatz 3 oder Artikel 43 Absatz 4 erlassenen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Artikel 76

Ausschussverfahren

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

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

Artikel 77

Änderung des Beschlusses 2007/533/JI

Der Beschluss 2007/533/JI wird wie folgt geändert:

1. Artikel 6 erhält folgende Fassung:

„*Artikel 6*

Nationale Systeme

(1) Jeder Mitgliedstaat ist dafür zuständig, dass sein N.SIS II errichtet, betrieben, gewartet sowie weiterentwickelt und an die NI-SIS angeschlossen wird.

(2) Jeder Mitgliedstaat ist dafür zuständig, die ununterbrochene Verfügbarkeit der SIS II-Daten für die Endnutzer zu gewährleisten.“

2. Artikel 11 erhält folgende Fassung:

„*Artikel 11*

Geheimhaltung — Mitgliedstaaten

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

(2) Arbeitet ein Mitgliedstaat bei Aufgaben im Zusammenhang mit dem SIS II mit externen Auftragnehmern zusammen, so überwacht er die Tätigkeiten des Auftragnehmers genau, um sicherzustellen, dass alle Vorschriften dieses Beschlusses, insbesondere betreffend Sicherheit, Geheimhaltung und Datenschutz, eingehalten werden.

(3) Das Betriebsmanagement des N.SIS II oder etwaiger technischer Kopien wird nicht an private Unternehmen oder private Organisationen übertragen."

3. Artikel 15 wird wie folgt geändert:

a) Folgender Absatz wird eingefügt:

„(3a) Die Verwaltungsbehörde entwickelt und pflegt einen Mechanismus und Verfahren für die Durchführung von Qualitätskontrollen der Daten in der CS-SIS. Sie erstattet den Mitgliedstaaten in diesem Zusammenhang regelmäßig Bericht.

Die Verwaltungsbehörde legt der Kommission regelmäßig Berichte über die aufgetretenen Probleme und die betroffenen Mitgliedstaaten vor.

Die Kommission legt dem Europäischen Parlament und dem Rat regelmäßig einen Bericht über die aufgetretenen Probleme im Zusammenhang mit der Datenqualität vor."

b) Absatz 8 erhält folgende Fassung:

„(8) Das Betriebsmanagement des zentralen SIS II umfasst alle Aufgaben, die erforderlich sind, um das zentrale SIS II im Einklang mit diesem Beschluss 24 Stunden pro Tag und 7 Tage die Woche betriebsbereit zu halten; dazu gehören insbesondere die für den einwandfreien Betrieb des Systems erforderlichen Wartungsarbeiten und technischen Anpassungen. Zu diesen Aufgaben gehören auch die Koordinierung, die Verwaltung und die Unterstützung von Tests des zentralen SIS II und der N.SIS II, die sicherstellen, dass das zentrale SIS II und die N.SIS II gemäß den in Artikel 9 dargelegten Anforderungen an die technische Konformität funktionieren."

4. In Artikel 17 werden die folgenden Absätze angefügt:

„(3) Arbeitet die Verwaltungsbehörde bei Aufgaben im Zusammenhang mit dem SIS II mit externen Auftragnehmern zusammen, so überwacht sie die Tätigkeiten des Auftragnehmers genau, um sicherzustellen, dass alle Vorschriften dieses Beschlusses, insbesondere jene betreffend Sicherheit, Geheimhaltung und Datenschutz, eingehalten werden.

(4) Das Betriebsmanagement der CS-SIS wird nicht an private Unternehmen oder private Organisationen übertragen."

5. In Artikel 21 wird folgender Absatz angefügt:

„Falls eine Person oder eine Sache im Rahmen einer Ausschreibung im Zusammenhang mit einer terroristischen Straftat gesucht wird, so wird davon ausgegangen, dass Angemessenheit, Relevanz und Bedeutung des Falles eine Ausschreibung im SIS II rechtfertigen. Aus Gründen der öffentlichen oder der nationalen Sicherheit können die Mitgliedstaaten ausnahmsweise von der Eingabe einer Ausschreibung absehen, wenn davon auszugehen ist, dass sie behördliche oder rechtliche Untersuchungen, Ermittlungen oder Verfahren behindert."

6. Artikel 22 erhält folgende Fassung:

„*Artikel 22*

Besondere Vorschriften für die Eingabe, Überprüfung oder die Abfrage anhand von Lichtbildern und Fingerabdrücken

(1) Lichtbilder und Fingerabdrücke werden nur nach einer speziellen Qualitätsprüfung eingegeben, mit der überprüft wird, ob sie Mindestqualitätsstandards einhalten. Die Bestimmungen über die spezielle Qualitätsprüfung werden gemäß dem in Artikel 67 vorgesehenen Verfahren festgelegt.

(2) Wenn Lichtbilder und Fingerabdruckdaten in einer Ausschreibung im SIS II verfügbar sind, sind diese Lichtbilder und Fingerabdruckdaten zu nutzen, um die Identität einer Person zu bestätigen, die durch eine alphanumerische Abfrage im SIS II aufgefunden wurde.

(3) Fingerabdruckdaten können in allen Fällen abgefragt werden, um eine Person zu identifizieren. Fingerabdruckdaten sind abzufragen, um eine Person zu identifizieren, wenn die Identität der Person nicht durch andere Mittel festgestellt werden kann. Zu diesem Zweck enthält das zentrale SIS II ein automatisiertes Fingerabdruck-Identifizierungssystem (AFIS).

(4) Fingerabduckdaten im SIS II im Zusammenhang mit gemäß den Artikeln 26, 32 und 36 eingegebenen können auch anhand vollständiger oder unvollständiger Fingerabdrucksätze abgefragt werden, die an untersuchten Tatorten schwerer oder terroristischer Straftaten vorgefunden wurden, diese Abdrücke mit hoher Wahrscheinlichkeit einem Täter zuzuordnen sind und die Abfrage gleichzeitig in den einschlägigen nationalen Fingerabdruck-Datenbanken des Mitgliedstaats durchgeführt wird."

7. Artikel 41 erhält folgende Fassung:

„*Artikel 41*

Zugriff von Europol auf Daten im SIS II

(1) Die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol), die durch die Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates (*) errichtet wurde, hat, soweit dies zur Erfüllung ihres Mandats notwendig ist, das Recht, auf Daten im SIS II zuzugreifen und diese abzufragen. Europol kann Zusatzinformationen im Einklang mit den Bestimmungen des SIRENE-Handbuchs austauschen und zusätzlich anfragen.

(2) Stellt sich bei einer Abfrage durch Europol heraus, dass eine Ausschreibung im SIS II gespeichert ist, setzt Europol den ausschreibenden Mitgliedstaat im Wege des Austauschs von Zusatzinformationen mithilfe der Kommunikationsinfrastruktur und gemäß den Bestimmungen des SIRENE-Handbuchs davon in Kenntnis. Bis Europol in der Lage ist, die für den Austausch von Zusatzinformationen vorgesehenen Funktionen zu verwenden, setzt es den ausschreibenden Mitgliedstaat über die in der Verordnung (EU) 2016/794 bestimmten Kanäle davon in Kenntnis.

(3) Europol kann die von den Mitgliedstaaten übermittelten Zusatzinformationen für die Zwecke ihres Abgleichs mit Europols Datenbanken und Projekten der operativen Analysen im Hinblick auf die Ermittlung etwaiger Zusammenhänge oder anderer relevanter Verbindungen sowie für die in Artikel 18 Absatz 2 Buchstaben a, b und c der Verordnung (EU) 2016/794 genannten strategischen, thematischen oder operativen Analysen verarbeiten. Jegliche Verarbeitung von Zusatzinformationen durch Europol für die Zwecke dieses Artikels erfolgt im Einklang mit jener Verordnung.

(4) Die Nutzung der durch eine Abfrage im SIS II oder durch die Verarbeitung von Zusatzinformationen gewonnenen Informationen durch Europol unterliegt der Zustimmung des ausschreibenden Mitgliedstaats. Gestattet der Mitgliedstaat die Nutzung derartiger Informationen, so erfolgt deren Verarbeitung durch Europol nach Maßgabe der Verordnung (EU) 2016/794. Europol gibt derartige Informationen nur mit Zustimmung des ausschreibenden Mitgliedstaats und unter uneingeschränkter Wahrung der Vorschriften des Unionsrechts zum Datenschutz an Drittländer und -stellen weiter.

(5) Europol

a) unterlässt es unbeschadet der Absätze 4 und 6, Teile des SIS II, zu denen sie Zugang hat, oder die hierin gespeicherten Daten, auf die sie Zugriff hat, mit einem von oder bei Europol betriebenen System für die Datenerhebung und -verarbeitung zu verbinden bzw. in ein solches zu übernehmen oder einen bestimmten Teil des SIS II herunterzuladen oder in anderer Weise zu vervielfältigen;

b) löscht ungeachtet des Artikels 31 Absatz 1 der Verordnung (EU) 2016/794 Zusatzinformationen, die personenbezogene Daten enthalten, spätestens ein Jahr nach der Löschung der entsprechenden Ausschreibung. Abweichend hiervon darf Europol, sofern Europol in ihren Datenbanken oder Projekten für die operationelle Analyse über Informationen zu einem Fall verfügt, der mit den Zusatzinformationen in Verbindung steht, ausnahmsweise die Zusatzinformationen über diese Frist hinaus speichern, sofern dies zur Erfüllung ihrer Aufgaben erforderlich ist. Erforderlichenfalls unterrichtet Europol den ausschreibenden und den vollziehenden Mitgliedstaat über die weitere Speicherung derartiger Zusatzinformationen und legt eine Begründung dafür vor;

c) beschränkt den Zugriff auf die Daten im SIS II, einschließlich der Zusatzinformationen, auf die eigens dazu ermächtigten Bediensteten von Europol, die diese Daten für die Erfüllung ihrer Aufgaben benötigen;

d) legt Maßnahmen zur Gewährleistung der Sicherheit, der Geheimhaltung und der Eigenkontrolle gemäß den Artikeln 10, 11 und 13 fest und wendet sie an;

e) stellt sicher, dass das zur Verarbeitung von SIS II-Daten ermächtigte Personal eine angemessene Schulung und Unterrichtung nach Artikel 14 erhält; und

f) gestattet dem Europäischen Datenschutzbeauftragten unbeschadet der Verordnung (EU) 2016/794, die Tätigkeiten Europols bei der Ausübung ihres Rechts auf Zugriff auf die Daten im SIS II und deren Abfrage sowie beim Austausch und bei der Verarbeitung von Zusatzinformationen zu überwachen und zu überprüfen.

(6) Europol darf Daten aus dem SIS II nur zu technischen Zwecken vervielfältigen, wenn dies zur direkten Abfrage durch die ordnungsgemäß ermächtigten Europol-Bediensteten erforderlich ist. Auf solche Vervielfältigungen findet dieser Beschluss Anwendung. Die technische Kopie wird nur für die Zwecke der Speicherung von SIS II-Daten verwendet, während diese Daten abgefragt werden. Sobald die Daten abgefragt wurden, werden sie gelöscht. Diese Verwendungen sind nicht als rechtswidriges Herunterladen oder Vervielfältigen von SIS II-Daten anzusehen. Europol darf Ausschreibungsdaten oder ergänzende Daten, die von Mitgliedstaaten oder der CS-SIS II übermittelt wurden, nicht in andere Europol-Systeme kopieren.

(7) Für die Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenkontrolle und der Sicherstellung der angemessenen Sicherheit und Integrität der Daten führt Europol gemäß den Bestimmungen des Artikels 12 über jeden Zugriff auf das SIS II und jede Abfrage im SIS II Protokolle. Diese Protokolle und Dokumentationen sind nicht als rechtswidriges Herunterladen oder Vervielfältigen eines Teils des SIS II anzusehen.

(8) Die Mitgliedstaaten unterrichten Europol im Wege des Austauschs von Zusatzinformationen über jeden Treffer zu Ausschreibungen im Zusammenhang mit terroristischen Straftaten. Die Mitgliedstaaten können ausnahmsweise davon absehen, Europol zu unterrichten, wenn dies laufende Ermittlungen oder die Sicherheit einer Person gefährden oder wesentlichen Interessen der Sicherheit des ausschreibenden Mitgliedstaats zuwiderlaufen würde.

(9) Absatz 8 gilt ab dem Zeitpunkt, zu dem Europol Zusatzinformationen gemäß Absatz 1 erhalten kann.

(*) 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).“

8. Folgender Artikel wird eingefügt:

„*Artikel 42a*

Zugriff von Mitgliedern der europäischen Grenz- und Küstenwacheteams, der Teams von mit rückkehrbezogenen Aufgaben betrautem Personal sowie der Teams zur Unterstützung der Migrationssteuerung auf Daten im SIS II

(1) Gemäß Artikel 40 Absatz 8 der Verordnung (EU) 2016/1624 des Europäischen Parlaments und des Rates (*) haben Mitglieder der Teams gemäß Artikel 2 Nummern 8 und 9 jener Verordnung im Rahmen ihres Mandats und insoweit dies zur Erfüllung ihrer Aufgaben erforderlich und im Einsatzplan für einen spezifischen Einsatz vorgesehen ist, das Recht auf Zugriff auf die in das Daten im SIS II und deren Abfrage, sofern sie zur Durchführung der Kontrollen gemäß Artikel 40 Absatz 1 dieses Beschlusses ermächtigt sind und die in Artikel 14 dieses Beschlusses vorgeschriebene Schulung absolviert haben. Der Zugriff auf die Daten im SIS II darf keinem anderen Teammitglied übertragen werden.

(2) Die Mitglieder der in Absatz 1 genannten Teams üben ihr Recht auf Zugriff auf die Daten im SIS II und deren Abfrage gemäß Absatz 1 unter Verwendung einer technischen Schnittstelle aus. Die technische Schnittstelle wird die von der Europäischen Agentur für die Grenz- und Küstenwache eingerichtet und gewartet und ermöglicht eine direkte Verbindung mit dem zentralen SIS II.

(3) Stellt sich bei der Abfrage durch ein Mitglied der Teams gemäß Absatz 1 dieses Artikels heraus, dass eine Ausschreibung im SIS II vorliegt, wird der ausschreibende Mitgliedstaat hiervon unterrichtet. Nach Artikel 40 der Verordnung (EU) 2016/1624 handeln die Mitglieder der Teams in Reaktion auf eine Ausschreibung im SIS II nur auf Anweisung und grundsätzlich nur in Gegenwart von Grenzschutzbeamten oder mit rückkehrbezogenen Aufgaben betrautem Personal des Einsatzmitgliedstaats, in dem sie tätig sind. Der Einsatzmitgliedstaat kann Teammitglieder ermächtigen, in seinem Namen zu handeln.

(4) Für die Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenkontrolle und der Sicherstellung der angemessenen Sicherheit und Integrität der Daten führt die Europäische Agentur für die Grenz- und Küstenwache gemäß den Bestimmungen des Artikels 12 über jeden Zugriff auf das SIS II und jede Abfrage im SIS II Protokolle.

(5) Die Europäische Agentur für die Grenz- und Küstenwache legt Maßnahmen zur Gewährleistung der Sicherheit, der Geheimhaltung und der Eigenkontrolle gemäß den Artikeln 10, 11 und 13 fest, wendet sie an und sorgt dafür, dass die in Absatz 1 dieses Artikels genannten Teams diese Maßnahmen anwenden.

(6) Dieser Artikel ist nicht so auszulegen, dass er sich auf die Bestimmungen der Verordnung (EU) 2016/1624 betreffend den Datenschutz oder die Haftung der Europäischen Agentur für die Grenz- und Küstenwache wegen unbefugter oder unrichtiger Datenverarbeitung durch diese auswirkt.

(7) Unbeschadet des Absatzes 2 dürfen weder Teile des SIS II mit einem der Erhebung und Verarbeitung von Daten dienenden System verbunden werden, das von den in Absatz 1 genannten Teams oder bei der Europäischen Agentur für die Grenz- und Küstenwache betrieben wird, noch dürfen die Daten im SIS II, auf die diese Teams Zugriff haben, an ein solches System übermittelt werden. Kein Teil des SIS II darf heruntergeladen oder kopiert werden. Die Protokollierung von Zugriffen und Abfragen ist nicht als Herunterladen oder Vervielfältigen von SIS II-Daten anzusehen.

(8) Die Europäische Agentur für die Grenz- und Küstenwache gestattet dem Europäischen Datenschutzbeauftragten, die Tätigkeiten der Teams gemäß diesem Artikel bei der Ausübung ihres Rechts auf Zugriff auf die Daten im SIS II und deren Abfrage zu überwachen und zu überprüfen. Dies gilt unbeschadet weiterer Bestimmungen der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates (**).

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

(**) 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).“

Artikel 78

Aufhebung

Die Verordnung (EG) Nr. 1986/2006 und die Beschlüsse 2007/533/JI und 2010/261/EU werden mit Wirkung ab dem in Artikel 79 Absatz 5 Unterabsatz 1 angegebenen Tag des Beginns der Anwendung der vorliegenden Verordnung aufgehoben.

Bezugnahmen auf die aufgehobene Verordnung (EG) Nr. 1986/2006 und den Beschluss 2007/533/JI gelten als Bezugnahmen auf die vorliegende Verordnung und sind nach Maßgabe der Entsprechungstabellen im Anhang zu lesen.

Artikel 79

Inkrafttreten, Inbetriebnahme und Anwendung

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

(2) Die Kommission erlässt spätestens am 28. Dezember 2021 einen Beschluss zur Festlegung des Datums der Inbetriebnahme des SIS gemäß dieser Verordnung, nachdem sie sich davon überzeugt hat, dass die folgenden Voraussetzungen erfüllt wurden:

a) Die für die Anwendung dieser Verordnung erforderlichen Durchführungsmaßnahmen wurden erlassen;

b) die Mitgliedstaaten haben der Kommission mitgeteilt, dass sie die erforderlichen technischen und rechtlichen Vorkehrungen zur Verarbeitung von SIS-Daten und zum Austausch von Zusatzinformationen gemäß dieser Verordnung getroffen haben, und

c) eu-LISA hat der Kommission mitgeteilt, dass sämtliche Tests im Hinblick auf die CS-SIS und die Interaktion zwischen N.SIS und CS-SIS erfolgreich abgeschlossen sind.

(3) Die Kommission überwacht aufmerksam die Fortschritte bei der schrittweisen Erfüllung der Voraussetzungen nach Absatz 2 und unterrichtet das Europäische Parlament und den Rat über die Ergebnisse der Überprüfung nach jenem Absatz.

(4) Die Kommission legt dem Europäischen Parlament und dem Rat bis zum 28. Dezember 2019 und danach jedes Jahr, bis der Beschluss der Kommission nach Absatz 2 erfolgt ist, einen Bericht über den Stand der Vorbereitungen für die vollumfängliche Durchführung dieser Verordnung vor. Dieser Bericht enthält auch genaue Angaben über die angefallenen Kosten und Informationen über sämtliche Risiken, die Auswirkungen auf die Gesamtkosten haben könnten.

(5) Diese Verordnung gilt ab dem gemäß Absatz 2 festgelegten Datum.

Abweichend von Unterabsatz 1

a) gelten Artikel 4 Absatz 4, Artikel 5, Artikel 8 Absatz 4, Artikel 9 Absätze 1 und 5, Artikel 12 Absatz 8, Artikel 15 Absatz 7, Artikel 19, Artikel 20 Absätze 4 und 5, Artikel 26 Absatz 6, Artikel 32 Absatz 9, Artikel 34 Absatz 3, Artikel 36 Absatz 6, Artikel 38 Absätze 3 und 4, Artikel 42 Absatz 5, Artikel 43 Absatz 4, Artikel 54 Absatz 5, Artikel 62 Absatz 4, Artikel 63 Absatz 6, Artikel 74 Absätze 7 und 10, Artikel 75, Artikel 76, Artikel 77 Nummern 1 bis 5 sowie die Absätze 3 und 4 des vorliegenden Artikels ab dem Tag des Inkrafttretens dieser Verordnung;

b) gilt Artikel 77 Nummern 7 und 8 ab dem 28. Dezember 2019;

c) gilt Artikel 77 Nummer 6 ab dem 28. Dezember 2020.

(6) Der Beschluss der Kommission gemäß Absatz 2 wird im *Amtsblatt der Europäischen Union* veröffentlicht.

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

Geschehen zu Brüssel am 28. November 2018.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Die Präsidentin*
A. TAJANI	K. EDTSTADLER

ANHANG

ENTSPRECHUNGSTABELLE

Beschluss 2007/533/JI	Vorliegende Verordnung
Artikel 1	Artikel 1
Artikel 2	Artikel 2
Artikel 3	Artikel 3
Artikel 4	Artikel 4
Artikel 5	Artikel 5
Artikel 6	Artikel 6
Artikel 7	Artikel 7
Artikel 8	Artikel 8
Artikel 9	Artikel 9
Artikel 10	Artikel 10
Artikel 11	Artikel 11
Artikel 12	Artikel 12
Artikel 13	Artikel 13
Artikel 14	Artikel 14
Artikel 15	Artikel 15
Artikel 16	Artikel 16
Artikel 17	Artikel 17
Artikel 18	Artikel 18
Artikel 19	Artikel 19
Artikel 20	Artikel 20
Artikel 21	Artikel 21
Artikel 22	Artikel 42 und 43
Artikel 23	Artikel 22
—	Artikel 23
Artikel 24	Artikel 24
Artikel 25	Artikel 25
Artikel 26	Artikel 26
Artikel 27	Artikel 27
Artikel 28	Artikel 28
Artikel 29	Artikel 29
Artikel 30	Artikel 30
Artikel 31	Artikel 31
Artikel 32	Artikel 32
Artikel 33	Artikel 33
Artikel 34	Artikel 34
Artikel 35	Artikel 35
Artikel 36	Artikel 36
Artikel 37	Artikel 37
Artikel 38	Artikel 38
Artikel 39	Artikel 39
—	Artikel 40
—	Artikel 41

Beschluss 2007/533/JI	Vorliegende Verordnung
Artikel 40	Artikel 44
—	Artikel 45
—	Artikel 46
—	Artikel 47
Artikel 41	Artikel 48
Artikel 42	Artikel 49
—	Artikel 51
Artikel 42a	Artikel 50
Artikel 43	Artikel 52
Artikel 44	Artikel 53
Artikel 45	Artikel 54
—	Artikel 55
Artikel 46	Artikel 56
Artikel 47	Artikel 57
Artikel 48	Artikel 58
Artikel 49	Artikel 59
—	Artikel 60
Artikel 50	Artikel 61
Artikel 51	Artikel 62
Artikel 52	Artikel 63
Artikel 53	Artikel 64
Artikel 54	Artikel 65
Artikel 55	—
Artikel 56	—
Artikel 57	Artikel 66
Artikel 58	Artikel 67
Artikel 59	Artikel 68
Artikel 60	Artikel 69
Artikel 61	Artikel 70
Artikel 62	Artikel 71
Artikel 63	—
Artikel 64	Artikel 72
Artikel 65	Artikel 73
Artikel 66	Artikel 74
—	Artikel 75
Artikel 67	Artikel 76
Artikel 68	—
—	Artikel 77
Artikel 69	—
—	Artikel 78
Artikel 70	—
Artikel 71	Artikel 79

Verordnung (EG) Nr. 1986/2006	Vorliegende Verordnung
Artikel 1, 2 und 3	Artikel 45