

Brüssel, den 21.12.2016  
COM(2016) 883 final

2016/0409 (COD)

Vorschlag für eine

**VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES**

**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 der Verordnung (EU) Nr. 515/2014 und zur Aufhebung der Verordnung (EG) Nr. 1986/2006, des Beschlusses 2007/533/JI des Rates und des Beschlusses 2010/261/EU der Kommission**

## **BEGRÜNDUNG**

### **1. KONTEXT DES VORSCHLAGS**

#### **• Gründe und Ziele des Vorschlags**

In den vergangenen zwei Jahren hat die Europäische Union daran gearbeitet, den separaten Herausforderungen der Migrationssteuerung, des integrierten Grenzmanagements an den EU-Außengrenzen sowie der Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität gleichzeitig zu begegnen. Der wirksame Informationsaustausch zwischen den Mitgliedstaaten sowie zwischen Mitgliedstaaten und den einschlägigen EU-Agenturen ist unerlässlich, um auf diese Herausforderungen entschlossen zu reagieren und eine wirksame und echte Sicherheitsunion aufzubauen.

Das Schengener Informationssystem (SIS) ist das erfolgreichste Instrument zur wirksamen Zusammenarbeit zwischen Einwanderungs-, Polizei-, Zoll- und Justizbehörden in der EU und den assoziierten Schengen-Ländern. Die zuständigen Behörden der Mitgliedstaaten, etwa Polizei, Grenzschutz und Zoll, müssen auf hochwertige Informationen über die von ihnen kontrollierten Personen oder Gegenstände zugreifen können und eindeutige Anweisungen dazu erhalten, wie in dem jeweiligen Fall vorzugehen ist. Dieses IT-Großsystem ist das Kernstück der Schengener Zusammenarbeit und spielt eine entscheidende Rolle bei der Erleichterung der Freizügigkeit im Schengen-Raum. Es ermöglicht zuständigen Behörden die Eingabe und Abfrage von Daten über gesuchte Personen, Personen, die unter Umständen nicht berechtigt sind, in die EU einzureisen oder sich dort aufzuhalten, vermisste Personen – insbesondere Kinder – und Gegenstände, die möglicherweise gestohlen oder unterschlagen wurden bzw. abhandengekommen sind. Neben Informationen über eine bestimmte Person oder einen bestimmten Gegenstand erhalten die zuständigen Behörden über das SIS auch eindeutige Anweisungen dazu, was zu tun ist, wenn sie die betreffende Person oder den betreffenden Gegenstand gefunden haben.

Im Jahr 2016, drei Jahre nach Inbetriebnahme des SIS der zweiten Generation, führte die Kommission eine umfassende Bewertung<sup>1</sup> des Systems durch. Diese Bewertung zeigte, dass das SIS in operativer Hinsicht ein großer Erfolg ist. Im Jahr 2015 kontrollierten zuständige nationale Behörden bei fast 2,9 Milliarden Gelegenheiten Personen und Gegenstände anhand der im SIS erfassten Daten und tauschten über 1,8 Millionen Zusatzinformationen aus. Dennoch sollten Wirksamkeit und Effizienz des Systems, wie im Arbeitsprogramm der Kommission für das Jahr 2017 angekündigt, auf dieser positiven Erfahrung aufbauend weiter gestärkt werden. Zu diesem Zweck legt die Kommission infolge der Bewertung ein erstes Bündel von drei Vorschlägen zur Verbesserung und Ausweitung der Nutzung des SIS vor; gleichzeitig setzt sie ihre Arbeit fort, um die Interoperabilität bestehender und künftiger Gefahrenabwehr-, Strafverfolgungs- und Grenzmanagementsysteme zu erhöhen, und knüpft damit an die laufende Arbeit der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität an.

Diese Vorschläge beziehen sich auf die Nutzung des Systems für a) das Grenzmanagement, b) die polizeiliche Zusammenarbeit und die justizielle Zusammenarbeit in Strafsachen und c) die

---

<sup>1</sup> Bericht an das Europäische Parlament und den Rat 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 und dazugehörige Arbeitsunterlage der Kommissionsdienststellen (ABl. ...).

Rückkehr/Rückführung illegal aufhältiger Drittstaatsangehöriger. Die ersten beiden Vorschläge bilden zusammen die Rechtsgrundlagen für die Einrichtung, den Betrieb und die Nutzung des SIS. Der Vorschlag über die Nutzung des SIS für die Rückkehr illegal aufhältiger Drittstaatsangehöriger ergänzt den Vorschlag für das Grenzmanagement und die darin enthaltenen Bestimmungen. Mit ihm wird eine neue Ausschreibungskategorie eingeführt, und er trägt zur Durchführung und Überwachung der Richtlinie 2008/115/EG<sup>2</sup> bei.

Aufgrund der variablen Geometrie der Beteiligung der Mitgliedstaaten an der EU-Politik im Raum der Freiheit, der Sicherheit und des Rechts ist es notwendig, drei separate Rechtsakte zu erlassen, die jedoch reibungslos zusammenwirken, um den umfassenden Betrieb und die umfassende Nutzung des Systems zu ermöglichen.

In der Absicht, das Informationsmanagement auf EU-Ebene zu stärken und zu verbessern, begann die Kommission im April 2016 zeitgleich mit einem Reflexionsprozess zum Thema „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“<sup>3</sup>. Übergreifendes Ziel ist es zu gewährleisten, dass die zuständigen Behörden systematisch alle notwendigen Informationen aus den unterschiedlichen ihnen zur Verfügung stehenden Informationssystemen erhalten. Zur Erreichung dieses Ziels hat die Kommission die vorhandene Informationsarchitektur überprüft, um Informationslücken und Schwachpunkte zu ermitteln, die auf Mängeln bei den Funktionen der vorhandenen Systeme und auf der Zersplitterung der EU-Gesamtarchitektur für Datenmanagement beruhen. Um diese Arbeit zu unterstützen, richtete die Kommission eine hochrangige Expertengruppe für Informationssysteme und Interoperabilität ein, deren vorläufige Erkenntnisse in Bezug auf die Datenqualität in diese ersten drei Vorschläge eingeflossen sind.<sup>4</sup> In seiner Rede zur Lage der Union vom September 2016 wies Präsident Juncker darauf hin, wie wichtig es ist, die derzeitigen Mängel der Informationssysteme zu beseitigen und die Interoperabilität und Vernetzung der bestehenden Informationssysteme zu verbessern.

Ausgehend von den Erkenntnissen der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität, die im ersten Halbjahr 2017 vorgestellt werden, wird die Kommission Mitte 2017 prüfen, ob ein zweites Bündel von Vorschlägen notwendig ist, um die Interoperabilität des SIS mit anderen IT-Systemen zu verbessern. Die Überprüfung der Verordnung (EU) Nr. 1077/2011<sup>5</sup> zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) ist auch ein wichtiges Element dieser Arbeit und wird wahrscheinlich Gegenstand separater Vorschläge der Kommission sein, die ebenfalls 2017 vorgelegt werden. Wichtige Aspekte bei der Bewältigung der gegenwärtigen Herausforderungen im Bereich der Sicherheit sind die Investition in einen schnellen und wirksamen Austausch qualitativ hochwertiger Informationen und die Gewährleistung der Interoperabilität der EU-Datenbanken und Informationssysteme.

---

<sup>2</sup> Richtlinie 2008/115/EG des Europäischen Parlaments und des Rates vom 16. Dezember 2008 über gemeinsame Normen und Verfahren in den Mitgliedstaaten zur Rückführung illegal aufhältiger Drittstaatsangehöriger (ABl. L 348 vom 24.12.2008, S. 98).

<sup>3</sup> COM(2016) 205 final vom 6.4.2016.

<sup>4</sup> Beschluss 2016/C 257/03 der Kommission vom 17.6.2016.

<sup>5</sup> Verordnung (EU) Nr. 1077/2011 des Europäischen Parlaments und des Rates vom 25. Oktober 2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (ABl. L 286 vom 1.11.2011, S. 1).

Dieser Vorschlag ist Teil einer ersten Reihe von Vorschlägen<sup>6</sup> zur Verbesserung der Funktionsweise, des Betriebs und der Nutzung des SIS im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen. Durch den Vorschlag wird Folgendes umgesetzt:

- (1) die Ankündigung der Kommission, den Mehrwert des SIS zu Gefahrenabwehr- und Strafverfolgungszwecken<sup>7</sup> im Hinblick auf die Reaktion auf neue Bedrohungen zu verbessern;
- (2) die Konsolidierung der Ergebnisse der Arbeit der vergangenen drei Jahre zur Umsetzung des SIS, wozu technische Änderungen am zentralen SIS gehören, um einige der bestehenden Ausschreibungskategorien zu erweitern und neue Funktionen bereitzustellen;
- (3) Empfehlungen für technische und verfahrensorientierte Änderungen, die aus der umfassenden Bewertung des SIS<sup>8</sup> abgeleitet werden;
- (4) Ersuchen von SIS-Endnutzern um technische Verbesserungen und
- (5) die vorläufigen Erkenntnisse der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität<sup>9</sup> in Bezug auf die Datenqualität.

Da dieser Vorschlag in direktem Zusammenhang mit dem Vorschlag der Kommission für eine Verordnung über die Einrichtung, den Betrieb und die Nutzung des SIS im Bereich der Grenzkontrollen steht, gelten eine Reihe von Bestimmungen für beide Texte. Dazu zählen Maßnahmen über die „End-to-End“-Nutzung des SIS, wozu sowohl der Betrieb des zentralen Systems und der nationalen Systeme als auch die Bedürfnisse der Endnutzer, verbesserte Maßnahmen im Hinblick auf die Betriebskontinuität, Maßnahmen bezüglich Datenqualität, Datenschutz und Datensicherheit sowie Bestimmungen über Überwachungs-, Bewertungs- und Berichterstattungsmodalitäten gehören. Beide Vorschläge sehen zudem die umfassendere Nutzung biometrischer Daten vor.<sup>10</sup>

Hinsichtlich seiner Anwendung zum Zwecke der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen stützt sich der geltende Rechtsrahmen des SIS der zweiten Generation auf einen Rechtsakt der ehemaligen dritten Säule, den Beschluss 2007/533/JI des Rates<sup>11</sup>, sowie auf einen Rechtsakt der ehemaligen ersten Säule, die Verordnung (EG) Nr. 1986/2006<sup>12</sup>. Mit diesem Vorschlag wird der Inhalt der bestehenden Rechtsakte konsolidiert; gleichzeitig werden neue Bestimmungen hinzugefügt, um:

---

<sup>6</sup> Verordnung (EU) 2018/xxx [Grenzkontrollen] und Verordnung (EU) 2018/xxx [Rückkehr illegal aufhältiger Drittstaatsangehöriger].

<sup>7</sup> Siehe die Mitteilung der Kommission zur „Umsetzung der Europäischen Sicherheitsagenda im Hinblick auf die Bekämpfung des Terrorismus und die Weichenstellung für eine echte und wirksame Sicherheitsunion“, S. 4f., COM(2016) 230 final vom 20.4.2016.

<sup>8</sup> Bericht an das Europäische Parlament und den Rat 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 und dazugehörige Arbeitsunterlage der Kommissionsdienststellen (ABl. ...).

<sup>9</sup> Hochrangige Expertengruppe – Bericht des Vorsitzenden vom 21. Dezember 2016.

<sup>10</sup> Siehe Abschnitt 5 „Weitere Angaben“ wegen ausführlicher Erläuterungen zu den in diesen Vorschlag aufgenommenen Änderungen.

<sup>11</sup> 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).

<sup>12</sup> 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

- die nationalen Verfahren für die Nutzung des SIS besser zu harmonisieren, insbesondere im Hinblick auf Straftaten mit Terrorismusbezug sowie die Entführung von Kindern durch ein Elternteil;
- den Anwendungsbereich des SIS durch Einführung neuer Elemente von biometrischen Identifikatoren neben den bestehenden Ausschreibungen zu erweitern;
- technische Änderungen zur Verbesserung der Sicherheit und zur Reduzierung des Verwaltungsaufwands einzuführen, indem nationale Kopien vorgeschrieben und gemeinsame technische Durchführungsstandards festgelegt werden;
- zur vollständigen End-to-End-Nutzung des SIS beizutragen, wozu nicht nur das zentrale System und die nationalen Systeme gehören; zudem ist nämlich zu gewährleisten, dass die Endnutzer alle zur Ausübung ihrer Aufgaben notwendigen Daten erhalten und bei der Verarbeitung von SIS-Daten alle Sicherheitsvorschriften einhalten.

• **Kohärenz mit der Politik der Union in anderen Bereichen sowie mit bestehenden und künftigen Rechtsinstrumenten**

Dieser Vorschlag ist mit anderen Bereichen der Unionspolitik eng verbunden und ergänzt diese, und zwar:

- (6) die **innere Sicherheit**, wie sie in der Europäischen Sicherheitsagenda<sup>13</sup> und den Maßnahmen der Kommission zur Schaffung einer wirksamen und echten Sicherheitsunion<sup>14</sup> hervorgehoben wird, um terroristische und andere schwere Straftaten zu verhüten, aufzudecken, zu ermitteln und zu verfolgen, indem Strafverfolgungsbehörden ermöglicht wird, personenbezogene Daten von Personen, die unter dem Verdacht stehen, an terroristischen Handlungen oder schweren Straftaten beteiligt zu sein, zu verarbeiten;
- (7) den **Datenschutz** insofern, als dieser Vorschlag den Schutz der Grundrechte von Personen gewährleistet, deren personenbezogene Daten im SIS verarbeitet werden.

Dieser Vorschlag ist zudem mit bestehenden Rechtsvorschriften der Union eng verbunden und ergänzt diese:

- (8) Die **Europäische Grenz- und Küstenwache** ist berechtigt, für die Zwecke des vorgeschlagenen Europäischen Reiseinformations- und -genehmigungssystems (ETIAS)<sup>15</sup> auf das SIS zuzugreifen; ebenso haben die europäischen Grenz- und Küstenwacheteams, die Teams von mit rückkehrbezogenen Aufgaben betrautem Personal und die Mitglieder der Teams zur Unterstützung des Migrationsmanagements im Rahmen ihres Auftrags das Recht, über eine technische Schnittstelle für den SIS-Zugang auf die in das SIS eingegebenen Daten zuzugreifen und diese abzufragen.
- (9) **Europol**, insofern als dieser Vorschlag Europol mit zusätzlichen Rechten für den Zugriff auf die in das SIS eingegebenen Daten und die Abfrage dieser Daten im Rahmen des Europol-Mandats ausstattet.

---

Dienststellen der Mitgliedstaaten zum Schengener Informationssystem der zweiten Generation (SIS II) (ABl. L 381 vom 28.12.2006, S. 1).

<sup>13</sup> COM(2015) 185 final.

<sup>14</sup> COM(2016) 230 final.

<sup>15</sup> COM(2016) 731 final.

- (10) **Prüm**, insofern als die in diesem Vorschlag vorgesehenen Entwicklungen, die die Identifizierung von Personen auf der Grundlage von Fingerabdrücken (sowie von Gesichtsbildern und DNA-Profilen) ermöglichen, die geltenden Prümer Bestimmungen<sup>16</sup> über den grenzüberschreitenden Online-Zugriff auf die benannten nationalen DNA-Datenbanken und automatisierte daktyloskopische Identifizierungssysteme ergänzen.

Dieser Vorschlag ist zudem mit den künftigen Rechtsvorschriften der Union eng verbunden und ergänzt diese:

- (11) **Grenzschutz an den Außengrenzen:** Der Vorschlag ergänzt das geplante neue Prinzip im Schengener Grenzkodex, wonach alle Reisenden, einschließlich der Unionsbürger, bei der Einreise in den und der Ausreise aus dem Schengen-Raum systematischen Kontrollen anhand der einschlägigen Datenbanken unterzogen werden; dieses Prinzip ist eine Reaktion auf das Phänomen ausländischer terroristischer Kämpfer.
- (12) **Einreise-/Ausreisensystem:** In dem Vorschlag wird die vorgeschlagene Nutzung einer Kombination aus Fingerabdruck und Gesichtsbild als biometrische Identifikatoren für den Betrieb des Einreise-/Ausreisensystems (EES) berücksichtigt.
- (13) **ETIAS:** Der Vorschlag trägt dem vorgeschlagenen System ETIAS Rechnung, das eine umfassende Sicherheitsbeurteilung vorsieht, einschließlich einer Überprüfung von Drittstaatsangehörigen im SIS, die in die EU einreisen möchten.

## 2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄSSIGKEIT

### • Rechtsgrundlage

Dieser Vorschlag sieht Artikel 82 Absatz 1 Buchstabe d, Artikel 85 Absatz 1, Artikel 87 Absatz 2 Buchstabe a und Artikel 88 Absatz 2 Buchstabe a des Vertrags über die Arbeitsweise der Europäischen Union als Rechtsgrundlagen für die Bestimmungen über die polizeiliche Zusammenarbeit und die justizielle Zusammenarbeit in Strafsachen vor.

### • Unterschiede im Geltungsbereich

Dieser Vorschlag stützt sich auf die Bestimmungen des Schengen-Besitzstands in Bezug auf die polizeiliche Zusammenarbeit und die justizielle Zusammenarbeit in Strafsachen. In diesem Bereich gibt es verschiedene Protokolle und Assoziierungsabkommen mit folgender Wirkung:

Dänemark: Nach Artikel 4 des den Verträgen beigefügten Protokolls Nr. 22 über die Position Dänemarks entscheidet Dänemark innerhalb von sechs Monaten, nachdem der Rat diese Verordnung beschlossen hat, ob es diese auf dem Schengen-Besitzstand aufbauende Verordnung in nationales Recht umsetzen wird.

Vereinigtes Königreich: Im Einklang mit Artikel 5 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls

---

<sup>16</sup> Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6.8.2008, S. 1) und 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).

zur Einbeziehung des Schengen-Besitzstands in den Rahmen der Europäischen Union sowie Artikel 8 Absatz 2 des Beschlusses 2000/365/EG des Rates vom 29. Mai 2000 zum Antrag des Vereinigten Königreichs Großbritannien und Nordirland, einzelne Bestimmungen des Schengen-Besitzstands auf es anzuwenden<sup>17</sup>, ist das Vereinigte Königreich durch diese Verordnung gebunden.

Irland: Im Einklang mit Artikel 5 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls zur Einbeziehung des Schengen-Besitzstands in den Rahmen der Europäischen Union sowie Artikel 6 Absatz 2 des Beschlusses 2002/192/EG des Rates vom 28. Februar 2002 zum Antrag Irlands auf Anwendung einzelner Bestimmungen des Schengen-Besitzstands auf Irland<sup>18</sup> ist Irland durch diese Verordnung gebunden.

Bulgarien und Rumänien: Diese Verordnung stellt einen auf dem Schengen-Besitzstand aufbauenden oder anderweitig damit zusammenhängenden Rechtsakt im Sinne des Artikels 4 Absatz 2 der Beitrittsakte von 2005 dar. Diese Verordnung muss in Verbindung mit dem Beschluss des Rates 2010/365/EU vom 29. Juni 2010<sup>19</sup> gelesen werden, der die Bestimmungen des Schengen-Besitzstands betreffend das Schengener Informationssystem in Bulgarien und Rumänien, mit einigen Einschränkungen, für anwendbar erklärt.

Zypern und Kroatien: Diese Verordnung stellt einen auf dem Schengen-Besitzstand aufbauenden oder anderweitig damit zusammenhängenden Rechtsakt im Sinne des Artikels 3 Absatz 2 der Beitrittsakte von 2003 bzw. des Artikels 4 Absatz 2 der Beitrittsakte von 2011 dar.

Assoziierte Länder: Auf der Grundlage der jeweiligen Abkommen, durch die diese Länder bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands assoziiert sind, werden Island, Norwegen, die Schweiz und Liechtenstein durch die vorgeschlagene Verordnung gebunden sein.

- **Subsidiarität**

Dieser Vorschlag baut auf dem bestehenden SIS auf, das seit 1995 in Betrieb ist, und entwickelt das System weiter. Der ursprüngliche zwischenstaatliche Rahmen wurde am 9. April 2013 durch Instrumente der Union ersetzt (Verordnung (EG) Nr. 1987/2006 und Beschluss 2007/533/JI des Rates). Eine vollständige Subsidiaritätsanalyse wurde bei früheren Gelegenheiten durchgeführt; diese Maßnahme zielt auf die weitere Präzisierung der bestehenden Bestimmungen ab, um ermittelte Lücken zu schließen und die operativen Verfahren zu verbessern.

Der beachtliche Informationsaustausch zwischen den Mitgliedstaaten über das SIS kann nicht durch dezentrale Lösungen erreicht werden. Wegen des Ausmaßes und der Auswirkungen der Maßnahme können die Ziele dieses Vorschlags auf Unionsebene besser erreicht werden.

---

<sup>17</sup> ABl. L 131 vom 1.6.2000, S. 43.

<sup>18</sup> ABl. L 64 vom 7.3.2002, S. 20.

<sup>19</sup> Beschluss 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).

Zu den Zielen dieses Vorschlags gehören unter anderem technische Verbesserungen zur Erhöhung der Effizienz des SIS sowie Anstrengungen zur Harmonisierung der Nutzung des Systems in allen teilnehmenden Mitgliedstaaten. Aufgrund des grenzübergreifenden Charakters dieser Ziele und der Herausforderungen bei der Gewährleistung eines wirksamen Informationsaustauschs, um den sich stets wandelnden Bedrohungen entgegenzuwirken, ist die EU gut aufgestellt, um Lösungen für diese Probleme vorzuschlagen, die von den Mitgliedstaaten allein nicht hinreichend erreicht werden können.

Werden die bestehenden Einschränkungen des SIS nicht angegangen, besteht die Gefahr, dass viele Möglichkeiten, eine optimale Effizienz und einen Mehrwert für die EU zu erzielen, ungenutzt bleiben und dass die bestehenden Schwächen die Arbeit der zuständigen Behörden gefährden. Das Fehlen harmonisierter Vorschriften für das Löschen von im System befindlichen gegenstandslosen Ausschreibungen kann beispielsweise zu einer Einschränkung der Freizügigkeit führen, die ein fundamentaler Grundsatz der Europäischen Union ist.

- **Verhältnismäßigkeit**

Artikel 5 des Vertrags über die Europäische Union besagt, dass die Maßnahmen der Union nicht über das zur Erreichung der Ziele der Verträge erforderliche Maß hinausgehen dürfen. Die Form, die für die betreffende EU-Maßnahme gewählt wird, muss ermöglichen, dass die Ziele des Vorschlags erreicht werden und dieser möglichst wirksam umgesetzt wird. Die vorgeschlagene Maßnahme beinhaltet eine Überarbeitung des SIS hinsichtlich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen.

Der Vorschlag orientiert sich am Grundsatz des *eingebauten Datenschutzes*. In Bezug auf das Recht auf Schutz personenbezogener Daten ist dieser Vorschlag verhältnismäßig, da er konkrete Bestimmungen zur Löschung von Ausschreibungen vorsieht und nicht vorschreibt, dass Daten länger als es für das Funktionieren des Systems und die Erreichung der damit angestrebten Ziele absolut notwendig ist erhoben und gespeichert werden. Auf der Grundlage der operativen Anforderungen wird durch diesen Vorschlag die Erfassungsdauer für Sachfahndungsausschreibungen reduziert und mit der von Personenausschreibungen in Einklang gebracht (da oftmals ein Bezug zu personenbezogenen Daten (persönliche Ausweispapiere, Kfz-Kennzeichen usw.) vorhanden ist). Erfahrungen aus der Polizeiarbeit zeigen, dass Diebesgut innerhalb relativ kurzer Zeit wiedererlangt werden kann, weshalb eine zehnjährige Ablaufrist bei Sachfahndungsausschreibungen unnötig lang ist.

SIS-Ausschreibungen enthalten nur die Daten, die erforderlich sind, um die Identität oder den Aufenthaltsort einer Person festzustellen oder einen Gegenstand ausfindig zu machen und eine geeignete operative Maßnahme zu ermöglichen. Alle weiteren ergänzenden Auskünfte werden über das SIRENE-Büro bereitgestellt, das den Austausch von Zusatzinformationen ermöglicht.

Des Weiteren sieht der Vorschlag die Umsetzung aller notwendigen Garantien und Verfahren für den wirksamen Schutz der Grundrechte der betroffenen Personen vor, insbesondere den Schutz ihrer Privatsphäre und der sie betreffenden personenbezogenen Daten. Er enthält zudem Bestimmungen, die insbesondere zur Erhöhung der Sicherheit der im SIS enthaltenen personenbezogenen Daten aufgenommen wurden.

Damit das System funktioniert, bedarf es keiner weiteren Verfahren oder Vereinheitlichung auf EU-Ebene. Die geplante Maßnahme ist verhältnismäßig, da sie – was ein Tätigwerden auf EU-Ebene anbelangt – nicht über das für die Erreichung der festgelegten Ziele erforderliche Maß hinausgeht.

- **Wahl des Instruments**

Die vorgeschlagene Überarbeitung erfolgt in Form einer Verordnung und ersetzt den Beschluss 2007/533/JI des Rates, wobei ein Großteil des Inhalts dieses Beschlusses übernommen wird. Der Beschluss 2007/533/JI wurde als „Instrument der dritten Säule“ nach dem ehemaligen Vertrag über die Europäische Union verabschiedet. Solche „Instrumente der dritten Säule“ wurden vom Rat ohne Mitwirkung des Europäischen Parlaments als Mitgesetzgeber verabschiedet. Die Rechtsgrundlage dieses Vorschlags ist der Vertrag über die Arbeitsweise der Europäischen Union (AEUV), da die Säulenstruktur nach dem Inkrafttreten des Vertrags von Lissabon am 1. Dezember 2009 weggefallen ist. Die Rechtsgrundlage schreibt die Anwendung des ordentlichen Gesetzgebungsverfahrens vor. Die Form einer Verordnung (des Europäischen Parlaments und des Rates) ist zu wählen, weil die Bestimmungen für alle Mitgliedstaaten verbindlich und in allen Mitgliedstaaten unmittelbar anwendbar sein sollen.

Der Vorschlag baut auf einem bestehenden zentralen System, durch das die Mitgliedstaaten miteinander kooperieren, auf und entwickelt es weiter, was eine gemeinsame Architektur und verbindliche Betriebsvorschriften erfordert. Zudem werden in dem Vorschlag verbindliche Vorschriften für den Zugriff auf das System festgelegt, unter anderem zum Zweck der Gefahrenabwehr und Strafverfolgung, die für alle Mitgliedstaaten sowie für die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts<sup>20</sup> (eu-LISA) einheitlich sind. Seit dem 9. Mai 2013 ist eu-LISA für das Betriebsmanagement des zentralen SIS zuständig, wozu alle Aufgaben gehören, die notwendig sind, um den Betrieb des zentralen SIS rund um die Uhr zu gewährleisten. Dieser Vorschlag baut auf den Zuständigkeiten von eu-LISA im Zusammenhang mit dem SIS auf.

Zudem sieht der Vorschlag unmittelbar anwendbare Vorschriften vor, die den betroffenen Personen den Zugang zu ihren eigenen Daten und zu Rechtsbehelfen ermöglichen, ohne dass hierzu weitere Durchführungsmaßnahmen erforderlich wären.

Deshalb kommt als Rechtsinstrument nur eine Verordnung in Frage.

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

- **Ex-post-Bewertungen/Eignungsprüfungen bestehender Rechtsvorschriften**

Gemäß der Verordnung (EG) Nr. 1987/2006 und dem Beschluss 2007/533/JI des Rates führte die Kommission drei Jahre nach der Inbetriebnahme des zentralen SIS II eine Gesamtbewertung des Systems sowie des bilateralen und multilateralen Austausches von Zusatzinformationen zwischen Mitgliedstaaten durch.

Das Ergebnis der Bewertung zeigte, dass Änderungen an der Rechtsgrundlage des SIS erforderlich sind, um auf die neuen Herausforderungen auf dem Gebiet der Sicherheit und der Migration besser reagieren zu können. Dazu gehört zum Beispiel ein Vorschlag zur End-to-End-Nutzung des SIS, der die Regulierung der Verwendung des Systems durch die Endnutzer betrifft und Datensicherheitsstandards vorsieht, die auch für Endnutzeranwendungen gelten. Des Weiteren wurde Folgendes vorgeschlagen: Stärkung des Systems im Hinblick auf die Terrorismusbekämpfung, indem eine neue zu ergreifende Maßnahme eingeführt wird,

---

<sup>20</sup> Errichtet durch die Verordnung (EU) Nr. 1077/2011 des Europäischen Parlaments und des Rates vom 25. Oktober 2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (ABl. L 286 vom 1.11.2011, S. 1).

Klärung der Situation von Kindern, die von der Entführung durch ihre Eltern bedroht sind, sowie Erweiterung der im System verfügbaren biometrischen Identifikatoren.

Die Ergebnisse der Bewertung zeigten zudem die Notwendigkeit rechtlicher Änderungen, um die technische Funktionsweise des Systems zu verbessern und die nationalen Verfahren zu straffen. Diese Maßnahmen werden die Wirksamkeit und Effizienz des SIS stärken, indem sie seine Nutzung erleichtern und unnötige Belastungen abbauen. Weitere Maßnahmen sollen die Datenqualität und die Transparenz des Systems durch eine eindeutigere Beschreibung der konkreten Berichterstattungspflichten der Mitgliedstaaten und der Agentur eu-LISA erhöhen.

Die Ergebnisse der umfassenden Bewertung (der Bewertungsbericht und die dazugehörige Arbeitsunterlage der Kommissionsdienststellen wurden am 21. Dezember 2016 verabschiedet<sup>21</sup>) bildeten die Grundlage für die in diesem Vorschlag enthaltenen Maßnahmen.

- **Konsultation der Interessenträger**

Im Verlauf der Bewertung des SIS ersuchte die Kommission die betroffenen Interessenträger, einschließlich der Delegierten des SIS/VIS-Ausschusses, um Rückmeldungen und Vorschläge nach dem Verfahren des Artikels 67 des Beschlusses 2007/533/JI des Rates. Diesem Ausschuss gehören Vertreter der Mitgliedstaaten an, die sowohl mit operativen SIRENE-Fragen (grenzübergreifende Zusammenarbeit in Bezug auf das SIS) als auch mit technischen Fragen zur Entwicklung und Wartung des SIS und der betreffenden SIRENE-Anwendung befasst sind.

Die Delegierten beantworteten ausführliche Fragebögen, die Bestandteil des Bewertungsverfahrens waren. Sofern weitere Erläuterungen notwendig waren bzw. ausführlicher auf das Thema eingegangen werden musste, wurde dies durch E-Mail-Kommunikation oder gezielte Gespräche erreicht. Durch dieses iterative Verfahren war es möglich, einzelne Themen umfassend und transparent zu erörtern. In den Jahren 2015 und 2016 diskutierten die Delegierten des SIS/VIS-Ausschusses diese Themen in speziellen Sitzungen und Workshops.

Zum Thema Datenschutz konsultierte die Kommission zudem insbesondere die nationalen Datenschutzbehörden der Mitgliedstaaten und die Mitglieder der SIS-II-Aufsichtskordinierungsgruppe. Die Mitgliedstaaten tauschten ihre Erfahrungen mit Anträgen auf Zugang zu den gespeicherten Daten und der Arbeit der nationalen Datenschutzbehörden aus, indem sie einen dafür vorgesehenen Fragebogen beantworteten. Die Antworten auf diesen Fragebogen vom Juni 2015 wurden bei der Ausarbeitung dieses Vorschlags berücksichtigt.

Intern richtete die Kommission eine dienststellenübergreifende Lenkungsgruppe ein, der Mitarbeiter des Generalsekretariats und der Generaldirektionen Migration und Inneres, Justiz und Verbraucher, Humanressourcen und Sicherheit sowie Informatik angehörten. Diese Lenkungsgruppe begleitete den Bewertungsprozess und bot erforderlichenfalls Orientierungshilfe.

Bei den Ergebnissen der Bewertung wurden zudem Informationen berücksichtigt, die bei den Bewertungsbesuchen in den Mitgliedstaaten vor Ort eingeholt wurden, wo ausführlich untersucht wurde, wie das SIS in der Praxis genutzt wird. Dazu wurden unter anderem

---

<sup>21</sup> Bericht an das Europäische Parlament und den Rat 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 und dazugehörige Arbeitsunterlage der Kommissionsdienststellen.

Diskussionen und Gespräche mit Anwendern, den Bediensteten der SIRENE-Büros und den zuständigen nationalen Behörden geführt.

Unter Berücksichtigung der Rückmeldungen sieht dieser Vorschlag Maßnahmen vor, die die technische und operative Wirksamkeit und Leistungsfähigkeit des Systems verbessern.

- **Einholung und Nutzung von Expertenwissen**

Neben den Konsultationen der Interessenträger holte die Kommission Expertenwissen auch durch drei Studien ein, deren Ergebnisse bei der Ausarbeitung dieses Vorschlags Berücksichtigung fanden:

- „SIS Technical Assessment“ (Technische Beurteilung des SIS) (Kurt Salmon)<sup>22</sup>

Bei dieser Beurteilung wurden die wichtigsten Probleme hinsichtlich der Funktionsweise des SIS und des künftigen Bedarfs ermittelt, die angegangen werden sollten. Hauptsächlich wurden Probleme bei der Optimierung der Betriebskontinuität und der Anpassung der Gesamtarchitektur entsprechend dem zunehmenden Kapazitätsbedarf festgestellt.

- „ICT Impact Assessment of Possible Improvements to the SIS II Architecture“ (Informations- und kommunikationstechnologische Folgenabschätzung möglicher Verbesserungen an der Architektur des SIS II) (Kurt Salmon)<sup>23</sup>

In dieser Studie wurden die gegenwärtigen Betriebskosten des SIS auf nationaler Ebene beurteilt und zwei mögliche technische Szenarien zur Verbesserung des Systems bewertet. Beide Szenarien enthalten eine Reihe von technischen Vorschlägen für Verbesserungen des zentralen Systems und der Gesamtarchitektur.

- „ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report“ (Informations- und kommunikationstechnologische Folgenabschätzung möglicher Verbesserungen an der Architektur des SIS II – Abschlussbericht), 10. November 2016 (Wavestone)<sup>24</sup>

In dieser Studie wurden die Auswirkungen der Kosten der Umsetzung einer nationalen Kopie auf die Mitgliedstaaten durch Analyse von drei Szenarien (ein vollständig zentrales System, eine von eu-LISA entwickelte und den Mitgliedstaaten bereitgestellte standardisierte N.SIS-Umsetzung und eine spezifische N.SIS-Umsetzung mit gemeinsamen technischen Standards) beurteilt.

- **Folgenabschätzung**

Die Kommission hat keine Folgenabschätzung durchgeführt.

Die drei vorgenannten unabhängigen Studien (unter „Einholung und Nutzung von Expertenwissen“) bildeten die Grundlage für die Ermittlung der Auswirkungen von Systemänderungen aus technischer Sicht. Zudem führte die Kommission seit 2013 – nachdem das SIS II am 9. April 2013 in Betrieb genommen worden und der Beschluss 2007/533/JI in

---

<sup>22</sup> Abschlussbericht der Europäischen Kommission – SIS II technical assessment (Technische Beurteilung des SIS II).

<sup>23</sup> Abschlussbericht der Europäischen Kommission – ICT Impact Assessment of Possible Improvements to the SIS II Architecture 2016 (Informations- und kommunikationstechnologische Folgenabschätzung möglicher Verbesserungen an der Architektur des SIS II).

<sup>24</sup> Abschlussbericht der Europäischen Kommission – „ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report“ (Informations- und kommunikationstechnologische Folgenabschätzung möglicher Verbesserungen an der Architektur des SIS II – Abschlussbericht), 10. November 2016 (Wavestone).

Kraft getreten war – zwei Überprüfungen des SIRENE-Handbuchs durch. Dazu gehören eine mittelfristige rückwirkende Beurteilung, die zur Einführung eines neuen SIRENE-Handbuchs<sup>25</sup> am 29. Januar 2015 führte. Die Kommission verabschiedete zudem einen Katalog von Empfehlungen und bewährten Praktiken.<sup>26</sup> Darüber hinaus nahmen eu-LISA und die Mitgliedstaaten regelmäßige, iterative technische Verbesserungen am System vor. Es wird davon ausgegangen, dass diese Optionen damit ausgeschöpft wurden und eine umfassende Änderung der Rechtsgrundlage erforderlich ist. Klarheit in Bereichen wie der Anwendung von Endnutzersystemen und ausführliche Bestimmungen über die Löschung von Ausschreibungen lassen sich nicht allein durch eine bessere Durchführung und Durchsetzung erreichen.

Zudem führte die Kommission eine umfassende Bewertung des SIS 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 durch und veröffentlichte eine dazugehörige Arbeitsunterlage der Kommissionsdienststellen. Die Ergebnisse der umfassenden Bewertung (der Bewertungsbericht und die diesbezügliche Arbeitsunterlage der Kommissionsdienststellen wurden am 21. Dezember 2016 verabschiedet) bildeten die Grundlage für die in diesem Vorschlag enthaltenen Maßnahmen.

Der in der Verordnung (EU) Nr. 1053/2013<sup>27</sup> vorgesehene Schengen-Bewertungsmechanismus ermöglicht die periodische rechtliche und operative Beurteilung der Funktionsweise des SIS in den Mitgliedstaaten. Die Bewertungen wurden von der Kommission und den Mitgliedstaaten gemeinsam durchgeführt. Ausgehend von den Bewertungen, die im Rahmen von ein- oder mehrjährigen Programmen durchgeführt wurden, richtet der Rat über diesen Mechanismus Empfehlungen an einzelne Mitgliedstaaten. Da diese Empfehlungen individueller Natur sind, können sie rechtlich verbindliche Vorschriften, die gleichzeitig in allen das SIS nutzenden Mitgliedstaaten anwendbar sind, nicht ersetzen.

Der SIS/VIS-Ausschuss erörtert regelmäßig praktische operative und technische Fragen. Obwohl die Sitzungen dieses Ausschusses wichtig für die Zusammenarbeit zwischen der Kommission und den Mitgliedstaaten sind, können die Ergebnisse dieser Gespräche (ausbleibende legislative Änderungen) nicht die Probleme beheben, die beispielsweise infolge unterschiedlicher nationaler Verfahren entstehen.

Die in dieser Verordnung vorgeschlagenen Änderungen stellen keine erhebliche wirtschaftliche Belastung oder Umweltbelastung dar. Sie werden jedoch voraussichtlich beträchtliche positive soziale Auswirkungen haben, da sie für mehr Sicherheit sorgen, indem bessere Verfahren zur Identifizierung von Personen eingeführt werden, die falsche Identitäten benutzen, von Straftätern, deren Identität nach der Verübung einer schweren Straftat

---

<sup>25</sup> Durchführungsbeschluss (EU) 2015/219 der Kommission vom 29. Januar 2015 zur Ersetzung des Anhangs zum Durchführungsbeschluss 2013/115/EU über das SIRENE-Handbuch und andere Durchführungsbestimmungen für das Schengener Informationssystem der zweiten Generation (SIS II) (ABl. L 44 vom 18.2.2015, S. 75).

<sup>26</sup> Empfehlung der Kommission zur Festlegung eines Katalogs von Empfehlungen und bewährten Praktiken für die korrekte Anwendung des Schengener Informationssystems der zweiten Generation (SIS II) und den Austausch von Zusatzinformationen durch die zuständigen Behörden der Mitgliedstaaten, die das SIS II umsetzen und nutzen (C(2015)9169/1).

<sup>27</sup> Verordnung (EU) Nr. 1053/2013 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).

unbekannt bleibt, und von vermissten Minderjährigen. Die Auswirkungen dieser Änderungen auf die Grundrechte und den Datenschutz wurden berücksichtigt und werden im nächsten Abschnitt („Grundrechte“) ausführlich erörtert.

Der Vorschlag wurde auf der Grundlage der für die Gesamtbewertung des SIS der zweiten Generation zusammengetragenen substanziellen Informationen ausgearbeitet, bei der die Funktionsweise des Systems und mögliche verbesserungsbedürftige Bereiche untersucht wurden. Zudem wurde eine Studie zur Folgenabschätzung der Kosten durchgeführt, um zu gewährleisten, dass die gewählte nationale Architektur am besten geeignet und verhältnismäßig ist.

- **Grundrechte und Datenschutz**

Dieser Vorschlag trägt zur Weiterentwicklung und Verbesserung eines bestehenden Systems bei statt ein neues System einzuführen und stützt sich folglich auf wichtige und wirksame Garantien, die bereits eingeführt wurden. Dennoch sind Auswirkungen auf die Grundrechte des Einzelnen möglich, da das System weiterhin personenbezogene Daten verarbeiten und weitere Kategorien sensibler biometrischer Daten enthalten wird. Diese Auswirkungen wurden sorgfältig berücksichtigt, und es wurden zusätzliche Garantien eingeführt, um die Erhebung und weitere Verarbeitung von Daten auf das absolut notwendige und in operativer Hinsicht erforderliche Maß zu begrenzen und nur jenen Personen Zugriff auf diese Daten zu gestatten, die sie verarbeiten müssen. In diesem Vorschlag werden eindeutige Datenspeicherfristen, einschließlich einer reduzierten Erfassungsdauer für Sachfahndungsausschreibungen, festgelegt. Zudem wird das Recht des Einzelnen, über die zu seiner Person erfassten Daten Auskunft zu erhalten und diese Daten berichtigen oder löschen zu lassen, im Einklang mit den Grundrechten ausdrücklich anerkannt und vorgesehen (siehe Abschnitt über Datenschutz und Datensicherheit).

Darüber hinaus stärkt der Vorschlag die Maßnahmen zum Schutz der Grundrechte, da mit ihm die Verpflichtung, eine Ausschreibung zu löschen, in einen Rechtsakt aufgenommen wird und im Fall einer Verlängerung der Ausschreibungsdauer eine Verhältnismäßigkeitsprüfung vorgesehen ist. Durch Verwendung biometrischer Daten zur Suche nach schutzbedürftigen vermissten Personen wird eine verlässlichere Identifizierung von Einzelpersonen möglich und zugleich sichergestellt, dass personenbezogene Daten sachlich richtig sind und angemessen geschützt werden. Mit dem Vorschlag werden umfassende und wirksame Garantien für die Verwendung von biometrischen Identifikatoren festgelegt, um Unannehmlichkeiten für unschuldige Personen zu vermeiden.

Der Vorschlag sieht zudem die durchgängige Sicherheit des Systems vor, um einen besseren Schutz der darin gespeicherten Daten zu gewährleisten. Mit der Einführung eines eindeutigen Störfallmanagementverfahrens und einer verbesserten Betriebskontinuität des SIS steht dieser Vorschlag hinsichtlich des Rechtes auf Schutz personenbezogener Daten vollständig mit der Charta der Grundrechte der Europäischen Union<sup>28</sup> im Einklang. Die Weiterentwicklung und fortdauernde Wirksamkeit des SIS wird zur Sicherheit der Menschen in der Gesellschaft beitragen.

In dem Vorschlag sind bedeutende Änderungen in Bezug auf biometrische Identifikatoren vorgesehen. Neben Fingerabdrücken sollten auch Handballenabdrücke abgenommen und gespeichert werden, sofern die rechtlichen Anforderungen erfüllt sind. Fingerabdruckprotokolle werden den alphanumerischen SIS-Ausschreibungen in der in den Artikeln 26, 32, 34 und 36 vorgesehenen Weise beigefügt. Es sollte künftig möglich sein,

---

<sup>28</sup> Charta der Grundrechte der Europäischen Union (2012/C 326/02).

diese daktylografischen Daten (Finger- und Handballenabdrücke) mit den an einem Tatort vorgefundenen Fingerabdrücken abzugleichen, sofern das Vergehen eine schwere oder terroristische Straftat darstellt und die Abdrücke mit hoher Wahrscheinlichkeit dem Täter zuzuordnen sind. Außerdem sieht der Vorschlag die Speicherung von Fingerabdrücken von „unbekannten gesuchten Personen“ vor (die Bedingungen sind in Abschnitt 5 Unterabschnitt „Lichtbilder, Gesichtsbilder, daktylografische Daten und DNA-Profile“ ausführlich erläutert). Kann die Identität einer Person anhand ihrer Dokumente nicht geklärt werden, sollten die zuständigen Behörden ihre Fingerabdrücke mit den in der SIS-Datenbank gespeicherten Abdrücken abgleichen.

In dem Vorschlag ist die Erhebung und Speicherung von ergänzenden Daten vorgesehen (etwa Angaben zu den persönlichen Ausweispapieren), die die Arbeit der Beamten vor Ort zur Feststellung der Identität einer Person erleichtern.

Der Vorschlag garantiert das Recht betroffener Personen auf wirksame Rechtsbehelfe, um Entscheidungen anzufechten; hierzu gehört in jedem Fall auch ein wirksamer Rechtsbehelf vor einem Gericht im Sinne des Artikels 47 der Charta der Grundrechte.

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

Das SIS stellt ein einziges Informationssystem dar. Folglich sollten die in den beiden Vorschlägen (also in dem vorliegenden und dem Vorschlag für eine Verordnung über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen) vorgesehenen Ausgaben nicht als zwei separate Beträge, sondern als ein einziger Betrag betrachtet werden. Die Auswirkungen der für die Umsetzung der beiden Vorschläge erforderlichen Änderungen auf den Haushalt sind in einem einzigen Finanzbogen enthalten.

Da der dritte Vorschlag (bezüglich der Rückkehr illegal aufhältiger Drittstaatsangehöriger) einen ergänzenden Charakter hat, werden dessen Auswirkungen auf den Haushalt gesondert in einem separaten Finanzbogen behandelt, der sich nur auf diese spezielle Ausschreibungskategorie bezieht.

Ausgehend von einer Beurteilung der verschiedenen Aspekte der Arbeit in Bezug auf das Netz und das zentrale SIS durch eu-LISA sowie der nationalen Entwicklungen in den Mitgliedstaaten erfordern die beiden Vorschläge für Verordnungen einen Gesamtbetrag von 64,3 Mio. EUR für den Zeitraum 2018 bis 2020.

Hierin enthalten sind die Kosten für eine Erhöhung der TESTA-NG-Bandbreite, da gemäß den beiden Vorschlägen über das Netz Fingerabdruckdateien und Gesichtsbilder übermittelt werden, was einen höheren Durchsatz und eine höhere Kapazität erfordert (9,9 Mio. EUR). Der Betrag enthält zudem die personellen und operativen Kosten von eu-LISA (17,6 Mio. EUR). eu-LISA teilte der Kommission mit, dass die Einstellung von drei neuen Vertragsbediensteten voraussichtlich im Januar 2018 stattfinden wird, damit die Entwicklungsphase rechtzeitig beginnen kann, um zu gewährleisten, dass die aktualisierten Funktionen des SIS 2020 in Betrieb genommen werden. Dieser Vorschlag hat technische Änderungen am zentralen SIS zur Folge, damit einige der bestehenden Ausschreibungskategorien ausgeweitet und neue Funktionen bereitgestellt werden können. Der diesem Vorschlag beigefügte Finanzbogen spiegelt einige dieser Änderungen wider.

Die Kommission führte zudem eine Studie zur Folgenabschätzung der Kosten durch, um die Kosten der durch diesen Vorschlag bedingten nationalen Entwicklungen zu beurteilen.<sup>29</sup> Die geschätzten Kosten belaufen sich auf 36,8 Mio. EUR, die als Pauschalbetrag auf die Mitgliedstaaten aufgeteilt werden sollten. Folglich erhält jeder Mitgliedstaat 1,2 Mio. EUR, um sein nationales System nach den in diesem Vorschlag dargelegten Anforderungen aufzurüsten, einschließlich der Erstellung einer nationalen Teilkopie, sofern noch nicht vorhanden, oder eines Backup-Systems.

Eine Neuprogrammierung des Restbetrags der Mittel, die für das Paket „Intelligente Grenzen“ im Rahmen des Fonds für die innere Sicherheit bereitgestellt wurden, ist geplant, um die Aufrüstungen durchzuführen und die in den beiden Vorschlägen vorgesehenen Funktionen umzusetzen. Die Verordnung ISF – Grenzen<sup>30</sup> ist das Finanzierungsinstrument, das die Mittel für die Umsetzung des Pakets „Intelligente Grenzen“ enthält. Artikel 5 dieser Verordnung sieht vor, dass 791 Mio. EUR für ein Programm zur Einführung von IT-Systemen verwendet werden, die die Steuerung von Migrationsströmen über die Außengrenzen gemäß den in Artikel 15 festgelegten Bedingungen unterstützen. Von den vorgenannten 791 Mio. EUR sind 480 Mio. EUR für die Entwicklung des Einreise-/Ausreisystems und 210 Mio. EUR für die Entwicklung des Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) vorgesehen. Der Restbetrag wird teilweise verwendet, um die Kosten der in den beiden Vorschlägen vorgesehenen Änderungen am SIS zu decken.

## **5. WEITERE ANGABEN**

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

Die Kommission, die Mitgliedstaaten und eu-LISA werden die Nutzung des SIS regelmäßig überprüfen und kontrollieren, um sicherzustellen, dass das System weiterhin wirksam und effizient funktioniert. Wie im Vorschlag vorgesehen, wird die Kommission bei der Durchführung der technischen und operativen Maßnahmen vom SIS/VIS-Ausschuss unterstützt.

Diese vorgeschlagene Verordnung sieht zudem in Artikel 71 Absätze 7 und 8 ein formelles, regelmäßiges Überprüfungs- und Bewertungsverfahren vor.

Alle zwei Jahre hat eu-LISA dem Europäischen Parlament und dem Rat einen Bericht über die technische Funktionsweise – einschließlich der Sicherheit – des SIS und der diesbezüglichen Kommunikationsinfrastruktur sowie über den bilateralen und multilateralen Austausch von Zusatzinformationen zwischen den Mitgliedstaaten zu unterbreiten.

Darüber hinaus hat die Kommission alle vier Jahre eine Gesamtbewertung des SIS und des Informationsaustauschs zwischen den Mitgliedstaaten vorzunehmen, die sie dem Parlament und dem Rat übermittelt. Dabei

- misst sie die Ergebnisse an den Zielen,

---

<sup>29</sup> Wavestone „ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report“ (Informations- und kommunikationstechnologische Folgenabschätzung möglicher Verbesserungen an der Architektur des SIS II – Abschlussbericht), 10. November 2016, Szenario 3, spezifische N.SIS-II-Umsetzung.

<sup>30</sup> Verordnung (EU) Nr. 515/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 zur Schaffung eines Instruments für die finanzielle Unterstützung für Außengrenzen und Visa im Rahmen des Fonds für die innere Sicherheit (ABl. L 150 vom 20.5.2014, S. 143).

- überprüft sie, ob die grundlegenden Prinzipien des Systems weiterhin Gültigkeit haben,
- prüft sie, inwieweit die Verordnung auf das zentrale System angewandt wird,
- bewertet sie die Sicherheit des zentralen Systems,
- untersucht sie die Auswirkungen auf den künftigen Betrieb des Systems.

Zudem hat eu-LISA nunmehr die Aufgabe, tägliche, monatliche und jährliche Statistiken über die Nutzung des SIS zu erstellen und somit für eine kontinuierliche Überwachung des Systems und seiner Funktionsweise anhand von Zielen zu sorgen.

- **Ausführliche Erläuterung der einzelnen Bestimmungen des Vorschlags**

**Bestimmungen, die sowohl dieser Vorschlag als auch der Vorschlag der Kommission für eine Verordnung über die Einrichtung, den Betrieb und die Nutzung des SIS im Bereich der Grenzkontrollen enthalten:**

- Allgemeine Bestimmungen (Artikel 1 bis 3)
- Systemarchitektur und Betrieb des SIS (Artikel 4 bis 14)
- Zuständigkeiten von eu-LISA (Artikel 15 bis 18)
- Zugriffsberechtigung und Erfassungsdauer für Ausschreibungen (Artikel 43, 46, 48, 50 und 51)
- Allgemeine Datenverarbeitungs- und Datenschutzbestimmungen (Artikel 53 bis 70)
- Kontrolle und Statistiken (Artikel 71)

**End-to-End-Nutzung des SIS**

Mit mehr als zwei Millionen Endnutzern in den zuständigen Behörden in ganz Europa ist das SIS ein außergewöhnlich stark genutztes und wirksames Instrument zum Austausch von Informationen. Diese Vorschläge enthalten Vorschriften, die den gesamten „End-to-End“-Betrieb des Systems betreffen, einschließlich des von eu-LISA betriebenen zentralen SIS, der nationalen Systeme und der Endnutzeranwendungen. Sie sind nicht nur auf das zentrale System und die nationalen Systeme ausgerichtet, sondern auch auf die technischen und operativen Bedürfnisse der Endnutzer.

Artikel 9 Absatz 2 sieht vor, dass die Endnutzer die zur Erfüllung ihrer Aufgaben erforderlichen Daten erhalten (insbesondere alle Daten, die für die Identifizierung der betroffenen Person und das Ergreifen der erforderlichen Maßnahmen notwendig sind). Zudem ist darin ein gemeinsamer Ansatz für die Umsetzung des SIS in den Mitgliedstaaten vorgesehen, der die Harmonisierung aller nationalen Systeme gewährleistet. In Artikel 6 ist festgelegt, dass alle Mitgliedstaaten die ununterbrochene Verfügbarkeit der SIS-Daten für die Endnutzer gewährleisten müssen, um mögliche Ausfallzeiten zu begrenzen und so den operativen Nutzen zu optimieren.

Artikel 10 Absatz 3 gewährleistet, dass die Sicherheit der Datenverarbeitung auch die Verarbeitungstätigkeiten des Endnutzers betrifft. Nach Artikel 14 sind die Mitgliedstaaten verpflichtet sicherzustellen, dass das Personal mit Berechtigung zum SIS-Zugang regelmäßig Schulungen in Fragen der Datensicherheit und in Bezug auf die Datenschutzvorschriften erhält.

Durch diese Maßnahmen wird in dem Vorschlag die vollständige „End-to-End“-Funktionsweise des SIS eingehender berücksichtigt – mit Vorschriften und Verpflichtungen,

die Millionen von Endnutzern in ganz Europa betreffen. Um eine möglichst wirkungsvolle Nutzung des SIS zu erreichen, sollten die Mitgliedstaaten gewährleisten, dass ihre Endnutzer bei jeder Datenabfrage in einer nationalen Polizei- oder Einwanderungsdatenbank immer auch eine Abfrage im SIS durchführen. Auf diese Weise kann das Ziel des SIS, das als wichtigste Ausgleichsmaßnahme im Raum ohne Binnengrenzkontrollen fungiert, erreicht werden, und die Mitgliedstaaten können besser auf die grenzüberschreitende Dimension der Kriminalität und die Mobilität von Straftätern reagieren. Diese gleichzeitige Abfrage muss im Einklang mit den Vorgaben des Artikels 4 der Richtlinie (EU) 2016/680<sup>31</sup> erfolgen.

### **Betriebskontinuität**

Die Vorschläge stärken die Bestimmungen über die Betriebskontinuität, sowohl auf nationaler Ebene als auch bei eu-LISA (Artikel 4, 6, 7 und 15). Dies gewährleistet, dass das SIS funktionsfähig und für die Bediensteten vor Ort zugänglich bleibt, auch wenn Probleme auftreten, die das System beeinflussen.

### **Datenqualität**

Der Vorschlag stützt sich auf den Grundsatz, dass der Mitgliedstaat, der die Daten besitzt, auch für die Richtigkeit der in das SIS eingegebenen Daten verantwortlich ist (Artikel 56). Allerdings muss ein von eu-LISA verwaltetes zentrales Verfahren vorgesehen werden, das den Mitgliedstaaten ermöglicht, regelmäßig Ausschreibungen zu überprüfen, bei denen die Pflichtdatenfelder möglicherweise Zweifel an der Qualität aufkommen lassen. Daher wird eu-LISA durch Artikel 15 des Vorschlags ermächtigt, regelmäßig Datenqualitätsberichte zu erstellen und diese den Mitgliedstaaten zu übermitteln. Diese Arbeit kann durch ein Datenregister für die Erstellung von statistischen Daten und Datenqualitätsberichten erleichtert werden (Artikel 71). Diese Verbesserungen spiegeln die vorläufigen Erkenntnisse der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität wider.

### **Lichtbilder, Gesichtsbilder, daktylografische Daten und DNA-Profile**

Die Möglichkeit, eine Abfrage anhand von Fingerabdrücken durchzuführen, um eine Person zu identifizieren, ist bereits in Artikel 22 der Verordnung (EG) Nr. 1987/2006 und im Beschluss 2007/533/JI des Rates vorgesehen. Mit den Vorschlägen wird diese Abfrage vorgeschrieben, wenn die Identität der Person auf anderem Wege nicht festgestellt werden kann. Außerdem werden Änderungen an Artikel 22 und die neuen Artikel 40, 41 und 42 die Verwendung von Gesichtsbildern, Handballenabdrücken und DNA-Profilen zur Identifizierung einer Person, zusätzlich zur Verwendung von Fingerabdrücken, ermöglichen. Gegenwärtig dürfen Gesichtsbilder nur verwendet werden, um die Identität einer Person anhand einer alphanumerischen Abfrage zu bestätigen; sie dienen nicht als Ausgangspunkt für eine Abfrage. Daktylografie ist die wissenschaftliche Untersuchung von Fingerabdrücken als Methode zur Feststellung der Identität einer Person. Nach Auffassung von Fachleuten für Daktylografie sind Handballenabdrücke einmalig und enthalten Bezugspunkte, anhand deren ebenso wie bei Fingerabdrücken ein präziser und schlüssiger Vergleich möglich ist. Handballenabdrücke können zur Feststellung der Identität einer Person auf dieselbe Weise wie Fingerabdrücke verwendet werden. Das Abnehmen von Handballenabdrücken gehört neben dem Abnehmen von zehn flachen und zehn gerollten Fingerabdrücken seit Jahrzehnten zur polizeilichen Praxis. Es gibt zwei Hauptverwendungen von Handballenabdrücken:

---

<sup>31</sup> Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (ABl. L 119 vom 4.5.2016, S. 89).

- i) Identifizierung, wenn die Fingerkuppen der betroffenen Person absichtlich oder unabsichtlich beschädigt wurden. Dies kann der Fall sein, wenn die betroffene Person eine Identifizierung oder die Abnahme von Fingerabdrücken verhindern möchte oder wenn die Fingerabdrücke infolge eines Unfalls oder schwerer manueller Arbeit beschädigt wurden. Bei den Gesprächen über die technischen Einzelheiten des SIS AFIS berichtete Italien von beachtlichen Erfolgen bei der Identifizierung von irregulären Migranten, die ihre Fingerkuppen absichtlich beschädigt hatten, um ihre Identifizierung zu verhindern. Die von den Behörden Italiens abgenommenen Handballenabdrücke ermöglichten eine nachträgliche Identifizierung.
- ii) Fingerabdruckspuren an Tatorten. Der Verdächtige hinterlässt an einem Tatort oft Spuren, die von der Handfläche stammen. Nur durch das routinemäßige Abnehmen von Handballenabdrücken von Personen, denen rechtmäßig Fingerabdrücke abgenommen werden dürfen, kann ein Verdächtiger identifiziert werden. Der Handballenabdruck enthält üblicherweise zudem Informationen von den Fingerwurzeln, die bei gerollten und flachen Fingerabdrücken oft fehlen, da Letztere auf die Fingerspitzen und oberen Gelenke ausgerichtet sind.

Die Verwendung von Gesichtsbildern für die Identifizierung wird eine bessere Abstimmung zwischen dem SIS und dem vorgeschlagenen EU-Einreise-/Ausreisensystem, elektronischen Gates und „Self-Service-Kiosks“ ermöglichen. Diese Funktion wird nur an regulären Grenzübergangsstellen verfügbar sein.

In Fällen, in denen keine Finger- oder Handballenabdrücke verfügbar sind, ist gemäß Artikel 22 Absatz 1 Buchstabe b die Verwendung von DNA-Profilen für vermisste Personen, die unter Schutz gestellt werden müssen, insbesondere Kinder, zulässig. Diese Funktion wird nur genutzt, falls keine Fingerabdrücke vorliegen, und ist ausschließlich befugten Nutzern zugänglich. Diese Bestimmung ermöglicht daher die Verwendung von DNA-Profilen in Bezug auf die vermisste Person bzw. die Eltern oder Geschwister des Kindes, damit nationale Behörden die betreffende Person identifizieren und ausfindig machen können. Die Mitgliedstaaten tauschen diese Informationen auf operativer Ebene bereits im Wege des Austausches von Zusatzinformationen miteinander aus. Der Vorschlag bildet einen Rechtsrahmen für diese Praxis, da diese in die sachliche Rechtsgrundlage für den Betrieb und die Nutzung des SIS aufgenommen wird und eindeutige Verfahren für die Umstände, unter denen solche Profile genutzt werden dürfen, festgelegt werden.

Die geplanten Änderungen erlauben auch, dass unbekannte, im Zusammenhang mit einer Straftat gesuchte Personen auf der Grundlage von Fingerabdrücken oder Handballenabdrücken im SIS ausgeschrieben werden (Artikel 40 bis 42). Diese Ausschreibungen können zum Beispiel dann erstellt werden, wenn am Tatort einer schweren Straftat Fingerabdruckspuren oder Handballenabdrücke entdeckt werden und es gewichtige Gründe für die Annahme gibt, dass die Fingerabdrücke dem Straftäter zuzuordnen sind – wenn beispielsweise an einer Waffe, die bei der Begehung der Straftat benutzt wurde, oder an einem anderen Gegenstand, den der Straftäter bei der Begehung der Straftat benutzte, Fingerabdrücke vorgefunden werden. Diese neue Ausschreibungskategorie ergänzt die Prüm-Bestimmungen, die eine Vernetzung der zu Strafverfolgungszwecken eingesetzten nationalen daktyloskopischen Identifizierungssysteme ermöglichen. Über das Prüm-Verfahren kann ein Mitgliedstaat abfragen, ob der Straftäter, dessen Fingerabdrücke vorgefunden wurden, in einem anderen Mitgliedstaat bekannt ist (üblicherweise für Ermittlungszwecke). Eine Person kann durch dieses Verfahren nur dann identifiziert werden, wenn ihr in einem anderen Mitgliedstaat zu Strafverfolgungszwecken Fingerabdrücke abgenommen wurden. Somit können Ersttäter nicht identifiziert werden. Die in diesem Vorschlag vorgesehenen neuen Maßnahmen, nämlich die Speicherung von Fingerabdrücken unbekannter gesuchter

Personen, ermöglicht, dass die Fingerabdrücke eines unbekanntes Straftäters in das SIS eingegeben werden können, damit er identifiziert werden kann, wenn er in einem anderen Mitgliedstaat gefunden wird. Die Anwendung dieser Funktion setzt voraus, dass der Mitgliedstaat zuvor alle verfügbaren nationalen und internationalen Quellen konsultiert hat und die Identität der betreffenden Person dabei nicht feststellen konnte. Der Vorschlag enthält ausreichende Garantien, um sicherzustellen, dass unter dieser Kategorie nur die Fingerabdrücke von Personen, die unter dringendem Verdacht stehen, eine schwere oder terroristische Straftat begangen zu haben, im SIS gespeichert werden. Daher ist diese neue Ausschreibungskategorie nur dann zulässig, wenn der unbekanntes Straftäter eine erhebliche Gefahr für die öffentliche Sicherheit darstellt, was einen Abgleich zwischen diesen Abdrücken und den Fingerabdrücken von Reisenden rechtfertigt, wenn zum Beispiel verhindert werden soll, dass die Person den Raum ohne Binnengrenzkontrollen verlässt.

Diese Bestimmung erlaubt Endnutzern nicht, unter dieser Kategorie Fingerabdrücke einzugeben, wenn deren Verbindung zum Straftäter nicht nachgewiesen werden kann. Eine weitere Bedingung besteht darin, dass die Identität der Person nicht mithilfe anderer nationaler, europäischer oder internationaler Datenbanken zur Speicherung von Fingerabdrücken festgestellt werden kann. Wenn ein solcher Fingerabdruck im SIS gespeichert ist, wird er zur Identifizierung von Personen genutzt, deren Identität nicht auf anderem Wege ermittelt werden kann. Wird bei dieser Überprüfung eine mögliche Übereinstimmung festgestellt, sollte der Mitgliedstaat die Fingerabdrücke weiter überprüfen und gegebenenfalls Fingerabdruckexperten hinzuziehen, um festzustellen, ob es sich um die Person handelt, deren Abdrücke im SIS gespeichert sind, und die Identität der Person sollte festgestellt werden. Die Verfahren unterliegen dem nationalen Recht. Die Identifizierung einer „unbekanntes gesuchten Person“, deren Abdrücke im SIS gespeichert sind, kann zu einer Verhaftung führen.

### **Zugang zum SIS**

In diesem Unterabschnitt werden die neuen Elemente der SIS-Zugangsrechte in Bezug auf die zuständigen nationalen Behörden sowie EU-Agenturen (institutionelle Nutzer) beschrieben.

### **Nationale Behörden – Einwanderungsbehörden**

Um eine optimale Nutzung des SIS sicherzustellen, wird nationalen Behörden, die für die Prüfung der Voraussetzungen und für Entscheidungen in Bezug auf die Einreise, den Aufenthalt und die Rückkehr von Drittstaatsangehörigen im Hoheitsgebiet der Mitgliedstaaten zuständig sind, mit diesem Vorschlag Zugang zum SIS gewährt. Diese Ergänzung ermöglicht die Konsultation des SIS im Zusammenhang mit irregulären Migranten, die bei regulären Grenzkontrollen nicht kontrolliert worden sind. Mit diesem Vorschlag wird gewährleistet, dass Drittstaatsangehörige, die die Außengrenzen an regulären Grenzübergangsstellen überschreiten (und damit Kontrollen unterliegen, die für Drittstaatsangehörige gelten) und Drittstaatsangehörige, die irregulär im Schengen-Raum eintreffen, die gleiche Behandlung erfahren.

Außerdem wird mit diesem Vorschlag gewährleistet, dass für die Zulassung von Kraftfahrzeugen (Artikel 44) sowie von Wasser- und Luftfahrzeugen zuständige Behörden, bei denen es sich um staatliche Stellen handelt, für die Ausübung ihrer Aufgaben eingeschränkter Zugang zum System erhalten. Dies wird dazu beitragen, die Zulassung der erwähnten Fahrzeuge zu verhindern, sofern diese gestohlen sind und in einem anderen Mitgliedstaat gesucht werden. Die Maßnahme ist in Bezug auf die Kfz-Zulassungsstellen nicht neu, da ihr Zugang zum SIS bereits gemäß Artikel 102a des Schengener

Durchführungsübereinkommens und der Verordnung (EG) Nr. 1986/2006<sup>32</sup> geregelt war. Nach derselben Logik ist im Vorschlag der Zugang der für die Zulassung von Wasserfahrzeugen und Luftfahrzeugen zuständigen Behörden zu SIS-Ausschreibungen in Bezug auf Wasserfahrzeuge und Luftfahrzeuge vorgesehen.

### **Institutionelle Nutzer**

Europol (Artikel 46), Eurojust (Artikel 47) und die Europäische Agentur für die Grenz- und Küstenwache – und ihre Teams, die Teams von mit rückkehrbezogenen Aufgaben betrautem Personal und die Mitglieder der Teams zur Unterstützung des Migrationsmanagements – (Artikel 48 und 49) haben im Bedarfsfall Zugriff auf das SIS und die im SIS enthaltenen Daten. Es wurden geeignete Garantien eingeführt, um zu gewährleisten, dass die im System enthaltenen Daten vorschriftsmäßig geschützt werden (einschließlich der Bestimmungen in Artikel 50, die vorsehen, dass diese Stellen nur auf diejenigen Daten zugreifen können, die sie zur Ausübung ihrer Aufgaben benötigen).

Diese Änderungen weiten den Zugriff von Europol auf das SIS auf Ausschreibungen von Vermissten aus, um zu gewährleisten, dass Europol das System bei der Ausübung seiner Aufgaben optimal nutzen kann; zudem werden neue Bestimmungen aufgenommen, die gewährleisten, dass die Europäische Agentur für die Grenz- und Küstenwache und ihre Teams auf das System zugreifen können, wenn sie im Rahmen ihres Auftrags verschiedene Maßnahmen zur Unterstützung der Mitgliedstaaten durchführen. Im Zuge der Arbeit der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität und im Hinblick auf die weitere Verstärkung des Informationsaustauschs zur Terrorismusbekämpfung wird die Kommission bewerten, ob Europol automatisch eine Benachrichtigung vom SIS erhalten sollte, wenn eine Ausschreibung zu einer Aktivität mit Terrorismusbezug erstellt wird.

Darüber hinaus wird die ETIAS-Zentralstelle der Europäischen Agentur für die Grenz- und Küstenwache gemäß dem Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS)<sup>33</sup> über das System ETIAS das SIS abfragen, um zu prüfen, ob eine Ausschreibung zu einem Drittstaatsangehörigen vorliegt, der eine Reisegenehmigung beantragt. Daher wird auch die ETIAS-Zentralstelle uneingeschränkter Zugriff auf das SIS haben.

### **Spezifische Änderungen an Ausschreibungen**

Nach Artikel 26 können Mitgliedstaaten Ausschreibungen zwecks Verhaftung (im Fall eines laufenden Polizeieinsatzes oder einer laufenden Ermittlung) vorübergehend aussetzen, wodurch sie für einen begrenzten Zeitraum lediglich für das SIRENE-Büro sichtbar sind, nicht jedoch für die Beamten vor Ort. Diese Bestimmung trägt dazu bei zu verhindern, dass ein vertraulicher Polizeieinsatz zur Verhaftung eines dringend gesuchten Straftäters durch einen nicht beteiligten Polizeibeamten gefährdet wird.

Artikel 32 und 33 betreffen Ausschreibungen von Vermissten. Änderungen an diesen Ausschreibungen erlauben präventive Ausschreibungen in Fällen, in denen ein hohes Risiko für eine Kindesentführung durch einen Elternteil besteht; zudem gewährleisten sie eine besser

---

<sup>32</sup> 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).

<sup>33</sup> COM(2016) 731 final.

abgestimmte Kategorisierung von Vermisstenausschreibungen. Kindesentführungen durch einen Elternteil geschehen oft unter präzise geplanten Umständen und mit der Absicht, den Mitgliedstaat, in dem die Sorgerechtsregelungen getroffen wurden, schnell zu verlassen. Mit diesen Änderungen wird eine mögliche Lücke im geltenden Rechtsrahmen behoben, wonach Ausschreibungen von Kindern erst eingegeben werden können, wenn diese vermisst werden. Somit können Behörden in den Mitgliedstaaten besonders gefährdete Kinder ausschreiben. Diese Änderungen bedeuten, dass Grenzschutz- und Strafverfolgungsbehörden in Fällen, in denen ein hohes Risiko einer unmittelbar bevorstehenden Kindesentführung durch ein Elternteil besteht, auf dieses Risiko hingewiesen werden, und dass sie, wenn ein gefährdetes Kind reist, die Umstände genauer untersuchen und das Kind gegebenenfalls in Schutzverwahrung nehmen können. Die SIRENE-Büros stellen zusätzliche Informationen, unter anderem in Bezug auf die Entscheidung der zuständigen Justizbehörde, die um die Ausschreibung ersucht hat, bereit. Das SIRENE-Handbuch wird entsprechend überarbeitet. Eine solche Ausschreibung erfordert eine entsprechende Entscheidung der Justizbehörde, nur einem Elternteil das Sorgerecht für das Kind zuzusprechen. Eine weitere Bedingung ist, dass eine Entführung unmittelbar bevorstehen könnte. Der Status von Ausschreibungen vermisster Kinder aktualisiert sich automatisch, um gegebenenfalls das Erreichen der Volljährigkeit anzuzeigen.

Nach Artikel 34 dürfen der Ausschreibung Daten über Fahrzeuge beigelegt werden, wenn es einen klaren Hinweis darauf gibt, dass diese mit der gesuchten Person in Verbindung stehen.

Mit Artikel 37 wird eine neue Form der Kontrolle eingeführt, nämlich die „Ermittlungsanfrage“. Sie dient insbesondere der Unterstützung von Maßnahmen zur Bekämpfung von Terrorismus und schweren Straftaten. Sie gestattet Behörden, die betroffene Person anzuhalten und zu befragen. Sie beinhaltet eine eingehendere Überprüfung als die bestehende verdeckte Kontrolle, umfasst jedoch keine Durchsuchung der Person und kommt keiner Verhaftung gleich. Sie kann jedoch ausreichende Informationen liefern, um über weitere zu ergreifende Maßnahmen zu entscheiden. Auch Artikel 36 wird geändert, um diese zusätzliche Art der Kontrolle zu berücksichtigen.

Dieser Vorschlag sieht vor, dass Ausschreibungen im SIS amtliche Blankodokumente und ausgestellte Ausweispapiere (Artikel 36) sowie Fahrzeuge, einschließlich Wasserfahrzeugen und Luftfahrzeugen (Artikel 32 und 34), umfassen können, sofern sie in Verbindung zu Personenausschreibungen nach diesen Artikeln stehen. Artikel 37 wird dahin gehend geändert, dass eine zu ergreifende Maßnahme auf der Grundlage dieser Ausschreibungen zu erfolgen hat. Diese Änderung dient ausschließlich Ermittlungszwecken, da sie Behörden ermöglicht, Situationen zu begegnen, in denen mehrere Personen echte Papiere verwenden, bei denen es sich aber um Doppelgängerdokumente handelt, deren rechtmäßige Inhaber sie nicht sind.

Artikel 38 enthält eine erweiterte Liste von Gegenständen, die ausgeschrieben werden können, wobei gefälschte Dokumente, Fahrzeuge unabhängig von ihrem Antriebssystem (d. h. Elektrofahrzeuge sowie Benzin-/Dieselfahrzeuge etc.), gefälschte Banknoten, IT-Ausrüstung und identifizierbare Teile von Fahrzeugen und Industrieausrüstung hinzugefügt wurden. Sie enthält keine Ausschreibungen von Zahlungsmitteln mehr, da die Wirksamkeit dieser Ausschreibungen sehr gering blieb und sie kaum Treffer hervorbrachten.

Um klarzustellen, wie vorzugehen ist, wenn ein ausgeschriebener Gegenstand gefunden worden ist, wird Artikel 39 um die Angabe ergänzt, dass Gegenstände im Einklang mit dem nationalen Recht beschlagnahmt werden müssen und zusätzlich die Behörde, die die Ausschreibung eingegeben hat, kontaktiert werden muss.

### **Datenschutz und Datensicherheit**

In diesem Vorschlag wird klargestellt, wer für die Verhütung und Meldung von Vorfällen sowie für die Reaktion auf Vorfälle zuständig ist, die die Sicherheit oder Integrität der SIS-Architektur, der SIS-Daten oder der Zusatzinformationen beeinträchtigen können (Artikel 10, 16 und 57).

Artikel 12 enthält Bestimmungen über das Führen und Abfragen von Protokollen der Historie der Ausschreibungen.

Artikel 12 enthält zudem Bestimmungen in Bezug auf die automatisierte Scansuche nach Kennzeichen von Kraftfahrzeugen mittels eines Systems zur automatischen Nummernschilderkennung, wonach die Mitgliedstaaten verpflichtet sind, diese Suchabfragen im Einklang mit dem nationalen Recht zu protokollieren.

Artikel 15 Absatz 3 übernimmt Artikel 15 Absatz 3 des Beschlusses 2007/533/JI des Rates und sieht vor, dass die Kommission weiterhin für die vertragliche Verwaltung der Kommunikationsinfrastruktur verantwortlich ist, wozu Aufgaben im Zusammenhang mit dem Haushaltsvollzug sowie der Erwerb und die Ersetzung von Ausrüstung gehören. Diese Aufgaben werden im zweiten Paket von SIS-Vorschlägen im Juni 2017 auf eu-LISA übertragen.

Artikel 21 weitet das Erfordernis, die Verhältnismäßigkeit, Relevanz und Bedeutung von Fällen zu prüfen, auf Entscheidungen über eine etwaige Verlängerung von Ausschreibungen aus. Neu ist, dass dieser Artikel die Mitgliedstaaten verpflichtet, gemäß den Artikeln 34, 36 bzw. 38 in Bezug auf Personen, deren Handlungen in den Anwendungsbereich der Artikel 1, 2, 3 und 4 des Rahmenbeschlusses 2002/475/JI des Rates zur Terrorismusbekämpfung fallen, oder in Bezug auf mit diesen Personen in Zusammenhang stehenden Gegenständen unter allen Umständen eine Ausschreibung zu erstellen.

#### Kategorien von Daten und Datenverarbeitung

Dieser Vorschlag erweitert die Arten von Informationen (Artikel 20), die über eine ausgeschriebene Person gespeichert werden können, um auch Folgendes zu erfassen:

- ob die Person an Handlungen beteiligt ist, die in den Anwendungsbereich der Artikel 1, 2, 3 und 4 des Rahmenbeschlusses 2002/475/JI des Rates fallen;
- andere personenbezogene Anmerkungen, den Ausschreibungsgrund;
- Angaben zur Eintragsnummer der Person in einem nationalen Register und zum Ort der Eintragung;
- Kategorisierung der Art des Vermisstenfalls (nur Ausschreibungen nach Artikel 32);
- Angaben zu den Ausweis- oder Reisedokumenten einer Person;
- Farbkopie der Ausweis- oder Reisedokumente der Person;
- DNA-Profil (nur falls keine für die Identifizierung geeigneten Fingerabdrücke verfügbar sind).

Mit Artikel 59 wird das Verzeichnis der personenbezogenen Daten ausgeweitet, die in Bezug auf Fälle des Missbrauchs der Identität einer Person in das SIS eingegeben und im SIS verarbeitet werden können. Diese Daten dürfen nur mit Zustimmung des Opfers der missbräuchlichen Identitätsverwendung eingegeben werden. Hierzu gehören nunmehr auch:

- Gesichtsbild;
- Handballenabdrücke;

- Angaben zu den Ausweispapieren;
- die Anschrift des Opfers;
- die Namen des Vaters und der Mutter des Opfers.

Artikel 20 sieht ausführlichere Angaben in Ausschreibungen vor. Dazu gehören die Angaben zu den persönlichen Ausweispapieren der betroffenen Personen und die Möglichkeit, vermisste Kinder entsprechend ihrem Verschwinden bestimmten Kategorien zuzuordnen, zum Beispiel vermisste Minderjährige, Entführung durch ein Elternteil, weggelaufene Kinder usw. Dies ist unerlässlich, damit die Endnutzer die erforderlichen Maßnahmen zum Schutz dieser Kinder ohne Verzögerung ergreifen können. Die erweiterten Informationen ermöglichen die bessere Identifizierung der betreffenden Person und befähigen die Endnutzer, besser fundierte Entscheidungen zu treffen. Zum Schutz der Endnutzer, die die Kontrollen durchführen, wird im SIS zudem angezeigt werden, ob die ausgeschriebene Person in den Anwendungsbereich der Artikel 1, 2, 3 und 4 des Rahmenbeschlusses 2002/475/JI des Rates zur Terrorismusbekämpfung<sup>34</sup> fällt.

In dem Vorschlag wird klargestellt, dass es den Mitgliedstaaten untersagt ist, die von einem anderen Mitgliedstaat eingegebenen Daten in andere nationale Dateien zu kopieren (Artikel 53).

#### Erfassungsdauer von Ausschreibungen

Die maximale Erfassungsdauer von Personenausschreibungen wird auf fünf Jahre verlängert, mit Ausnahme von Ausschreibungen zu verdeckten Kontrollen, Ermittlungsanfragen oder gezielten Kontrollen, für die die Erfassungsdauer weiterhin ein Jahr beträgt. Die Mitgliedstaaten können jederzeit kürzere Erfassungszeiten festlegen. Auf welchen Zeitraum die Ablauffrist einer Ausschreibung höchstens verlängert werden kann, hängt von den nationalen Praktiken zur Verlängerung der Frist in Fällen ab, in denen eine Ausschreibung ihren Zweck noch nicht erfüllt hat, die betroffene Person aber immer noch gesucht wird. Zudem war es erforderlich, die Erfassungsdauer im SIS mit der Erfassungsdauer im Rahmen von anderen Instrumenten wie der Rückführungsrichtlinie und Eurodac in Einklang zu bringen. Im Interesse der Transparenz und Klarheit ist es erforderlich, für Personenausschreibungen die gleiche Erfassungsdauer vorzusehen, mit Ausnahme von Ausschreibungen zu verdeckten Kontrollen, Ermittlungsanfragen oder gezielten Kontrollen. Die Verlängerung der Erfassungsdauer gefährdet die Interessen der betroffenen Personen nicht, da eine Ausschreibung nicht länger gespeichert werden darf als dies für ihren Zweck erforderlich ist. Die Regeln zur Löschung von Ausschreibungen sind in Artikel 52 ausdrücklich festgelegt. In Artikel 51 ist der Zeitrahmen für die Überprüfung von Ausschreibungen festgelegt, insbesondere die reduzierte Erfassungsdauer für Sachfahndungsausschreibungen. Da keine operativen Erfordernisse für eine längere Erfassungsdauer bei Sachfahndungsausschreibungen vorliegen, wurde sie auf fünf Jahre reduziert, um sie mit der Erfassungsdauer für Personenausschreibungen in Einklang zu bringen. Die Frist für ausgestellte und Blankodokumente beträgt jedoch weiterhin zehn Jahre, da die Gültigkeitsdauer von Dokumenten zehn Jahre beträgt.

#### Löschung

In Artikel 52 sind die Umstände dargelegt, unter denen Ausschreibungen gelöscht werden müssen, wodurch eine bessere Harmonisierung der nationalen Vorgehensweisen auf diesem

<sup>34</sup> Rahmenbeschluss 2002/475/JI des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung (ABl. L 164 vom 22.6.2002, S. 3).

Gebiet erreicht wird. Artikel 51 enthält besondere Bestimmungen für die Bediensteten von SIRENE-Büros zur proaktiven Löschung von nicht mehr erforderlichen Ausschreibungen, wenn keine Antwort von den zuständigen Behörden erhalten wurde.

#### Recht der betroffenen Personen auf Auskunft über Daten, Berichtigung unrichtiger Daten und Löschung unrechtmäßig gespeicherter Daten

Die ausführlichen Regelungen zu den Rechten der betroffenen Personen sind unverändert geblieben, da die bestehenden Regelungen bereits ein hohes Schutzniveau gewährleisten und mit der Verordnung (EU) 2016/679<sup>35</sup> sowie der Richtlinie 2016/680<sup>36</sup> in Einklang stehen. Zudem sind in Artikel 63 die Umstände dargelegt, unter denen die Mitgliedstaaten beschließen können, Informationen nicht an die betroffenen Personen weiterzugeben. Eine solche Entscheidung darf aus einem der in diesem Artikel aufgeführten Gründe getroffen werden und muss eine verhältnismäßige und notwendige Maßnahme im Sinne der nationalen Rechtsvorschriften darstellen.

Datenaustausch mit Interpol über gestohlene, unterschlagene, auf sonstige Weise abhandengekommene oder für ungültig erklärte Dokumente

In Artikel 63 wurde Artikel 55 des Beschlusses 2007/533/JI des Rates unverändert übernommen, da die bessere Interoperabilität der Dokumentenrubrik des SIS und der Interpol-Datenbank für gestohlene und verlorene Dokumente in der Mitteilung der hochrangigen Expertengruppe und im zweiten Paket von SIS-Vorschlägen im Juni 2017 behandelt wird.

#### Statistiken

Um einen Überblick über die Inanspruchnahme von Rechtsbehelfen in der Praxis zu bieten, ist in Artikel 66 ein statistisches Standardsystem für die Bereitstellung von Jahresberichten festgelegt, in denen folgende Zahlen zu erfassen sind:

- Anträge von betroffenen Personen auf Datenauskunft;
- Anträge auf Berichtigung unrichtiger Daten und Löschung unrechtmäßig gespeicherter Daten;
- vor Gericht anhängige Fälle;
- Fälle, in denen das Gericht zugunsten des Antragstellers entschieden hat, und
- Bemerkungen zu Fällen der gegenseitigen Anerkennung endgültiger Entscheidungen der Gerichte oder Behörden anderer Mitgliedstaaten über Ausschreibungen, die vom ausschreibenden Staat erstellt wurden.

#### Kontrolle und Statistiken

Artikel 71 enthält die Modalitäten, die festzulegen sind, um die ordnungsgemäße Überwachung des SIS und seiner Funktionsweise anhand der Ziele zu gewährleisten. Zu diesem Zweck wurde eu-LISA beauftragt, tägliche, monatliche und jährliche Statistiken über die Nutzung des Systems bereitzustellen.

---

<sup>35</sup> 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).

<sup>36</sup> Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (ABl. L 119 vom 4.5.2016, S. 89).

Artikel 71 Absatz 5 verpflichtet eu-LISA, statistische Berichte zu erstellen und diese der Kommission, Europol, Eurojust und der Europäischen Agentur für die Grenz- und Küstenwache vorzulegen, und gestattet der Kommission, zusätzliche statistische Daten und Datenqualitätsberichte über das SIS und die SIRENE-Kommunikation anzufordern.

Artikel 71 Absatz 6 sieht vor, dass eu-LISA im Rahmen der Überwachung der Funktionsweise des SIS ein Zentralregister einrichtet und hostet. Dadurch wird entsprechend ermächtigten Bediensteten der Mitgliedstaaten, der Kommission, von Europol, Eurojust und der Europäischen Agentur für die Grenz- und Küstenwache ermöglicht, auf die in Artikel 71 Absatz 3 aufgeführten Daten zuzugreifen, um die erforderlichen Statistiken zu erstellen.

Vorschlag für eine

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

**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 der Verordnung (EU) Nr. 515/2014 und zur Aufhebung der Verordnung (EG) Nr. 1986/2006, des Beschlusses 2007/533/JI 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,

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 fungiert als eine der wichtigsten Ausgleichsmaßnahmen zur Wahrung eines hohen Maßes an Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts der Europäischen Union, indem es die operative Zusammenarbeit zwischen Grenzschutz, Polizei, Zoll- und anderen Strafverfolgungsbehörden und Justizbehörden in Strafsachen unterstützt.
- (2) Das SIS wurde gemäß den Bestimmungen von Titel 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<sup>37</sup> (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<sup>38</sup> und dem Beschluss 2001/886/JI des Rates<sup>39</sup> die

<sup>37</sup> ABl. L 239 vom 22.9.2000, S. 19. Geändert durch die Verordnung (EG) Nr. 1160/2005 des Europäischen Parlaments und des Rates zur Änderung des Übereinkommens (ABl. L 191 vom 22.7.2005, S. 18).

<sup>38</sup> ABl. L 328 vom 13.12.2001, S. 4.

<sup>39</sup> 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).

Kommission betraut, und es wurde durch die Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates<sup>40</sup> sowie den Beschluss 2007/533/JI des Rates<sup>41</sup> 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 Artikel 24 Absatz 5, Artikel 43 Absatz 5 und Artikel 50 Absatz 5 der Verordnung (EG) Nr. 1987/2006 sowie Artikel 59 und Artikel 66 Absatz 5 des Beschlusses 2007/533/JI durch. Der Bewertungsbericht und die zugehörige Arbeitsunterlage der Kommissionsdienststellen wurden am 21. Dezember 2016 angenommen<sup>42</sup>. Die in diesen Dokumenten enthaltenen Empfehlungen sollten gegebenenfalls in diese Verordnung eingehen.
- (4) Diese Verordnung bildet die erforderliche Rechtsgrundlage für das SIS in Bezug auf die Angelegenheiten, die in den Anwendungsbereich von Titel V Kapitel 4 und 5 des Vertrags über die Arbeitsweise der Europäischen Union fallen. Die Verordnung (EU) 2018/... des Europäischen Parlaments und des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen<sup>43</sup> bildet die erforderliche Rechtsgrundlage für das SIS in Bezug auf die Angelegenheiten, die in den Anwendungsbereich von Titel V Kapitel 2 des Vertrags über die Arbeitsweise der Europäischen Union fallen.
- (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. Einige Bestimmungen dieser Rechtsinstrumente sollten daher identisch sein.
- (6) Es ist notwendig, die Ziele, die Systemarchitektur und die Finanzierung des SIS zu präzisieren und Vorschriften für den End-to-End-Betrieb und die End-to-End-Nutzung des Systems sowie die Zuständigkeiten, die in das System einzugebenden Datenkategorien, die Eingabezwecke und -kriterien, die zugriffsberechtigten Behörden, die Verwendung biometrischer Identifikatoren sowie weitere Vorschriften über die Datenverarbeitung festzulegen.
- (7) Das SIS umfasst ein zentrales System (im Folgenden „zentrales SIS“) und nationale Systeme mit einer vollständigen oder teilweisen Kopie der SIS-Datenbank. Angesichts der Tatsache, dass das SIS das wichtigste Instrument für den Informationsaustausch in Europa ist, muss sein ununterbrochener Betrieb sowohl auf zentraler als auch auf nationaler Ebene gewährleistet sein. Daher sollte jeder Mitgliedstaat eine teilweise oder vollständige Kopie der SIS-Datenbank anlegen und ein Backup-System einrichten.

---

<sup>40</sup> 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).

<sup>41</sup> 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).

<sup>42</sup> Bericht an das Europäische Parlament und den Rat 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 und die dazugehörige Arbeitsunterlage der Kommissionsdienststellen. (ABl. L ...).

<sup>43</sup> Verordnung (EU) 2018/...

- (8) Es ist notwendig, ein Handbuch zu pflegen, das Durchführungsvorschriften für den Austausch von bestimmten Zusatzinformationen im Hinblick auf die aufgrund der Ausschreibung erforderliche Maßnahme enthält. Die nationalen Behörden jedes Mitgliedstaats (die SIRENE-Büros) sollten den Austausch dieser Informationen gewährleisten.
- (9) Damit der effiziente Austausch von Zusatzinformationen über die gemäß der Ausschreibung zu treffenden Maßnahmen weiterhin garantiert ist, ist es zweckmäßig, die Funktionsweise der SIRENE-Büros zu verbessern und zu diesem Zweck die Anforderungen bezüglich der verfügbaren Ressourcen, der Schulung der Nutzer und der Reaktionszeit auf die aus anderen SIRENE-Büros eingegangenen Anfragen festzulegen.
- (10) Das Betriebsmanagement der zentralen Komponenten des SIS wird von der Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts<sup>44</sup> (im Folgenden „Agentur“) übernommen. Damit die Agentur die notwendigen finanziellen und personellen Ressourcen für alle Aspekte des Betriebsmanagements des zentralen SIS zuweisen kann, sollten ihre Aufgaben in dieser Verordnung ausführlich dargelegt werden, insbesondere hinsichtlich der technischen Aspekte des Austauschs von Zusatzinformationen.
- (11) Unbeschadet der Verantwortung der Mitgliedstaaten für die Richtigkeit der in das SIS eingegebenen Daten sollte die Agentur die Zuständigkeit für die Verbesserung der Datenqualität durch Einführung eines zentralen Instruments für die Überwachung der Datenqualität und für die regelmäßige Übermittlung entsprechender Berichte an die Mitgliedstaaten übernehmen.
- (12) Um eine bessere Überwachung der Nutzung des SIS für die Analyse von Trends im Zusammenhang mit Straftaten zu ermöglichen, sollte die Agentur in der Lage sein, ein dem neuesten Stand der Technik entsprechendes System für die statistische Berichterstattung an die Mitgliedstaaten, die Kommission, Europol und die Europäische Agentur für die Grenz- und Küstenwache zu entwickeln, bei dem die Integrität der Daten nicht beeinträchtigt wird. Daher sollte ein zentraler Speicher für statistische Daten eingerichtet werden. Die erstellten Statistiken sollten keine personenbezogenen Daten enthalten.
- (13) Das SIS sollte weitere Datenkategorien enthalten, um es den Endnutzern zu ermöglichen, ohne Zeitverlust fundierte Entscheidungen auf der Grundlage einer Ausschreibung zu treffen. Zur Erleichterung der Identifizierung von Personen und zur Aufdeckung von Mehrfachidentitäten sollten Datenkategorien zu Personen daher eine Bezugnahme auf das persönliche Ausweispapier oder dessen Nummer und, falls verfügbar, eine Kopie dieses Papiers umfassen.
- (14) Im SIS sollten keine für 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 des N.SIS sowie der Integrität und Sicherheit der Daten.

---

<sup>44</sup> Errichtet durch die Verordnung (EU) Nr. 1077/2011 des Europäischen Parlaments und des Rates vom 25. Oktober 2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (ABl. L 286 vom 1.11.2011, S. 1).

- (15) Das SIS sollte die Verarbeitung biometrischer Daten ermöglichen, damit die betroffenen Personen zuverlässiger identifiziert werden können. Ebenso sollte das SIS die Verarbeitung von Daten über Personen ermöglichen, deren Identität missbraucht wurde (um den Betroffenen Unannehmlichkeiten aufgrund einer falschen Identifizierung zu ersparen); eine solche Datenverarbeitung sollte an angemessene Garantien geknüpft sein, insbesondere an die Zustimmung der betroffenen Personen und an eine strikte Beschränkung der Zwecke, zu denen diese Daten rechtmäßig verarbeitet werden dürfen.
- (16) Die Mitgliedstaaten sollten die erforderlichen technischen Vorkehrungen dafür treffen, dass bei jeder Abfrage einer nationalen Polizei- oder Einwanderungsdatenbank durch dazu befugte Endnutzer automatisch auch eine Abfrage im SIS gemäß Artikel 4 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates<sup>45</sup> erfolgt. Damit soll dafür gesorgt werden, dass das SIS als wichtigste Ausgleichsmaßnahme im Raum ohne Kontrollen an den Binnengrenzen fungiert, und besser gegen die grenzüberschreitende Dimension der Kriminalität und die Mobilität von Straftätern vorgegangen werden kann.
- (17) In dieser Verordnung sollen die Voraussetzungen für die Verwendung von daktylografischen Daten und Gesichtsbildern zu Identifizierungszwecken festgelegt werden. Die Verwendung von Gesichtsbildern im SIS zu Identifizierungszwecken soll auch dazu beitragen, einheitliche Grenzkontrollverfahren sicherzustellen, bei denen die Identifizierung und die Überprüfung der Identität mittels Fingerabdruck und Gesichtsbild vorgeschrieben sind. Bei Zweifeln bezüglich der Identität einer Person sollte die Abfrage anhand daktylografischer Daten vorgeschrieben sein. Gesichtsbilder sollten nur im Rahmen regulärer Grenzkontrollen an „Self-Service-Kiosks“ und elektronischen Gates zu Identifizierungszwecken verwendet werden.
- (18) Durch die Einführung einer Funktion zur automatisierten Fingerabdruck-Identifizierung im SIS wird das bestehende Prüm-Verfahren über den grenzüberschreitenden Online-Zugriff auf spezielle nationale DNA-Datenbanken und automatisierte daktyloskopische Identifizierungssysteme<sup>46</sup> ergänzt. Das Prüm-Verfahren ermöglicht es, nationale daktyloskopische Identifizierungssysteme miteinander zu verbinden, sodass ein Mitgliedstaat abfragen kann, ob die Identität des Täters einer Straftat, dessen Fingerabdrücke vorgefunden wurden, in einem anderen Mitgliedstaat bekannt ist. Anhand des Prüm-Verfahrens wird geprüft, ob sich diese Fingerabdrücke bereits einer Person zuordnen lassen; selbst wenn die Identität eines Täters zu einem späteren Zeitpunkt festgestellt wird, wird er nicht unbedingt erfasst. Mit der Abfrage anhand von Fingerabdrücken im SIS kann aktiv nach dem Täter gesucht werden. Es sollte daher möglich sein, Fingerabdrücke eines unbekanntem Täters in das SIS einzugeben, sofern die Fingerabdrücke mit einer hohen

---

<sup>45</sup> Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

<sup>46</sup> Rahmenbeschluss 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). 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).

Wahrscheinlichkeit dem Täter einer schweren oder terroristischen Straftat zugeordnet werden können. Dies gilt insbesondere, wenn Fingerabdrücke auf einer Waffe oder einem Gegenstand vorgefunden werden, die bzw. der für eine Straftat verwendet wurde. Das bloße Vorfinden von Fingerabdrücken am Tatort sollte jedoch nicht als Indiz dafür gelten, dass es sich mit hoher Wahrscheinlichkeit um die Fingerabdrücke des Täters handelt. Eine weitere Voraussetzung für das Erstellen einer entsprechenden Ausschreibung sollte sein, dass die Identität eines Straftäters nicht mithilfe anderer nationaler, europäischer oder internationaler Datenbanken festgestellt werden kann. Im Falle einer möglichen Übereinstimmung sollte der Mitgliedstaat diese Fingerabdrücke weiter überprüfen und gegebenenfalls Fingerabdruckexperten hinzuziehen, um zu ermitteln, ob es sich um die Person handelt, deren Abdrücke im SIS gespeichert sind, und die Identität der Person sollte festgestellt werden. Die Verfahren sollten dem nationalen Recht unterliegen. Die Zuordnung der Abdrücke zu einer „unbekannten gesuchten Person“ im SIS kann wesentlich zu den Ermittlungen beitragen und zu einer Festnahme führen, sofern alle Bedingungen für eine Festnahme erfüllt sind.

- (19) Der Abgleich von an einem Tatort gefundenen Fingerabdrücken mit den im SIS gespeicherten Fingerabdrücken sollte zulässig sein, wenn sie mit hoher Wahrscheinlichkeit dem Täter zuzuordnen sind, der die schwere oder terroristische Straftat begangen hat. Schwere Straftaten sollten die im Rahmenbeschluss 2002/584/JI des Rates<sup>47</sup> aufgeführten Straftaten sein, und terroristische Straftaten sollten Straftaten nach einzelstaatlichem Recht im Sinne des Rahmenbeschlusses 2002/475/JI des Rates<sup>48</sup> sein.
- (20) Für den Fall, dass keine daktylografischen Daten verfügbar sind, sollte es möglich sein, ein DNA-Profil hinzuzufügen; das 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 Eltern oder Geschwister zur Identifizierung zu verwenden. Die rassische Herkunft sollte aus DNA-Daten nicht hervorgehen.
- (21) Das SIS sollte Personenausschreibungen zum Zwecke der Übergabe- oder Auslieferungshaft enthalten. Zusätzlich zu den Ausschreibungen sollte der Austausch ergänzender Daten vorgesehen werden, die für die Übergabe- und Auslieferungsverfahren erforderlich sind. Insbesondere sollten Daten im Sinne von Artikel 8 des Rahmenbeschlusses 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten<sup>49</sup> im SIS verarbeitet werden. Aus operativen Gründe ist es angemessen, dass der ausschreibende Mitgliedstaat eine bestehende Ausschreibung zur Verhaftung nach Ermächtigung der Justizbehörden vorübergehend nicht verfügbar macht, wenn eine Person, gegen die ein Europäischer Haftbefehl erlassen wurde, intensiv und aktiv gesucht wird und nicht an der konkreten Suche beteiligte Endnutzer den Erfolg der Suche gefährden könnten. Diese vorübergehende Nichtverfügbarkeit solcher Ausschreibungen sollte nicht länger als 48 Stunden dauern.

---

<sup>47</sup> 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).

<sup>48</sup> Rahmenbeschluss 2002/475/JI des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung (ABl. L 164 vom 22.6.2002, S. 3).

<sup>49</sup> 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).

- (22) 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.
- (23) Das SIS sollte Ausschreibungen von Vermissten enthalten, damit diese geschützt und etwaige Gefahren für die öffentliche Sicherheit abgewährt werden können. Ausschreibungen von Kindern, die dem Risiko einer Entführung ausgesetzt sind (d. h. Ausschreibungen die vorgenommen werden, um - wie bei Kindern, die dem Risiko einer Kindesentführungen durch einen Elternteil ausgesetzt sind - künftigen, noch nicht eingetretenen Schaden abzuwenden) sollten nur im beschränkten Umfang im SIS eingegeben werden können; diesbezüglich sollten strenge und angemessene Schutzmaßnahmen vorgesehen werden. Ausschreibungen von Kindern und die entsprechenden Verfahren sollten dem Wohl des Kindes gemäß Artikel 24 der Charta der Grundrechte der Europäischen Union und dem Übereinkommen der Vereinten Nationen von 20. November 1989 dienen.
- (24) Für Fälle im Zusammenhang mit einem Verdacht auf Terrorismus und schwerer Kriminalität sollte eine neue Maßnahme vorgesehen werden, die es ermöglicht, dass eine Person, die im Verdacht steht, eine schwere Straftat begangen zu haben oder bei der Grund zu der Annahme besteht, dass sie eine schwere Straftat begehen wird, angehalten und befragt werden kann, damit der ausschreibende Mitgliedstaat möglichst genaue Angaben erhält. Diese neue Maßnahme sollte nicht darauf hinauslaufen, dass die Person gesucht oder verhaftet wird. Sie sollte jedoch ausreichende Informationen liefern, damit weitere Maßnahmen beschlossen werden können. Schwere Straftaten sollten die im Rahmenbeschluss 2002/584/JI des Rates aufgeführten Straftaten sein.
- (25) Das SIS sollte neue Kategorien für Gegenstände von hohem Wert – wie elektronische und technische Ausrüstung – berücksichtigen, die mithilfe einer eindeutigen Kennnummer ermittelt und gesucht werden können.
- (26) Jeder Mitgliedstaat sollte die Möglichkeit haben, einer Ausschreibung einen Vermerk („Kennzeichnung“) hinzuzufügen, um deutlich zu machen, dass die gemäß der Ausschreibung zu ergreifende Maßnahme in seinem Hoheitsgebiet nicht vollzogen wird. Bei Ausschreibungen zum Zwecke der Übergabe sollte keine Bestimmung dieses Beschlusses dahin gehend ausgelegt werden dürfen, dass hiermit von der Anwendung der im Rahmenbeschluss 2002/584/JI enthaltenen Bestimmungen abgewichen oder deren Anwendung verhindert wird. Die Entscheidung, eine Kennzeichnung hinzuzufügen, sollte nur auf die im Rahmenbeschluss angegebenen Ablehnungsgründe gestützt sein.
- (27) Wurde eine Kennzeichnung hinzugefügt und konnte der Aufenthaltsort der zum Zwecke der Übergabe gesuchten Person ermittelt werden, so sollte der Aufenthaltsort 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.
- (28) Die Mitgliedstaaten sollten die Möglichkeit haben, Ausschreibungen im SIS miteinander zu verknüpfen. Das Verknüpfen von zwei oder mehr Ausschreibungen durch einen Mitgliedstaat sollte sich nicht auf die zu ergreifende Maßnahme, die Erfassungsdauer oder den Zugang zu den Ausschreibungen auswirken.
- (29) Ausschreibungen sollten nicht länger als für den verfolgten Zweck erforderlich im SIS gespeichert werden. Um den Verwaltungsaufwand für die verschiedenen Behörden,

die an der Verarbeitung von Daten zu Einzelpersonen für unterschiedliche Zwecke beteiligt sind, zu verringern, sollte die Erfassungsdauer von Ausschreibungen von Personen an die vorgesehene Erfassungsdauer für die Zwecke der Rückführung und des illegalen Aufenthalt angepasst werden. Darüber hinaus verlängern die Mitgliedstaaten regelmäßig die Ablauffrist von Personenausschreibungen, wenn die erforderliche Maßnahme nicht innerhalb der ursprünglichen Frist vollzogen werden konnte. Daher sollte die Erfassungsdauer von Ausschreibungen von Personen höchstens fünf Jahre betragen. Generell sollten Ausschreibungen von Personen nach fünf Jahren automatisch aus dem SIS gelöscht werden; dies gilt nicht für Ausschreibungen zu verdeckten Kontrollen, Ermittlungsanfragen oder gezielten Kontrollen. Diese sollten nach einem Jahr gelöscht werden. Sachfahndungsausschreibungen für verdeckte Kontrollen, Ermittlungsanfragen oder gezielten Kontrollen sollten nach einem Jahr automatisch aus dem SIS gelöscht werden, da sie stets im Zusammenhang mit Personen stehen. Sachfahndungsausschreibungen zur Sicherstellung oder Beweissicherung in Strafverfahren sollten nach fünf Jahren automatisch aus dem SIS gelöscht werden, da es sehr unwahrscheinlich ist, dass die betreffenden Gegenstände danach noch aufgefunden werden und da ihr wirtschaftlicher Wert danach wesentlich gesunken ist. Ausschreibungen zu ausgestellten Ausweispapieren und Blankoausweispapieren sollten zehn Jahre gespeichert werden, da der Gültigkeitszeitraum der Dokumente ab Ausstellungsdatum zehn Jahre beträgt. Die etwaige Entscheidung, Personenausschreibungen länger zu speichern, sollte auf der Grundlage einer umfassenden individuellen Bewertung ergehen. Die Mitgliedstaaten sollten Ausschreibungen von Personen innerhalb dieses Fünfjahreszeitraums überprüfen und Statistiken über die Zahl der Personenausschreibungen führen, deren Erfassungsdauer verlängert worden ist.

- (30) Vor Eingabe und Verlängerung der Ablauffrist einer SIS-Ausschreibung sollte geprüft werden, ob Angemessenheit, Relevanz und Bedeutung des konkreten Falles die Eingabe einer Ausschreibung in das SIS rechtfertigen und somit das Kriterium der Verhältnismäßigkeit erfüllt ist. Straftaten nach den Artikeln 1, 2, 3 und 4 des Rahmenbeschlusses 2002/475/JI des Rates zur Terrorismusbekämpfung<sup>50</sup> stellen eine schwerwiegende Bedrohung für die öffentliche Sicherheit, für die Unversehrtheit des Lebens von Personen und die Gesellschaft dar; diese Straftaten lassen sich in einem Raum ohne Binnengrenzkontrollen, in dem sich potenzielle Straftäter frei bewegen können, nur äußerst schwer verhindern, aufdecken und untersuchen. Wird im Zusammenhang mit diesen Straftaten nach einer Person oder einem Gegenstand gesucht, muss im SIS stets eine entsprechende Ausschreibung von Personen, die im Hinblick auf ein Strafverfahren gesucht werden, von Personen oder Gegenständen für verdeckte Kontrollen, Ermittlungsanfragen oder gezielte Kontrollen sowie von Gegenständen zur Sicherstellung erstellt werden, da diese Vorgehensweise für diesen Zweck am wirksamsten ist.
- (31) Bezüglich der Löschung von Ausschreibungen bedarf es einiger Präzisierungen. Eine Ausschreibung sollte nur so lange im SIS gespeichert werden, bis der Zweck, für den sie eingegeben wurden, erfüllt ist. Wegen der unterschiedlichen Gepflogenheiten der Mitgliedstaaten bei der Festlegung des Zeitpunkts, zu dem eine Ausschreibung ihren

---

<sup>50</sup> Rahmenbeschluss 2002/475/JI des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung (ABl. L 164 vom 22.6.2002, S. 3).

Zweck erfüllt hat, sollten für jede Ausschreibungskategorie genaue Kriterien dafür festgelegt werden, wann eine Ausschreibung aus dem SIS zu löschen ist.

- (32) 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 und ein einheitliches Meldeverfahren für Zwischenfälle verbindlich sein.
- (33) Daten, die im SIS in Anwendung dieser Verordnung verarbeitet werden, sollten Drittstaaten oder internationalen Organisationen nicht übermittelt oder zur Verfügung gestellt werden. Gleichwohl sollte, um die Zusammenarbeit zwischen der Europäischen Union und Interpol zu stärken, ein effizienter Austausch von Passdaten gefördert werden. Werden personenbezogene Daten aus dem SIS an Interpol weitergeleitet, so sollten diese personenbezogenen Daten einem angemessenen Schutz unterliegen, der durch ein Abkommen gewährleistet wird, das strenge Schutzmaßnahmen und Bedingungen vorsieht.
- (34) Es ist angezeigt, den für die Zulassung von Kraft-, Wasser- und Luftfahrzeugen zuständigen Behörden Zugriff auf das SIS zu gewähren, damit diese prüfen können, ob ein Fahrzeug bereits in einem Mitgliedstaat zur Sicherstellung oder zur Kontrolle ausgeschrieben ist. Behörden, bei denen es sich um staatliche Stellen handelt, sollten direkten Zugriff erhalten. Dabei sollte sich der Zugriff auf Ausschreibungen der entsprechenden Fahrzeuge und Zulassungsbescheinigungen oder Kennzeichen beschränken. Die Bestimmungen der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates<sup>51</sup> sollten daher in die vorliegende Verordnung aufgenommen werden, und die genannte Verordnung sollte aufgehoben werden.
- (35) Auf die Verarbeitung von Daten durch die zuständigen nationalen Behörden für die Zwecke der Verhütung, Untersuchung und Aufdeckung von schwerwiegenden oder terroristischen Straftaten oder die Verfolgung von Straftaten und die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sollten die nationalen Vorschriften zur Umsetzung der Richtlinie (EU) 2016/680 Anwendung finden. Die Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates<sup>52</sup> und der Richtlinie (EU) 2016/680 sollten in dieser Verordnung erforderlichenfalls präzisiert werden.
- (36) Für die Verarbeitung personenbezogener Daten im Rahmen dieser Verordnung durch die nationalen Behörden sollte die Verordnung (EU) 2016/679 gelten, wenn die Richtlinie (EU) 2016/680 keine Anwendung findet. Die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates<sup>53</sup> sollte für die Verarbeitung

---

<sup>51</sup> 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).

<sup>52</sup> 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).

<sup>53</sup> 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).

personenbezogener Daten durch die Organe und Einrichtungen der Union bei der Wahrnehmung ihrer Aufgaben aufgrund dieser Verordnung gelten.

- (37) Die Bestimmungen der Richtlinie (EU) 2016/680, der Verordnung (EU) 2016/679 und der Verordnung (EG) Nr. 45/2001 sollten in dieser Verordnung erforderlichenfalls präzisiert werden. Für die Verarbeitung personenbezogener Daten durch Europol ist die Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol-Verordnung)<sup>54</sup> maßgeblich.
- (38) Die Datenschutzbestimmungen des Beschlusses 2002/187/JI vom 28. Februar 2002<sup>55</sup> über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität gelten für die Verarbeitung von SIS-Daten durch Eurojust; dies schließt auch die Kontrollbefugnisse der gemäß jenem Beschlusses eingesetzten Gemeinsamen Kontrollinstanz in Bezug auf die Tätigkeiten von Eurojust und die Haftung bei rechtswidriger Verarbeitung personenbezogener Daten durch Eurojust ein. Stellt sich bei von Eurojust im SIS durchgeführten Abfragen heraus, dass eine von einem Mitgliedstaat erstellte Ausschreibung vorliegt, kann Eurojust nicht die erforderlichen Maßnahmen ergreifen. Daher sollte Eurojust den betreffenden Mitgliedstaat unterrichten, damit dieser den Fall weiterverfolgen kann.
- (39) Was die Geheimhaltung anbelangt, so unterliegen die Beamten und sonstigen Bediensteten, die in Verbindung mit dem SIS eingesetzt oder tätig werden, den einschlägigen Bestimmungen des Statuts der Beamten und der Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union.
- (40) Sowohl die Mitgliedstaaten als auch die Agentur sollten über Sicherheitspläne verfügen, die die Erfüllung der Sicherheitsanforderungen erleichtern; ferner sollten sie zusammenarbeiten, um Sicherheitsfragen aus einem gemeinsamen Blickwinkel zu betrachten.
- (41) Die unabhängigen nationalen Aufsichtsbehörden sollten die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der vorliegenden Verordnung überwachen. Die Rechte der betroffenen Person auf Zugang, Berichtigung und Löschung ihrer im SIS gespeicherten personenbezogenen Daten und etwaige Rechtsbehelfe vor nationalen Gerichten sowie die gegenseitige Anerkennung von Entscheidungen sollten präzisiert werden. Daher sollten von den Mitgliedstaaten zur Vorlage jährliche Statistiken verpflichtet werden.
- (42) Die Aufsichtsbehörden sollten gewährleisten, dass die Datenverarbeitungsvorgänge in ihrem N.SIS mindestens alle vier Jahre nach internationalen Prüfstandards überprüft werden. Die Prüfung sollte entweder von den Aufsichtsbehörden durchgeführt werden, oder die nationalen Aufsichtsbehörden sollten einen unabhängigen Datenschutzprüfer direkt beauftragen. Der unabhängige Prüfer sollte kontinuierlich unter der Kontrolle und der Verantwortung der nationalen Aufsichtsbehörde(n) arbeiten, die deshalb die Prüfung selbst in Auftrag geben und Zweck, Tragweite und Methodik der Prüfung klar

---

<sup>54</sup> Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 25.5.2016, S. 53).

<sup>55</sup> Beschluss 2002/187/JI des Rates vom 28. Februar 2002 über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität (ABl. L 63 vom 6.3.2002, S. 1).

vorgeben, Leitlinien festlegen sowie die Prüfung und ihre endgültigen Ergebnisse überwachen sollte(n).

- (43) Nach der Verordnung (EU) 2016/794 (Europol-Verordnung) unterstützt und verstärkt Europol die Tätigkeit der zuständigen Behörden der Mitgliedstaaten sowie deren Zusammenarbeit bei der Bekämpfung von Terrorismus und schwerer Kriminalität und erstellt Bedrohungs- und andere Analysen. 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 neuen, Europol eingeräumten Zugriff auf Ausschreibungen von Vermissten im SIS profitieren, insbesondere in Fällen von reisenden Sexualstraftätern und des sexuellen Missbrauchs von Kindern im Internet, in denen Straftäter oftmals behaupten, dass sie Kontakt zu Kindern haben oder aufnehmen können; dabei könnte es sich um vermisst gemeldete Kinder handeln. Ebenso spielt das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Migrantenschleusung eine wichtige strategische Rolle bei der Eindämmung der irregulären Migration und sollte daher Zugang zu Ausschreibungen von Personen erhalten, denen die Einreise in das oder der Aufenthalt im Hoheitsgebiet eines Mitgliedstaats entweder aus strafrechtlichen Gründen oder wegen Nichteinhaltung der Visums- und der Aufenthaltsbedingungen verweigert werden.
- (44) Um die bestehenden Lücken beim Informationsaustausch über Terrorismus, insbesondere über ausländische terroristische Kämpfer – bei denen die Überwachung ihrer Bewegungen von entscheidender Bedeutung ist – zu beseitigen, sollten die Mitgliedstaaten bei der Eingabe einer Ausschreibung in das SIS gleichzeitig etwaige Informationen über Aktivitäten mit Terrorismusbezug an Europol weitergeben; ebenso sollten sie Informationen über Treffer und damit verbundene Informationen an Europol übermitteln. Das bei Europol angesiedelte Europäische Zentrum zur Terrorismusbekämpfung sollte somit überprüfen können, ob in den Datenbanken von Europol zusätzliche Hintergrundinformationen vorliegen, und hochwertige Analysen erstellen können, die zur Zerschlagung terroristischer Netze beitragen und, wo möglich, Anschläge verhindern.
- (45) Ferner müssen Europol klare Regeln für die Verarbeitung und das Herunterladen von SIS-Daten vorgegeben werden, um eine möglichst umfassende Nutzung des SIS unter Wahrung der in dieser Verordnung und der Verordnung (EU) 2016/794 festgelegten Datenschutzstandards zu ermöglichen. Stellt sich bei von Europol im SIS vorgenommenen Abfragen heraus, dass eine von einem Mitgliedstaat erstellte Ausschreibung vorliegt, kann Europol nicht die erforderlichen Maßnahmen ergreifen. Daher sollte Europol den betreffenden Mitgliedstaat unterrichten, damit dieser den Fall weiterverfolgen kann.
- (46) In der Verordnung (EU) 2016/1624 des Europäischen Parlaments und des Rates<sup>56</sup> ist für die Zwecke der vorliegenden Verordnung vorgesehen, dass der

---

<sup>56</sup> 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

Einsatzmitgliedstaat die von der Europäischen Agentur für die Grenz- und Küstenwache entsandten Mitglieder der europäischen Grenz- und Küstenwacheteams oder der Teams von mit rückkehrbezogenen Aufgaben betrautem Personal ermächtigt, europäische Datenbanken abzufragen, wenn dies für die Erfüllung der im Einsatzplan für Grenzübertrittskontrollen, Grenzüberwachung und Rückkehr jeweils festgelegten Ziele erforderlich ist. Andere zuständige 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 europäischen Grenz- und Küstenwacheteams, der Teams von mit rückkehrbezogenen Aufgaben betrautem Personal und der Teams zur Unterstützung der Migrationssteuerung ist es, den ersuchenden Mitgliedstaaten – vor allem denjenigen, die einem unverhältnismäßigen Migrationsdruck ausgesetzt sind – als technische und operative Verstärkung zu dienen. Für die Erfüllung der Aufgaben, die den europäischen Grenz- und Küstenwacheteams, den Teams von mit rückkehrbezogenen Aufgaben betrautem Personal und den Teams zur Unterstützung der Migrationssteuerung zugewiesen sind, 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 dem Personalteam oder den Personalteams im SIS durchgeführten Abfragen heraus, dass eine von einem Mitgliedstaat eingegebene Ausschreibung vorliegt, kann das Teammitglied oder das Personal die erforderliche Maßnahme nur treffen, wenn es vom Einsatzmitgliedstaat dazu ermächtigt wird. Daher sollte es den betreffenden Mitgliedstaat unterrichten, damit der Fall weiterverfolgt werden kann.

- (47) Im Einklang mit dem Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS)<sup>57</sup> wird die ETIAS-Zentralstelle der Europäischen Agentur für die Grenz- und Küstenwache über ETIAS Überprüfungen im SIS vornehmen, um die Anträge auf Erteilung einer Reisegenehmigung zu prüfen; bei dieser Prüfung ist unter anderem vorgeschrieben, dass festgestellt werden muss, ob der Drittstaatsangehörige, der eine Reisegenehmigung beantragt, Gegenstand einer SIS-Ausschreibung ist. Zu diesem Zweck sollte die ETIAS-Zentralstelle innerhalb der Europäischen Agentur für die Grenz- und Küstenwache auch in dem für die Erfüllung ihres Auftrags erforderlichen Maße Zugriff auf das SIS haben, das heißt auf alle Kategorien von Ausschreibungen zu Personen und zu amtlichen Blankodokumenten und ausgestellten Ausweispapieren.
- (48) Bestimmte Aspekte des SIS können aufgrund ihres technischen Charakters, ihrer Detailliertheit und der Notwendigkeit einer regelmäßigen Aktualisierung durch die Bestimmungen dieser Verordnung nicht erschöpfend geregelt werden. Hierzu zählen beispielsweise technische Vorschriften für die Eingabe, Aktualisierung, Löschung und Abfrage von Daten, die Datenqualität, die Abfragerregeln im Zusammenhang mit biometrischen Identifikatoren, Vorschriften über die Vereinbarkeit und Priorität von Ausschreibungen, die Hinzufügung von Kennzeichnungen, Verknüpfungen zwischen Ausschreibungen, die Festlegung neuer Kategorien von Gegenständen innerhalb der Kategorie der technischen und elektronischen Ausrüstung, die Festlegung der

---

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).  
COM(2016) 731 final.

<sup>57</sup>

Ablauffrist von Ausschreibungen innerhalb der maximalen Frist und der Austausch von Zusatzinformationen. Die Durchführungsbefugnisse für diese Aspekte sollten daher der Kommission übertragen werden. Bei den technischen Vorschriften über die Abfrage von Ausschreibungen sollte auf die Wahrung eines reibungslosen Funktionierens der nationalen Anwendungen geachtet werden.

- (49) Um einheitliche Bedingungen für die Durchführung dieser Verordnung zu gewährleisten, sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011<sup>58</sup> ausgeübt werden. Die Durchführungsmaßnahmen für diese Verordnung sollten nach dem gleichen Verfahren angenommen werden wie Durchführungsmaßnahmen für die Verordnung (EU) 2018/xxx (Grenzkontrollen).
- (50) Im Sinne der Transparenz sollte die Agentur alle zwei Jahre einen Bericht über die technische Funktionsweise des zentralen SIS und der Kommunikationsinfrastruktur, einschließlich ihrer Sicherheit, und über den Austausch von Zusatzinformationen vorlegen. Die Kommission sollte alle vier Jahre eine Gesamtbewertung vornehmen.
- (51) Da die Ziele dieser Verordnung, nämlich die Einrichtung eines gemeinsamen Informationssystems und die diesbezügliche Regelung sowie der Austausch damit verbundener Zusatzinformationen, aufgrund von deren Beschaffenheit durch die Mitgliedstaaten nicht in ausreichendem Maße verwirklicht werden können und deshalb besser auf Unionsebene zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union niedergelegten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus.
- (52) Diese Verordnung steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden. Diese Verordnung zielt insbesondere darauf ab, ein sicheres Umfeld für alle Personen, die sich im Gebiet der Europäischen Union aufhalten, und den besonderen Schutz von Kindern vor Menschenhandel und Entführung durch einen Elternteil zu gewährleisten, und gleichzeitig den Schutz personenbezogener Daten uneingeschränkt zu wahren.
- (53) Nach den Artikeln 1 und 2 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 22 über die Position Dänemarks beteiligt sich Dänemark nicht an der Annahme dieser Verordnung, die daher für Dänemark weder bindend noch Dänemark gegenüber anwendbar ist. 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.
- (54) Das Vereinigte Königreich beteiligt sich an dieser Verordnung im Einklang mit Artikel 5 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 19 über den in den Rahmen der Europäischen Union einbezogenen Schengen-Besitzstand sowie im

---

<sup>58</sup> Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

Einklang mit Artikel 8 Absatz 2 des Beschlusses 2000/365/EG des Rates zum Antrag des Vereinigten Königreichs Großbritannien und Nordirland, einzelne Bestimmungen des Schengen-Besitzstands<sup>59</sup> auf sie anzuwenden.

- (55) Irland beteiligt sich an dieser Verordnung im Einklang mit im Einklang mit Artikel 5 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 19 über den in den Rahmen der Europäischen Union einbezogenen Schengen-Besitzstand sowie im Einklang mit Artikel 6 Absatz 2 des Beschlusses 2002/192/EG des Rates vom 28. Februar 2002 zum Antrag Irlands auf Anwendung einzelner Bestimmungen des Schengen-Besitzstands auf Irland<sup>60</sup>.
- (56) Für Island und Norwegen stellt diese Verordnung eine Weiterentwicklung von 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 dieser beiden letztgenannten Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands<sup>61</sup> dar, die in den in Artikel 1 Buchstabe G des Beschlusses 1999/437/EG des Rates<sup>62</sup> genannten Bereich fallen.
- (57) Für die Schweiz stellt diese Verordnung eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar, die in den in Artikel 1 Buchstabe G des Beschlusses 1999/437/EG in Verbindung mit Artikel 4 Absatz 1 der Beschlüsse 2004/849/EG<sup>63</sup> und 2004/860/EG des Rates<sup>64</sup> genannten Bereich fallen.
- (58) 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<sup>65</sup> dar, die zu dem in Artikel 1 Buchstabe G des Beschlusses 1999/437/EG

---

<sup>59</sup> ABl. L 131 vom 1.6.2000, S. 43.

<sup>60</sup> ABl. L 64 vom 7.3.2002, S. 20.

<sup>61</sup> ABl. L 176 vom 10.7.1999, S. 36.

<sup>62</sup> ABl. L 176 vom 10.7.1999, S. 31.

<sup>63</sup> Beschluss 2004/849/EG des Rates vom 25. Oktober 2004 über die Unterzeichnung — 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 und die vorläufige Anwendung einiger Bestimmungen dieses Abkommens (ABl. L 368 vom 15.12.2004, S. 26).

<sup>64</sup> Beschluss 2004/860/EG des Rates vom 25. Oktober 2004 über die Unterzeichnung im Namen der Europäischen Gemeinschaft 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 und die vorläufige Anwendung einiger Bestimmungen dieses Abkommens (ABl. L 370 vom 17.12.2004, S. 78).

<sup>65</sup> ABl. L 160 vom 18.6.2011, S. 21.

in Verbindung mit Artikel 3 des Beschlusses 2011/349/EU des Rates<sup>66</sup> und Artikel 3 des Beschlusses 2011/350/EU des Rates<sup>67</sup> genannten Bereich gehören.

- (59) 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 dem Beschluss 2010/365/EU des Rates über die Anwendung der Bestimmungen des Schengen-Besitzstands über das Schengener Informationssystem in der Republik Bulgarien und Rumänien<sup>68</sup> gelesen werden.
- (60) Für Zypern und Kroatien 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 und des Artikels 4 Absatz 2 der Beitrittsakte von 2011 dar.
- (61) 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.
- (62) Die in dieser Verordnung veranschlagten Kosten für die Aufrüstung der nationalen Systeme des SIS und die Implementierung der neuen Funktionen sind niedriger als der verbleibende Betrag in der Haushaltslinie für „Intelligente Grenzen“ gemäß der Verordnung (EU) Nr. 515/2014 des Europäischen Parlaments und des Rates<sup>69</sup>. Daher sollte mit der vorliegenden Verordnung der gemäß Artikel 5 Absatz 5 Buchstabe b der Verordnung (EU) Nr. 515/2014 für die Entwicklung von IT-Systemen zur Unterstützung der Steuerung von Migrationsströmen über die Außengrenzen zugewiesene Betrag neu zugewiesen werden.
- (63) Der Beschluss 2007/533/JI des Rates und der Beschluss 2010/261/EU der Kommission<sup>70</sup> sollten daher aufgehoben werden.

---

<sup>66</sup> 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).

<sup>67</sup> Beschluss 2011/350/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 in Bezug auf die Abschaffung der Kontrollen an den Binnengrenzen und den freien Personenverkehr (ABl. L 160 vom 18.6.2011, S. 19).

<sup>68</sup> ABl. L 166 vom 1.7.2010, S. 17.

<sup>69</sup> Verordnung (EU) Nr. 515/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 zur Schaffung eines Instruments für die finanzielle Unterstützung für Außengrenzen und Visa im Rahmen des Fonds für die innere Sicherheit (ABl. L 150 vom 20.5.2014, S. 143).

<sup>70</sup> 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).

- (64) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 angehört und hat am [...] 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 in dem 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 Bestimmungen des Dritten Teils Titel V Kapitel 4 und 5 des Vertrags über die Arbeitsweise der Europäischen Union im Bereich des Personenverkehrs in ihrem Hoheitsgebiet anzuwenden.

#### *Artikel 2*

#### *Anwendungsbereich*

- (1) In dieser Verordnung werden die Bedingungen 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, die Zuständigkeiten der Mitgliedstaaten und der Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, die allgemeine Datenverarbeitung, die Rechte der betroffenen Personen und die Haftung.

#### *Artikel 3*

#### *Begriffsbestimmungen*

- (1) Für die Zwecke dieser Verordnung bezeichnet der Ausdruck
  - a) „Ausschreibung“ einen in das SIS eingegebenen Datensatz einschließlich biometrischer Identifikatoren im Sinne der Artikel 22 und 40, der den zuständigen Behörden die Identifizierung einer Person oder einer Sache im Hinblick auf die Ergreifung spezifischer Maßnahmen ermöglicht;
  - b) „Zusatzinformationen“ Informationen, die nicht zu den im SIS gespeicherten Ausschreibungsdaten gehören, aber mit SIS-Ausschreibungen verknüpft sind und in folgenden Fällen ausgetauscht werden:
    - (1) bei Eingabe einer Ausschreibung, damit sich die Mitgliedstaaten konsultieren und unterrichten können;
    - (2) nach einem Treffer, damit die erforderlichen Maßnahmen ergriffen werden können;

- (3) in Fällen, in denen die erforderlichen Maßnahmen nicht ergriffen werden können;
  - (4) bei Fragen der Qualität der SIS-Daten;
  - (5) bei Fragen der Vereinbarkeit und Priorität von Ausschreibungen;
  - (6) bei Fragen des Auskunftsrechts;
- c) „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 System aufgefunden wird;
- d) „personenbezogene Daten“ alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“);
- e) „bestimmbare natürliche Person“ eine Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;
- f) „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 Protokollieren, die Organisation, das Ordnen, die Speicherung, 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;
- g) „Treffer“ im SIS, dass
- (1) von einem Benutzer eine Abfrage durchgeführt wird,
  - (2) die Abfrage ergibt, dass ein anderer Mitgliedstaat eine Ausschreibung in das SIS eingegeben hat,
  - (3) die Daten der Ausschreibung im SIS den für die Abfrage verwendeten Daten entsprechen und
  - (4) weitere Maßnahmen ergriffen werden müssen;
- h) „Kennzeichnung“ die Aussetzung einer Ausschreibung auf nationaler Ebene, die Ausschreibungen zwecks Verhaftung, Ausschreibungen von Vermissten und Ausschreibungen zu verdeckten Kontrollen, Ermittlungsanfragen und gezielten Kontrollen hinzugefügt werden kann, wenn ein Mitgliedstaat der Auffassung ist, dass die Durchführung einer Ausschreibung mit seinem nationalen Recht, mit internationalen Verpflichtungen oder wesentlichen nationalen Interessen nicht vereinbar ist. Wird eine Kennzeichnung hinzugefügt, so wird die aufgrund der Ausschreibung verlangte Maßnahme im Hoheitsgebiet dieses Mitgliedstaats nicht vollzogen.
- i) „ausschreibender Mitgliedstaat“ den Mitgliedstaat, der die Ausschreibung in das SIS eingegeben hat;

- j) „vollziehender Mitgliedstaat“ den Mitgliedstaat, der nach einem Treffer die erforderlichen Maßnahmen ergreift oder ergriffen hat;
- k) „Endnutzer“ die zuständigen Behörden, die direkt Abfragen in der CS-SIS, dem N.SIS oder einer technischen Kopie davon durchführen;
- l) „daktylografische Daten“ Daten zu Fingerabdrücken und Handballenabdrücken, die aufgrund ihrer Einzigartigkeit und der darin enthaltenen Bezugspunkte präzise und schlüssige Abgleiche zur Identität einer Person ermöglichen;
- m) „schwere Straftaten“ die in Artikel 2 Absätze 1 und 2 des Rahmenbeschlusses 2002/584/JI vom 13. Juni 2002<sup>71</sup> aufgeführten Straftaten;
- n) „terroristische Straftaten“ die nach nationalem Recht strafbaren Handlungen im Sinne der Artikel 1 bis 4 des Rahmenbeschlusses 2002/475/JI vom 13. Juni 2002<sup>72</sup>.

#### *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:
    - eine technische Unterstützungseinheit (im Folgenden „CS-SIS“), die eine Datenbank, die „SIS-Datenbank“, enthält;
    - eine einheitliche nationale Schnittstelle („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. Jedes N.SIS umfasst einen Datenbestand (im Folgenden „nationale Kopie“), der eine vollständige oder Teilkopie der SIS-Datenbank sowie ein Backup-N.SIS enthält. Das N.SIS und sein Backup können gleichzeitig verwendet werden, um die ununterbrochene Verfügbarkeit für die Endnutzer zu gewährleisten;
  - c) einer Kommunikationsinfrastruktur zwischen der 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.
- (2) Die Eingabe, Aktualisierung, Löschung und Abfrage von SIS-Daten erfolgen über die verschiedenen N.SIS. Eine nationale Teilkopie oder vollständige nationale Kopie dient innerhalb des Hoheitsgebiets der jeweiligen Mitgliedstaaten, die eine derartige Kopie verwenden, zur Abfrage im automatisierten Verfahren. Die nationale Teilkopie enthält mindestens die in Artikel 20 Absatz 2 dieser Verordnung aufgeführten Daten in Bezug auf Gegenstände und die Daten gemäß Artikel 20

<sup>71</sup> 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).

<sup>72</sup> Rahmenbeschluss 2002/475/JI des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung (ABl. L 164 vom 22.6.2002, S. 3).

Absatz 3 Buchstaben a bis v in Bezug auf Ausschreibungen von Personen. Die Datensätze der N.SIS anderer Mitgliedstaaten können nicht abgefragt werden.

- (3) Die CS-SIS ist für die technische Überwachung und die Verwaltung zuständig und verfügt über eine Backup-CS-SIS, die alle Funktionen der Haupt-CS-SIS bei einem Ausfall dieses Systems übernehmen kann. Die CS-SIS und die Backup-CS-SIS befinden sich an den beiden technischen Standorten der mit der Verordnung (EU) Nr. 1077/2011<sup>73</sup> errichteten Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (im Folgenden „Agentur“). Die CS-SIS oder die Backup-CS-SIS können eine zusätzliche Kopie der SIS-Datenbank enthalten und im aktiven Betrieb gleichzeitig genutzt werden, sofern jede von ihnen in der Lage ist, alle Transaktionen im Zusammenhang mit SIS-Ausschreibungen zu verarbeiten.
- (4) Die CS-SIS bietet die erforderlichen Dienste für die Eingabe und Verarbeitung der SIS-Daten, einschließlich der Abfrage der SIS-Datenbank. Die CS-SIS
  - a) nimmt Online-Aktualisierungen der nationalen Kopien vor;
  - b) gewährleistet die Synchronisierung und die Kohärenz zwischen den nationalen Kopien und der SIS-Datenbank;
  - c) ermöglicht die Initialisierung und Wiederherstellung der nationalen Kopien;
  - d) 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 Europäischen Union finanziert.
- (2) Diese Kosten beinhalten die Arbeiten in Bezug auf die CS-SIS zur Gewährleistung der in Artikel 4 Absatz 4 genannten Dienste.
- (3) 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 für zuständig, dass sein N.SIS errichtet, betrieben, gewartet sowie weiterentwickelt und an die NI-SIS angeschlossen wird.

---

<sup>73</sup> Errichtet durch die Verordnung (EU) Nr. 1077/2011 des Europäischen Parlaments und des Rates vom 25. Oktober 2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (ABl. L 286 vom 1.11.2011, S. 1).

Jeder Mitgliedstaat ist für den fortlaufenden Betrieb des N.SIS, seinen Anschluss an die NIS und die ununterbrochene Verfügbarkeit von SIS-Daten für die Endnutzer zuständig.

#### *Artikel 7*

##### *N.SIS-Stelle und SIRENE-Büro*

- (1) Jeder Mitgliedstaat benennt 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 Zugang der zuständigen Behörden zum SIS und trifft die erforderlichen Maßnahmen zur Gewährleistung der Einhaltung der Bestimmungen dieser Verordnung. Sie ist dafür zuständig, dass sämtliche Funktionen des SIS den Endnutzern auf angemessene Weise zur Verfügung gestellt werden.

Jeder Mitgliedstaat übermittelt seine Ausschreibungen über seine N.SIS-Stelle.

- (2) Jeder Mitgliedstaat bestimmt die Behörde (im Folgenden „SIRENE-Büro“), die den Austausch und die Verfügbarkeit aller Zusatzinformationen im Einklang mit den Bestimmungen des SIRENE-Handbuchs gemäß Artikel 8 gewährleistet.

Diese Büros koordinieren ferner die Überprüfung der Qualität der in das SIS eingegebenen Daten. Für diese Zwecke haben sie Zugriff auf im SIS verarbeitete Daten.

- (3) Die Mitgliedstaaten unterrichten die Agentur über ihre N.SIS-Stelle und ihr SIRENE-Büro. Die Agentur veröffentlicht die diesbezügliche Liste zusammen mit der in Artikel 53 Absatz 8 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 fortlaufenden Austausch von Zusatzinformationen sicherzustellen. Sollte die Kommunikationsinfrastruktur nicht zur Verfügung stehen, können die Mitgliedstaaten auf andere in angemessener Weise gesicherte technische Mittel für den Austausch von Zusatzinformationen zurückgreifen.
- (2) Zusatzinformationen dürfen nur für die Zwecke verwendet werden, für die sie gemäß Artikel 61 übermittelt wurden, es sei denn, der ausschreibende Mitgliedstaat hat vorher seine Zustimmung zu einer anderweitigen Verwendung erteilt.
- (3) Die SIRENE-Büros erfüllen ihre Aufgabe schnell und effizient, insbesondere indem sie Ersuchen so schnell wie möglich, spätestens jedoch 12 Stunden nach Eingang des Ersuchens, beantworten.
- (4) Genaue Vorschriften für den Austausch von Zusatzinformationen werden im Wege von Durchführungsmaßnahmen gemäß dem in Artikel 72 Absatz 2 genannten Prüfverfahren in Form eines Handbuchs mit der Bezeichnung „SIRENE-Handbuch“ festgelegt.

*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 der CS-SIS für die zügige und wirksame Übermittlung von Daten zu gewährleisten. Diese gemeinsamen Standards, Protokolle und technischen Verfahren werden im Wege von Durchführungsmaßnahmen nach dem in Artikel 72 Absatz 2 genannten Prüfverfahren angenommen.
- (2) Die Mitgliedstaaten stellen über die Dienste der CS-SIS sicher, dass die in der nationalen Kopie gespeicherten Daten durch automatische Aktualisierungen gemäß Artikel 4 Absatz 4 mit den Daten in der SIS-Datenbank identisch und kohärent sind und dass eine Abfrage in der nationalen Kopie ein gleichwertiges Ergebnis liefert wie eine Abfrage in der SIS-Datenbank. Endnutzer erhalten die zur Erfüllung ihrer Aufgaben erforderlichen Daten, insbesondere alle Daten, die für die Identifizierung der betroffenen Person und das Ergreifen der erforderlichen Maßnahmen notwendig sind.

*Artikel 10*  
*Sicherheit – Mitgliedstaaten*

- (1) Jeder Mitgliedstaat trifft für sein N.SIS die erforderlichen Maßnahmen, einschließlich der Annahme eines Sicherheitsplans, eines Betriebskontinuitätsplans und eines Notfallwiederherstellungsplans, 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) das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verhindern (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 Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle);
  - f) zu gewährleisten, dass die zur Benutzung eines automatisierten Datenverarbeitungssystems Berechtigten nur mittels einer persönlichen und eindeutigen Benutzerkennung und vertraulicher Zugriffsverfahren ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle);
  - g) zu gewährleisten, 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 nationalen

- Aufsichtsbehörden nach Artikel 66 auf deren Anfrage unverzüglich zur Verfügung stellen (Personalprofile);
- h) zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mithilfe von Datenübertragungseinrichtungen übermittelt werden können (Übermittlungskontrolle);
  - i) zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit, von wem und zu welchem Zweck in automatisierte Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle);
  - j) insbesondere durch geeignete Verschlüsselungstechniken zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle);
  - k) die Effizienz der in diesem Absatz genannten Sicherheitsmaßnahmen zu überwachen und die erforderlichen organisatorischen Maßnahmen bezüglich der internen Überwachung zu treffen (Eigenkontrolle).
- (2) Die Mitgliedstaaten treffen für die Verarbeitung und den Austausch von Zusatzinformationen einschließlich der Sicherung der Räumlichkeiten des SIRENE-Büros Sicherheitsmaßnahmen, die den in Absatz 1 genannten entsprechen.
- (3) Die Mitgliedstaaten treffen für die Verarbeitung von SIS-Daten durch die in Artikel 43 genannten Behörden Sicherheitsmaßnahmen, die den in Absatz 1 genannten entsprechen.

*Artikel 11*  
*Geheimhaltung - Mitgliedstaaten*

Jeder Mitgliedstaat wendet nach Maßgabe seines nationalen Rechts die einschlägigen Vorschriften über die berufliche Schweigepflicht beziehungsweise eine andere vergleichbare Geheimhaltungspflicht auf alle Personen und Stellen an, die mit SIS-Daten 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.

*Artikel 12*  
*Führen von Protokollen auf nationaler Ebene*

- (1) Die Mitgliedstaaten stellen sicher, dass jeder Zugriff auf personenbezogene Daten und jeder Austausch solcher Daten mit der CS-SIS in ihrem N.SIS protokolliert werden, damit die Rechtmäßigkeit der Abfrage und die Rechtmäßigkeit der Datenverarbeitung kontrolliert und eine Eigenkontrolle durchgeführt und das einwandfreie Funktionieren des N.SIS sowie die Datenintegrität und -sicherheit gewährleistet werden kann.
- (2) Die Datensätze enthalten insbesondere die Historie der Ausschreibung, das Datum und die Uhrzeit der Datenverarbeitung, die für die Abfrage verwendeten Daten, die Angaben zu den übermittelten Daten sowie den Namen der zuständigen Behörde und des für die Verarbeitung Verantwortlichen.

- (3) Bei Abfragen anhand von daktylografischen Daten oder des Gesichtsbilds gemäß Artikel 40, 41 und 42 enthalten die Protokolle insbesondere die Art der für die Abfrage verwendeten Daten, Angaben zur Art der übermittelten Daten sowie den Namen der zuständigen Behörde und des für die Verarbeitung Verantwortlichen.
- (4) Die Protokolle dürfen nur für den in Absatz 1 genannten Zweck verwendet werden und werden frühestens ein Jahr und spätestens drei Jahre, nachdem sie angelegt wurden, gelöscht.
- (5) Die Protokolle können über einen längeren Zeitraum gespeichert werden, wenn sie für ein bereits laufendes Kontrollverfahren benötigt werden.
- (6) Die zuständigen nationalen 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 diesen Protokollen, damit sie ihre Aufgaben wahrnehmen können.
- (7) Führen Mitgliedstaaten 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. Der Inhalt dieses Protokolls wird im Wege von Durchführungsmaßnahmen nach dem in Artikel 72 Absatz 2 genannten Prüfverfahren festgelegt. Im Falle einer Übereinstimmung mit im SIS oder in einer nationalen oder technischen Kopie des SIS gespeicherten Daten wird eine vollständige Abfrage im SIS durchgeführt, um zu prüfen, ob tatsächlich eine Übereinstimmung vorliegt. Für diese vollständige Abfrage gelten die Absätze 1 bis 6 des vorliegenden Artikels.

### *Artikel 13 Eigenkontrolle*

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

### *Artikel 14 Schulung des Personals*

Das Personal der zum Zugang zum 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 Datenschutzvorschriften und der Verfahren für die Datenverarbeitung gemäß dem SIRENE-Handbuch. Das Personal wird über alle einschlägigen Straftatbestände und Strafen informiert.

## KAPITEL III

### ZUSTÄNDIGKEITEN DER AGENTUR

#### *Artikel 15*

#### *Betriebsmanagement*

- (1) Für das Betriebsmanagement des zentralen SIS ist die Agentur zuständig. Die Agentur 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) Die Agentur ist ferner für folgende Aufgaben im Zusammenhang mit der Kommunikationsinfrastruktur zuständig:
  - a) Überwachung;
  - b) Sicherheit;
  - c) Koordinierung der Beziehungen zwischen den Mitgliedstaaten und dem Betreiber.
- (3) Die Kommission ist für alle sonstigen Aufgaben im Zusammenhang mit der Kommunikationsinfrastruktur zuständig, insbesondere für
  - a) Aufgaben im Zusammenhang mit dem Haushaltsvollzug;
  - b) Anschaffung und Erneuerung;
  - c) vertragliche Fragen.
- (4) Die Agentur ist ferner für folgende Aufgaben im Zusammenhang mit den SIRENE-Büros und der Kommunikation zwischen den SIRENE-Büros zuständig:
  - a) Koordinierung und Verwaltung von Tests;
  - b) Pflege und Aktualisierung der technischen Spezifikationen für den Austausch von Zusatzinformationen zwischen den SIRENE-Büros und die Kommunikationsinfrastruktur sowie Bewältigung der Auswirkungen technischer Änderungen, wenn diese sowohl das SIS als auch den Austausch von Zusatzinformationen zwischen SIRENE-Büros betreffen.
- (5) Die Agentur entwickelt und pflegt einen Mechanismus und Verfahren für die Durchführung von Qualitätskontrollen der Daten in der CS-SIS und erstattet den Mitgliedstaaten regelmäßig Bericht. Die Agentur legt der Kommission regelmäßig Berichte über die festgestellten Probleme und die betroffenen Mitgliedstaaten vor. Dieser Mechanismus, diese Verfahren und die Auslegung der Einhaltung der Datenqualität werden im Wege von Durchführungsmaßnahmen nach dem in Artikel 72 Absatz 2 genannten Prüfverfahren festgelegt.
- (6) Das Betriebsmanagement des zentralen SIS umfasst alle Aufgaben, die erforderlich sind, um das zentrale SIS 24 Stunden am Tag und 7 Tage in der Woche betriebsbereit zu halten; dazu gehören insbesondere die für den einwandfreien Betrieb des Systems erforderlichen Wartungsarbeiten und technischen Anpassungen. Zu diesen Aufgaben gehören auch Tests, die sicherstellen, dass das zentrale SIS und die nationalen Systeme gemäß den technischen und funktionellen Anforderungen nach Artikel 9 dieser Verordnung funktionieren.

*Artikel 16*  
*Sicherheit*

- (1) Die Agentur trifft die erforderlichen Maßnahmen, einschließlich der Annahme eines Sicherheitsplans sowie eines Betriebskontinuitätsplans und eines Notfallwiederherstellungsplans, um 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) das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verhindern (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 Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle);
  - f) zu gewährleisten, dass die zur Benutzung eines automatisierten Datenverarbeitungssystems Berechtigten nur mittels einer persönlichen und eindeutigen Benutzerkennung und vertraulicher Zugriffsverfahren ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle);
  - g) 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 nach Artikel 64 auf dessen Anfrage unverzüglich zur Verfügung zu stellen (Personalprofile);
  - h) zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mithilfe von Datenübertragungseinrichtungen übermittelt werden können (Übermittlungskontrolle);
  - i) zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle);
  - j) insbesondere durch geeignete Verschlüsselungstechniken zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle);
  - k) die Effizienz der in diesem Absatz genannten Sicherheitsmaßnahmen zu überwachen und die notwendigen organisatorischen Maßnahmen im Zusammenhang mit der internen Überwachung zu treffen, um die Einhaltung der Bestimmungen dieser Verordnung sicherzustellen (Eigenkontrolle).

- (2) Die Agentur trifft für die Verarbeitung und den Austausch von Zusatzinformationen über die Kommunikationsinfrastruktur Sicherheitsmaßnahmen, die den in Absatz 1 genannten entsprechen.

*Artikel 17*  
*Geheimhaltung - Agentur*

- (1) Unbeschadet des Artikels 17 des Statuts der Beamten und der Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union wendet die Agentur 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 vergleichbare Standards einzuhalten sind. Diese Pflicht besteht auch nach dem Ausscheiden dieser Personen aus dem Amt oder Dienstverhältnis oder nach der Beendigung ihrer Tätigkeit weiter.
- (2) Die Agentur trifft für den Austausch von Zusatzinformationen über die Kommunikationsinfrastruktur Geheimhaltungsmaßnahmen, die den in Absatz 1 genannten entsprechen.

*Artikel 18*  
*Führen von Protokollen auf zentraler Ebene*

- (1) Die Agentur stellt sicher, dass jeder Zugriff auf personenbezogene Daten und jeder Austausch personenbezogener Daten innerhalb der CS-SIS für die in Artikel 12 Absatz 1 genannten Zwecke protokolliert werden.
- (2) Die Protokolle enthalten insbesondere die Historie der Ausschreibungen, das Datum und die Uhrzeit der Datenübermittlung, die Art der für die Abfrage verwendeten Daten, Angaben zur Art der übermittelten Daten sowie die Bezeichnung der für die Datenverarbeitung verantwortlichen zuständigen Behörde.
- (3) Bei Abfragen anhand von daktylografischen Daten oder des Gesichtsbilds gemäß Artikel 40, 41 und 42 enthalten die Protokolle insbesondere die Art der für die Abfrage verwendeten Daten, Angaben zur Art der übermittelten Daten sowie den Namen der zuständigen Behörde und des für die Verarbeitung Verantwortlichen.
- (4) Die Protokolle dürfen nur für die in Absatz 1 genannten Zwecke verwendet werden und werden frühestens ein Jahr und spätestens drei Jahre, nachdem sie angelegt wurden, gelöscht. Die Protokolle, die die Historie von Ausschreibungen beinhalten, werden ein bis drei Jahre nach Löschung der betreffenden Ausschreibung gelöscht.
- (5) Die Protokolle können über einen längeren Zeitraum gespeichert werden, wenn sie für ein bereits laufendes Kontrollverfahren benötigt werden.
- (6) Die zuständigen Behörden, die die Rechtmäßigkeit der Abfrage kontrollieren, die Rechtmäßigkeit der Datenverarbeitung überwachen, eine Eigenkontrolle durchführen und das einwandfreie Funktionieren der CS-SIS sowie die Datenintegrität und -sicherheit gewährleisten, haben im Rahmen ihrer Zuständigkeiten auf Anfrage Zugang zu diesen Protokollen, damit sie ihre Aufgaben wahrnehmen können.

# KAPITEL IV

## INFORMATION DER ÖFFENTLICHKEIT

### *Artikel 19* *Aufklärungskampagnen über das SIS*

Die Kommission führt in Zusammenarbeit mit den nationalen Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten regelmäßig Aufklärungskampagnen zur Information der Öffentlichkeit über die Ziele des SIS, die gespeicherten Daten, die zum Zugang zum SIS berechtigten Behörden und die Rechte der betroffenen Personen durch. Die Mitgliedstaaten entwickeln in Zusammenarbeit mit ihren nationalen Aufsichtsbehörden die erforderlichen Maßnahmen zur allgemeinen Information ihrer Bürger über das SIS und setzen diese um.

# KAPITEL V

## KATEGORIEN VON DATEN UND KENNZEICHNUNG

### *Artikel 20* *Kategorien von Daten*

- (1) Unbeschadet von Artikel 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 für die in den Artikeln 26, 32, 34, 36 und 38 festgelegten Zwecke erforderlich sind.
- (2) Die Datenkategorien sind:
  - a) Informationen über ausgeschriebene Personen;
  - b) Informationen über die in den Artikeln 32, 36 und 38 aufgeführten Gegenstände.
- (3) Die Angaben zu ausgeschriebenen Personen enthalten nur Folgendes:
  - a) Nachname(n);
  - b) Vorname(n);
  - c) Geburtsname(n);
  - d) frühere Namen und Aliasnamen;
  - e) besondere objektive unveränderliche körperliche Merkmale;
  - f) Geburtsort;
  - g) Geburtsdatum;
  - h) Geschlecht;
  - i) Staatsangehörigkeit(en);
  - j) den Hinweis, ob die Person bewaffnet oder gewalttätig ist oder ob sie entflohen oder an einer Handlung beteiligt ist, die in den Artikeln 1, 2, 3 und 4 des Rahmenbeschlusses 2002/475/JI des Rates zur Terrorismusbekämpfung genannt ist;

- k) Ausschreibungsgrund;
  - l) ausschreibende Behörde;
  - m) eine Bezugnahme auf die Entscheidung, die der Ausschreibung zugrunde liegt;
  - n) zu ergreifende Maßnahme;
  - o) Verknüpfung(en) zu anderen Ausschreibungen im SIS nach Artikel 53;
  - p) die Art der Straftat, die der Ausschreibung zugrunde liegt;
  - q) die Eintragsnummer der Person in einem nationalen Register;
  - r) eine Kategorisierung der Art des Vermisstenfalls (nur bei Ausschreibungen nach Artikel 32);
  - s) Kategorie des Ausweispapiers der Person;
  - t) Ausstellungsland des Ausweispapiers der Person;
  - u) Anzahl der Ausweispapiere der Person;
  - v) Ausstellungsdatum des Ausweispapiers der Person;
  - w) Lichtbilder und Gesichtsbilder;
  - x) einschlägige DNA-Profile nach Maßgabe von Artikel 22 Absatz 1 Buchstabe b dieser Verordnung;
  - y) daktylografische Daten;
  - z) eine Farbkopie des Ausweispapiers.
- (4) Die technischen Vorschriften für die Eingabe, Aktualisierung, Löschung und Abfrage der Daten nach den Absätzen 2 und 3 werden im Wege von Durchführungsmaßnahmen nach dem in Artikel 72 Absatz 2 genannten Prüfverfahren festgelegt und entwickelt.
- (5) Die technischen Vorschriften für die Abfrage der Daten nach Absatz 3 werden nach dem in Artikel 72 Absatz 2 genannten Prüfverfahren festgelegt und entwickelt. Diese technischen Vorschriften müssen mit Abfragen in der CS-SIS, in nationalen Kopien und technischen Kopien nach Artikel 53 Absatz 2 vergleichbar und auf gemeinsame Standards gestützt sein, die im Wege von Durchführungsmaßnahmen nach dem in Artikel 72 Absatz 2 genannten Prüfverfahren festgelegt und entwickelt werden.

*Artikel 21*  
*Verhältnismäßigkeit*

- (1) Vor einer Ausschreibung und bei einer etwaigen Verlängerung der Gültigkeitsdauer einer Ausschreibung stellen die Mitgliedstaaten fest, ob Angemessenheit, Relevanz und Bedeutung des Falls die Aufnahme einer Ausschreibung in das SIS rechtfertigen.
- (2) Falls eine Person oder ein Gegenstand von einem Mitgliedstaat im Zusammenhang mit einer unter die Artikel 1 bis 4 des Rahmenbeschlusses 2002/475/JI des Rates zur Terrorismusbekämpfung fallenden Straftat gesucht wird, erstellt der Mitgliedstaat unter allen Umständen die entsprechende Ausschreibung nach Artikel 34, 36 oder 38.

## Artikel 22

### *Besondere Vorschriften für die Eingabe von Lichtbildern, Gesichtsbildern, daktylografischen Daten und DNA-Profilen*

- (1) Die Eingabe der in Artikel 20 Absatz 3 Buchstaben w, x und y genannten Daten in das SIS erfolgt gemäß den folgenden Vorgaben:
  - a) Lichtbilder, Gesichtsbilder, daktylografische Daten und DNA-Profile werden nur nach einer Qualitätsprüfung eingegeben, damit gewährleistet wird, dass Mindestqualitätsstandards eingehalten werden.
  - b) Ein DNA-Profil darf nur einer Ausschreibung gemäß Artikel 32 Absatz 2 Buchstaben a und c hinzugefügt werden, und nur für den Fall, dass keine zur Identifizierung geeigneten Lichtbilder, Gesichtsbilder oder daktylografischen Daten verfügbar sind. Die DNA-Profile von Personen, die direkte Verwandte in aufsteigender Linie, Verwandte in absteigender Linie oder Geschwister der ausgeschriebenen Person sind, können der Ausschreibung hinzugefügt werden, sofern diese Personen dem ausdrücklich zustimmen. Die rassische Herkunft der Person wird nicht in das DNA-Profil aufgenommen.
- (2) Für die Speicherung von Daten nach Absatz 1 Buchstabe a dieses Artikels und des Artikels 40 werden Qualitätsstandards festgelegt. Die Spezifikationen dieser Standards werden im Wege von Durchführungsmaßnahmen festgelegt und nach dem in Artikel 72 Absatz 2 genannten Prüfverfahren aktualisiert.

## Artikel 23

### *Anforderung an die Eingabe einer Ausschreibung*

- (1) Mit Ausnahme der in Artikel 40 genannten Situationen dürfen Ausschreibungen zu Personen nicht ohne die Angaben nach Artikel 20 Absatz 3 Buchstaben a, g, k, m und n sowie - falls anwendbar - Buchstabe p eingegeben werden.
- (2) Zudem sind alle übrigen in Artikel 20 Absatz 3 aufgeführten Angaben, soweit verfügbar, einzugeben.

## Artikel 24

### *Allgemeine Bestimmungen über die Kennzeichnung*

- (1) Ist ein Mitgliedstaat der Auffassung, dass die Durchführung einer nach den Artikeln 26, 32 oder 36 eingegebenen Ausschreibung mit seinem nationalen Recht, mit internationalen Verpflichtungen oder wesentlichen nationalen Interessen nicht vereinbar ist, so kann er nachträglich verlangen, die Ausschreibung so zu kennzeichnen, 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 nachträgliche Kennzeichnung einer Ausschreibung nach Artikel 26 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 Mitgliedstaat die nötigen Vorkehrungen, damit die Maßnahme unverzüglich ausgeführt werden kann.

#### *Artikel 25*

##### *Kennzeichnung von Personenfahndungsausschreibungen zum Zwecke der Übergabehaft*

- (1) Findet der Rahmenbeschluss 2002/584/JI Anwendung, so wird eine die Festnahme verhindernde Kennzeichnung einer Ausschreibung zum Zwecke der Übergabehaft nur hinzugefügt, 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.
- (2) Auf Anordnung einer nach nationalem Recht zuständigen Justizbehörde kann jedoch entweder aufgrund einer allgemeinen Anweisung oder in einem besonderen Fall auch nachträglich verlangt werden, dass eine Ausschreibung zum Zwecke der Übergabehaft gekennzeichnet wird, 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) Daten zu Personen, nach denen zum Zwecke der Übergabehaft mit Europäischem Haftbefehl gesucht wird oder nach denen zum Zwecke der Auslieferungshaft gesucht wird, werden auf Antrag der Justizbehörde des ausschreibenden Mitgliedstaats eingegeben.
- (2) Daten zu Personen, nach denen zum Zwecke der Übergabehaft gesucht wird, werden auch auf der Grundlage eines Haftbefehls eingegeben, der gemäß Übereinkünften zwischen der Union und Drittländern aufgrund von Artikel 37 des Vertrags über die Europäische Union über die 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 Europäischen Union und Drittländern auf der Grundlage von Artikel 37 des EU-Vertrags hinsichtlich der Übergabe von Personen auf der Grundlage eines Haftbefehls, die die Übermittlung eines solchen Haftbefehls über das SIS vorsehen, mit einschließen.
- (4) Der ausschreibende Mitgliedstaat kann im Fall einer laufenden Suche und nach Ermächtigung der zuständigen Justizbehörde des ausschreibenden Mitgliedstaats eine bestehende Ausschreibung zur Verhaftung gemäß Artikel 26 dieser Verordnung vorübergehend nicht für die Suche verfügbar machen, sodass die Ausschreibung für den Endnutzer nicht auffindbar ist und nur das SIRENE-Büro auf sie zugreifen kann. Diese Funktion darf für maximal 48 Stunden verwendet werden. Wenn es für operative Zwecke erforderlich ist, kann dieser Zeitraum jedoch um weitere

Zeiträume von jeweils 48 Stunden verlängert werden. Die Mitgliedstaaten führen Statistiken über die Zahl der Ausschreibungen, bei denen von dieser Funktion Gebrauch gemacht wurde.

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

#### *Artikel 28*

##### *Zusatzinformationen zu zum Zwecke der Übergabehaft gesuchten Personen*

Der Mitgliedstaat, der die Ausschreibung zum Zwecke der Übergabehaft in das SIS 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 die Ausschreibung zum Zwecke der Auslieferungshaft in das SIS eingegeben hat, übermittelt die folgenden Informationen im Wege des Austauschs von Zusatzinformationen an die anderen Mitgliedstaaten:
  - 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;
  - 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 werden nicht übermittelt, wenn die in den Artikeln 27 und 28 genannten Daten bereits mitgeteilt wurden und vom betroffenen Mitgliedstaat für die Durchführung einer Ausschreibung als ausreichend erachtet werden.

#### *Artikel 30*

##### *Umwandlung von Ausschreibungen zu zum Zwecke der Übergabe- oder Auslieferungshaft gesuchten Personen*

Ist eine Festnahme entweder wegen einer die Festnahme ablehnenden Entscheidung eines ersuchten Mitgliedstaats nach den in den Artikeln 24 oder 25 festgelegten Verfahren für die

Kennzeichnung oder im Falle einer Ausschreibung zum Zwecke der Auslieferungshaft wegen einer noch nicht abgeschlossenen Untersuchung nicht möglich, so behandelt der ersuchte Mitgliedstaat die Ausschreibung als Ausschreibung zur Aufenthaltsermittlung.

#### *Artikel 31*

#### *Maßnahmen aufgrund einer Personenausschreibung zum Zwecke der Festnahme mit dem Ziel der Übergabe oder der Auslieferung*

- (1) Findet der Rahmenbeschluss 2002/584/JI Anwendung, so stellt eine in das SIS eingegebene Ausschreibung nach Artikel 26 zusammen mit den ergänzenden Daten nach Artikel 27 einen gemäß diesem Rahmenbeschluss ausgestellten Europäischen Haftbefehl dar und hat die gleiche Wirkung wie dieser.
- (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**

#### *Artikel 32*

#### *Ausschreibungsziele und -bedingungen*

- (1) Daten in Bezug auf Vermisste oder sonstige Personen, die in Gewahrsam genommen werden müssen und/oder deren Aufenthaltsort festgestellt werden muss, werden auf Ersuchen der zuständigen Behörde des ausschreibenden Mitgliedstaats in das SIS eingegeben.
- (2) Folgende Kategorien von Vermissten können eingegeben werden:
  - a) Vermisste, die
    - i) im Interesse ihres eigenen Schutzes oder
    - ii) zur Gefahrenabwehr in Gewahrsam genommen werden müssen, und
  - b) Vermisste, die nicht in Gewahrsam genommen werden müssen;
  - c) von Entführung bedrohte Kinder gemäß Absatz 4.
- (3) Absatz 2 Buchstabe a findet insbesondere auf Kinder und Personen Anwendung, die aufgrund einer Anordnung einer zuständigen Stelle zwangsweise untergebracht werden müssen.
- (4) In Fällen, in denen das konkrete und offensichtliche Risiko besteht, dass ein Kind im Sinne von Absatz 2 Buchstabe c in Kürze aus dem Mitgliedstaat, der die Zuständigkeit in Fragen der elterlichen Verantwortung im Einklang mit der Verordnung (EG) Nr. 2201/2003 des Rates<sup>74</sup> hat, entführt wird, wird auf Antrag der

---

<sup>74</sup> Verordnung (EG) Nr. 2201/2003 des Rates vom 27. November 2003 über die Zuständigkeit, Anerkennung und Vollstreckung von Entscheidungen in Ehesachen und in Verfahren betreffend die

zuständigen Justizbehörde dieses Mitgliedstaats eine Ausschreibung zu dem betreffenden Kind eingegeben. In den Mitgliedstaaten, die Vertragsparteien des Haager Übereinkommens vom 19. Oktober 1996 über die Zuständigkeit, das anzuwendende Recht, die Anerkennung, Vollstreckung und Zusammenarbeit auf dem Gebiet der elterlichen Verantwortung und der Maßnahmen zum Schutz von Kindern sind, und in denen die Verordnung (EG) Nr. 2201/2003 des Rates nicht anwendbar ist, sind die Bestimmungen des Haager Übereinkommens anwendbar.

- (5) Die Mitgliedstaaten stellen sicher, dass aus den in das SIS eingegebenen Daten jeweils hervorgeht, in welche der in Absatz 2 genannten Kategorien die vermisste Person einzuordnen ist. Die Mitgliedstaaten sorgen zudem dafür, dass aus den in das SIS eingegebenen Daten hervorgeht, um welche Art eines Vermisstenfalls oder eines Falls einer gefährdeten Person es sich handelt. Die Bestimmungen über die Kategorisierung der Fallarten und über die Eingabe der betreffenden Daten werden im Wege von Durchführungsmaßnahmen gemäß dem Prüfverfahren nach Artikel 72 Absatz 2 festgelegt und weiterentwickelt.
- (6) Vier Monate bevor ein Kind, das Gegenstand einer Ausschreibung gemäß dieses Artikels ist, das Erwachsenenalter erreicht, teilt die CS-SIS automatisch dem ausschreibenden Mitgliedstaat mit, dass der Grund des Ersuchens und die zu ergreifenden Maßnahmen aktualisiert werden müssen oder die Ausschreibung gelöscht werden muss.
- (7) Besteht ein eindeutiger Hinweis darauf, dass Kraft-, Wasser- oder Luftfahrzeuge mit einer Person verbunden sind, die Gegenstand einer Ausschreibung gemäß Absatz 2 ist, können Ausschreibungen zu den betreffenden Kraft-, Wasser- oder Luftfahrzeugen vorgenommen werden, um die Person ausfindig zu machen. In derartigen Fällen werden die Ausschreibung der vermissten Person und die Ausschreibung des Gegenstands im Einklang mit Artikel 60 miteinander verknüpft. Die technischen Vorschriften für die Eingabe, Aktualisierung, Löschung und Abfrage der in diesem Absatz genannten Daten werden im Wege von Durchführungsmaßnahmen nach dem in Artikel 72 Absatz 2 genannten Prüfverfahren festgelegt und weiterentwickelt.

### *Artikel 33*

#### *Maßnahmen aufgrund einer Ausschreibung*

- (1) Werden Personen nach Artikel 32 ausfindig gemacht, so teilen die zuständigen Behörden dem ausschreibenden Mitgliedstaat vorbehaltlich des Absatzes 2 den Aufenthaltsort dieser Personen mit. Im Falle von vermissten Kindern oder Kindern, die unter Schutz gestellt werden müssen, konsultiert der vollziehende Mitgliedstaat sofort den ausschreibenden Mitgliedstaat, um unverzüglich die zur Wahrung des Wohls des Kindes zu treffenden Maßnahmen zu vereinbaren. Die zuständigen Behörden können die Personen in den in Artikel 32 Absatz 2 Buchstaben a und c genannten Fällen in Gewahrsam nehmen, um ihre Weiterreise zu verhindern, soweit es das nationale Recht erlaubt.
- (2) Bei volljährigen vermissten Personen, die ausfindig gemacht wurden, bedarf die Mitteilung von Daten, ausgenommen die Mitteilung von Daten zwischen den

---

elterliche Verantwortung und zur Aufhebung der Verordnung (EG) Nr. 1347/2000 (ABl. L 338 vom 23.12.2003, S. 1).

zuständigen Behörden, der Einwilligung des Betroffenen. Die zuständigen Behörden können jedoch einer 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 Daten 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 Kraft-, Wasser- oder Luftfahrzeuge mit einer Person verbunden sind, die Gegenstand einer Ausschreibung gemäß Absatz 1 ist, können Ausschreibungen zu den betreffenden Kraft-, Wasser- oder Luftfahrzeugen vorgenommen werden, um die Person ausfindig zu machen. In derartigen Fällen werden die Ausschreibung der Person und die Ausschreibung des Gegenstands im Einklang mit Artikel 60 miteinander verknüpft. Die technischen Vorschriften für die Eingabe, Aktualisierung, Löschung und Abfrage der in diesem Absatz genannten Daten werden im Wege von Durchführungsmaßnahmen nach dem in Artikel 72 Absatz 2 genannten Prüfverfahren festgelegt und entwickelt.

#### *Artikel 35*

#### *Maßnahme aufgrund einer Ausschreibung*

Die erbetenen Informationen werden dem ersuchenden 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) Daten in Bezug auf Personen oder Kraft-, Wasser- oder Luftfahrzeuge oder Container werden nach Maßgabe des nationalen Rechts des ausschreibenden Mitgliedstaats für verdeckte Kontrollen, für Ermittlungsanfragen oder für gezielte Kontrollen gemäß Artikel 37 Absatz 4 eingegeben.
- (2) Eine Ausschreibung dieser Art ist zulässig zur Strafverfolgung, zur Strafvollstreckung und zur Abwehr von Gefahren für die öffentliche Sicherheit, wenn
  - a) eindeutige Anhaltspunkte dafür vorliegen, dass eine Person eine schwere Straftat, insbesondere eine der in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten, plant oder begeht,
  - b) die in Artikel 37 Absatz 1 genannten Informationen zur Vollstreckung eines wegen einer schweren Straftat, insbesondere wegen einer der in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten, ergangenen strafrechtlichen Urteils erforderlich sind, oder
  - c) die Gesamtbeurteilung einer Person, insbesondere aufgrund der bisher von ihr begangenen Straftaten, erwarten lässt, dass sie auch künftig schwere Straftaten, insbesondere eine der in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten, begehen wird.
- (3) Eine Ausschreibung ist ferner, soweit das nationale Recht es erlaubt, auf Veranlassung der für die Sicherheit des Staates zuständigen Stellen zulässig, 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 nach diesem Absatz ausschreibende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten darüber. Jeder Mitgliedstaat bestimmt, an welche Behörden diese Informationen übermittelt werden.
- (4) Besteht ein eindeutiger Hinweis darauf, dass Kraft-, Wasser- oder Luftfahrzeuge oder Container im Zusammenhang mit schweren Straftaten nach Absatz 2 stehen oder mit den erheblichen Gefahren nach Absatz 3 verbunden sind, können Ausschreibungen zu diesen Kraft-, Wasser- oder Luftfahrzeugen oder Containern vorgenommen werden.
- (5) Besteht ein eindeutiger Hinweis darauf, dass amtliche Blankodokumente oder ausgestellte Ausweispapiere im Zusammenhang mit schweren Straftaten nach Absatz 2 stehen oder mit den erheblichen Gefahren nach Absatz 3 verbunden sind, können unabhängig von der Identität eines etwaigen ursprünglichen Inhabers des Ausweispapiers Ausschreibungen zu diesen Dokumenten vorgenommen werden. Die technischen Vorschriften für die Eingabe, Aktualisierung, Löschung und Abfrage der

in diesem Absatz genannten Daten werden im Wege von Durchführungsmaßnahmen nach dem in Artikel 72 Absatz 2 genannten Prüfverfahren festgelegt und entwickelt.

#### *Artikel 37*

##### *Maßnahmen aufgrund einer Ausschreibung*

- (1) Für verdeckte Kontrollen, für Ermittlungsanfragen oder für gezielte Kontrollen können bei Grenzkontrollen und sonstigen polizeilichen und zollrechtlichen Überprüfungen in einem Mitgliedstaat die nachstehenden Informationen ganz oder teilweise eingeholt und der ausschreibenden Stelle übermittelt werden:
  - a) die Tatsache, dass die ausgeschriebene Person, das ausgeschriebene Kraft-, Wasser- oder Luftfahrzeug, der ausgeschriebene Container oder das ausgeschriebene amtliche Blanko- bzw. Ausweispapier ausfindig gemacht wurde;
  - b) Ort, Zeit und Grund der Kontrolle bzw. Ermittlungsanfrage;
  - c) Route und Bestimmungsort;
  - d) Begleitpersonen des Betroffenen oder des Inhabers des amtlichen Blanko- oder Ausweispapiers bzw. Insassen des Kraft-, Wasser- oder Luftfahrzeugs, bei denen nach Lage der Dinge davon ausgegangen werden kann, dass sie mit den betreffenden Personen in Verbindung stehen;
  - e) die offengelegte Identität nebst Beschreibung der Person, die das ausgeschriebene amtliche Blankodokument bzw. Ausweispapier verwendet hat;
  - f) benutztes Kraft-, Wasser- oder Luftfahrzeug oder benutzter Container;
  - g) mitgeführte Gegenstände einschließlich Reisedokumente;
  - h) die Umstände, unter denen die Person, das Kraft-, Wasser- oder Luftfahrzeug, der Container, das amtliche Blankodokument oder das ausgestellte Ausweispapier aufgefunden wurde.
- (2) Informationen nach Absatz 1 werden im Wege des Austauschs von Zusatzinformationen übermittelt.
- (3) Je nach Umständen und im Einklang mit dem nationalen Recht umfasst eine verdeckte Kontrolle eine routinemäßige Kontrolle einer Person oder eines Gegenstands im Hinblick auf die Erhebung möglichst vieler der in Absatz 1 aufgeführten Informationen ohne Gefährdung des verdeckten Charakters der Kontrollmaßnahme.
- (4) Je nach Umständen und im Einklang mit dem nationalen Recht umfasst eine Ermittlungsanfrage eine eingehendere Überprüfung nebst Befragung der betreffenden Person. Wenn nach dem Recht eines Mitgliedstaats Ermittlungsanfragen nicht zulässig sind, erfolgt für diesen Mitgliedstaat stattdessen automatisch eine verdeckte Kontrolle.
- (5) Bei der gezielten Kontrolle können die Person, das Kraft-, Wasser- oder Luftfahrzeug, der Container oder die mitgeführten Gegenstände nach Maßgabe des nationalen Rechts zu den in Artikel 36 genannten Zwecken durchsucht werden. Durchsuchungen erfolgen nach Maßgabe des nationalen Rechts. Wenn nach dem Recht eines Mitgliedstaats gezielte Kontrollen nicht zulässig sind, erfolgt für diesen Mitgliedstaat stattdessen automatisch eine Ermittlungsanfrage.

# KAPITEL X

## SACHFAHNDUNGSAUSSCHREIBUNGEN ZUR SICHERSTELLUNG ODER BEWEISSICHERUNG IN STRAFVERFAHREN

### *Artikel 38*

#### *Ausschreibungsziele und -bedingungen*

- (1) Daten in Bezug auf Gegenstände, die zur Sicherstellung für Strafverfolgungszwecke oder zur Beweissicherung in Strafverfahren gesucht werden, werden in das SIS eingegeben.
- (2) Es werden folgende Kategorien von leicht identifizierbaren Gegenständen einbezogen:
  - a) Kraftfahrzeuge im Sinne des nationalen Rechts und unabhängig vom Antriebssystem;
  - b) Anhänger mit einem Leergewicht von mehr als 750 kg;
  - c) Wohnwagen;
  - d) Industrieausrüstung;
  - e) Wasserfahrzeuge;
  - f) Bootsmotoren;
  - g) Container;
  - h) Luftfahrzeuge;
  - i) Feuerwaffen;
  - j) gestohlene, unterschlagene oder auf sonstige Weise abhandengekommene amtliche Blankodokumente;
  - k) gestohlene, unterschlagene, auf sonstige Weise abhandengekommene, für ungültig erklärte oder gefälschte ausgefüllte Ausweispapiere wie Pässe, Personalausweise, Führerscheine, Aufenthaltstitel und Reisedokumente;
  - l) gestohlene, unterschlagene, auf sonstige Weise abhandengekommene, für ungültig erklärte oder gefälschte Kfz-Zulassungsbescheinigungen und Kfz-Kennzeichen;
  - m) registrierte Banknoten und gefälschte Banknoten;
  - n) technische Ausrüstung, Informationstechnik und andere hochwertige, leicht identifizierbare Gegenstände;
  - o) identifizierbare Teile von Kraftfahrzeugen;
  - p) identifizierbare Teile von Industrieausrüstung.
- (3) Die Definitionen neuer Unterkategorien von Gegenständen unter Absatz 2 Buchstabe n und die technischen Vorschriften für die Eingabe, Aktualisierung, Löschung und Abfrage der Daten nach Absatz 2 werden im Wege von Durchführungsmaßnahmen nach dem in Artikel 72 Absatz 2 genannten Prüfverfahren festgelegt und entwickelt.

*Artikel 39*  
*Maßnahme aufgrund einer Ausschreibung*

- (1) Ergibt eine Abfrage, dass eine Sachfahndungsausschreibung besteht, so beschlagnahmt die aufgreifende Stelle den betreffenden Gegenstand nach Maßgabe ihres nationalen Rechts und setzt sich mit der ausschreibenden Stelle 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 aufgreifende Mitgliedstaat ergreift die erbetenen Maßnahmen nach Maßgabe seines nationalen Rechts.

## **KAPITEL XI**

### **AUSSCHREIBUNGEN ZU UNBEKANNTEN GESUCHTEN PERSONEN ZWECKS IDENTIFIZIERUNG NACH MASSGABE DES NATIONALEN RECHTS UND SUCHE ANHAND BIOMETRISCHER DATEN**

*Artikel 40*  
*Ausschreibungen von unbekanntem gesuchten Personen zur Festnahme nach Maßgabe des nationalen Rechts*

In das SIS können auch daktylografische Daten von Personen eingegeben werden, die nicht mit den ausgeschriebenen Personen verbunden sind. Dies betrifft vollständige oder unvollständige Sätze von Finger- oder Handballenabdrücken, die an den untersuchten Tatorten schwerer oder terroristischer Straftaten vorgefunden wurden und bei denen eine hohe Wahrscheinlichkeit besteht, dass sie zum Täter gehören. Daktylografische Daten dieser Art werden als Daten der Kategorie „unbekannte verdächtige oder gesuchte Person“ gespeichert, sofern die zuständigen Behörden die Identität der Person nicht mithilfe anderer nationaler, europäischer oder internationaler Datenbanken ermitteln können.

*Artikel 41*  
*Maßnahmen aufgrund einer Ausschreibung*

Im Falle eines Treffers oder einer möglichen Übereinstimmung mit den nach Artikel 40 gespeicherten Daten wird die Identität der Person nach Maßgabe des nationalen Rechts und durch Überprüfung, ob die im SIS gespeicherten daktylografischen Daten zu der Person gehören, festgestellt. Die Mitgliedstaaten tauschen Zusatzinformationen aus, um die zügige Untersuchung des Falles zu erleichtern.

*Artikel 42*  
*Besondere Vorschriften für die Überprüfung oder Suche anhand von Lichtbildern,  
Gesichtsbildern, daktylografischen Daten und DNA-Profilen*

- (1) Um die Identität einer Person zu überprüfen, die durch eine alphanumerische Abfrage im SIS ermittelt wurde, werden Lichtbilder, Gesichtsbilder, daktylografische Daten und DNA-Profile aus dem SIS abgerufen.
- (2) Daktylografische Daten können auch zur Identifizierung einer Person verwendet werden. Wenn die Identität einer Person nicht durch andere Mittel festgestellt

werden kann, wird eine Suche anhand der im SIS gespeicherten daktylografischen Daten zu Identifizierungszwecken durchgeführt.

- (3) Die im SIS in Bezug auf Ausschreibungen nach Artikel 26, Artikel 34 Absatz 1 Buchstaben b und d und Artikel 36 gespeicherten daktylografischen Daten können auch anhand vollständiger oder unvollständiger Sätze von Finger- oder Handballenabdrücken abgefragt werden, die an untersuchten Tatorten vorgefunden wurden und mit hoher Wahrscheinlichkeit dem Täter zuzuordnen sind, sofern die zuständigen Behörden die Identität der betreffenden Person nicht mithilfe anderer nationaler, europäischer oder internationaler Datenbanken feststellen können.
- (4) Sobald die technische Möglichkeit besteht, dürfen Lichtbilder und Gesichtsbilder zur Identifizierung einer Person verwendet werden, wobei eine hochgradige Zuverlässigkeit der Identifizierung gewährleistet sein muss. Die Identifizierung anhand von Lichtbildern oder Gesichtsbildern wird nur an regulären Grenzübergangsstellen mit Self-Service-Systemen und automatisierten Grenzkontrollsystemen angewendet.

## **KAPITEL XII**

### **RECHT AUF ZUGRIFF UND ERFASSUNGSDAUER DER AUSSCHREIBUNGEN**

#### *Artikel 43*

#### *Zum Zugriff auf Ausschreibungen berechnete Behörden*

- (1) Der Zugriff auf die in das SIS eingegebenen Daten mit dem Recht, diese unmittelbar oder in einer Kopie der SIS-Daten abzufragen, ist solchen Stellen vorbehalten, die zuständig sind für
  - a) Grenzkontrollen gemäß der Verordnung (EU) Nr. 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex);
  - b) polizeiliche und zollrechtliche Überprüfungen in dem betreffenden Mitgliedstaat und deren Koordinierung durch hierfür bezeichnete Behörden;
  - c) sonstige Strafverfolgungsmaßnahmen zum Zwecke der Verhütung, Aufdeckung und Untersuchung von Straftaten in dem betreffenden Mitgliedstaat;
  - d) die Prüfung der Voraussetzungen für bzw. Entscheidungen über die Einreise und den Aufenthalt von Drittstaatsangehörigen im Hoheitsgebiet der Mitgliedstaaten, einschließlich der Aufenthaltstitel und Visa für den längerfristigen Aufenthalt sowie der Rückführung von Drittstaatsangehörigen.
- (2) Zudem können die nationalen Justizbehörden, einschließlich derjenigen, die für die Erhebung der öffentlichen Klage im Strafverfahren und justizielle Ermittlungen vor Anklageerhebung zuständig sind, sowie ihre Koordinierungsstellen zur Ausführung ihrer Aufgaben – wie in den nationalen Rechtsvorschriften vorgesehen – Zugriff auf die in das SIS eingegebenen Daten nehmen und diese unmittelbar abfragen.
- (3) Die zur Wahrnehmung der Aufgaben nach Absatz 1 Buchstabe c befugten Behörden können das Recht auf Zugang zu den im SIS gespeicherten Daten und auf deren Direktabfrage im Zuge der Erfüllung ihrer Aufgaben ausüben. Der Zugriff auf die

Daten durch diese Behörden erfolgt nach Maßgabe des Rechts des jeweiligen Mitgliedstaats.

- (4) Die in diesem Artikel genannten Behörden werden in die Liste nach Artikel 53 Absatz 8 aufgenommen.

*Artikel 44*  
*Kfz-Zulassungsstellen*

- (1) Die für die Ausstellung von Kfz-Zulassungsbescheinigungen im Sinne der Richtlinie 1999/37/EG<sup>75</sup> zuständigen Stellen der Mitgliedstaaten erhalten ausschließlich zur Überprüfung, ob das ihnen zur Zulassung vorgeführte Fahrzeug gestohlen, unterschlagen oder auf sonstige Weise abhandengekommen ist bzw. zur Beweissicherung in Strafverfahren gesucht wird, Zugang zu folgenden gemäß Artikel 38 Absatz 2 Buchstaben a, b, c und l dieser Verordnung im SIS gespeicherten Daten:
- a) Daten über Kraftfahrzeuge im Sinne des nationalen Rechts und unabhängig vom Antriebssystem;
  - b) Daten über Anhänger mit einem Leergewicht von mehr als 750 kg und Wohnwagen;
  - c) Daten über gestohlene, unterschlagene, auf sonstige Weise abhandengekommene oder für ungültig erklärte Kfz-Zulassungsbescheinigungen und Kfz-Kennzeichen.

Der Zugriff auf diese Daten durch die für die Ausstellung von Zulassungsbescheinigungen für Fahrzeuge zuständigen Stellen erfolgt nach Maßgabe des nationalen Rechts des betreffenden Mitgliedstaats.

- (2) Stellen gemäß Absatz 1, bei denen es sich um staatliche Stellen handelt, dürfen die im SIS gespeicherten Daten direkt abrufen.
- (3) Stellen gemäß Absatz 1, bei denen es sich um nichtstaatliche Stellen handelt, erhalten nur über eine Behörde nach Artikel 43 dieser Verordnung Zugang zu den im SIS gespeicherten Daten. 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 dieser Verordnung gilt nicht für den gemäß dem vorliegenden Artikel erfolgenden Datenabruf. Die Weitergabe von Informationen, die die Stellen gemäß Absatz 1 aufgrund des Zugangs zum SIS erhalten haben und die auf eine strafbare Handlung hindeuten, an die Polizei- oder Justizbehörden erfolgt nach Maßgabe des innerstaatlichen Rechts.

---

<sup>75</sup> Richtlinie 1999/37/EG des Rates vom 29. April 1999 über Zulassungsdokumente für Fahrzeuge (ABl. L 138 vom 1.6.1999, S. 57).

*Artikel 45*  
*Zulassungsstellen für Wasser- und Luftfahrzeuge*

- (1) Die für die Ausstellung von Zulassungsbescheinigungen für Wasserfahrzeuge (einschließlich Bootsmotoren) und Luftfahrzeuge oder für das Verkehrsmanagement von Wasser- und Luftfahrzeugen zuständigen Stellen erhalten ausschließlich zur Überprüfung, ob die ihnen zur Zulassung vorgeführten Wasserfahrzeuge (einschließlich Bootsmotoren), Luftfahrzeuge und Container beziehungsweise die ihrem Verkehrsmanagement unterliegenden Wasser- und Luftfahrzeuge und Container gestohlen, unterschlagen oder auf sonstige Weise abhandengekommen sind oder als Beweismittel in Strafverfahren gesucht werden, Zugang zu folgenden gemäß Artikel 38 Absatz 2 dieser Verordnung im SIS gespeicherten Daten:
- a) Daten über Wasserfahrzeuge;
  - b) Daten über Bootsmotoren;
  - c) Daten über Luftfahrzeuge.

Vorbehaltlich des Absatzes 2 erfolgt der Zugriff auf diese Daten durch die betreffenden Stellen nach Maßgabe des Rechts des jeweiligen Mitgliedstaats. Der Zugang zu den unter den Buchstaben a bis c dieses Absatzes genannten Daten wird auf die spezifische Zuständigkeit der betroffenen Dienststellen begrenzt.

- (2) Stellen gemäß Absatz 1, bei denen es sich um staatliche Stellen handelt, dürfen die im SIS gespeicherten Daten direkt abrufen.
- (3) Stellen gemäß Absatz 1, bei denen es sich um nichtstaatliche Stellen handelt, erhalten nur über eine Behörde nach Artikel 43 dieser Verordnung Zugang zu den im SIS gespeicherten Daten. 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 dieser Verordnung gilt nicht für den gemäß dem vorliegenden Artikel erfolgenden Datenabruf. Die Weitergabe von Informationen, die die Stellen gemäß Absatz 1 aufgrund des Zugangs zum SIS erhalten haben und die auf eine strafbare Handlung hindeuten, an die Polizei- oder Justizbehörden erfolgt nach Maßgabe des innerstaatlichen Rechts.

*Artikel 46*  
*Zugriff von Europol auf SIS-Daten*

- (1) Die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) hat im Rahmen ihres Mandats das Recht, auf die in das SIS eingegebenen Daten zuzugreifen und diese abzufragen.
- (2) Stellt sich bei einer Abfrage durch Europol heraus, dass eine Ausschreibung im SIS gespeichert ist, setzt Europol den ausschreibenden Mitgliedstaat über die in der Verordnung (EU) 2016/794 bestimmten Kanäle davon in Kenntnis.
- (3) Die Nutzung der durch eine Abfrage im SIS eingeholten Informationen unterliegt der Zustimmung des betreffenden Mitgliedstaats. Gestattet der Mitgliedstaat die Nutzung derartiger Informationen, so erfolgt die Verarbeitung dieser Informationen durch

Interpol nach Maßgabe der Verordnung (EU) 2016/794. Europol darf derartige Informationen nur mit Zustimmung des betreffenden Mitgliedstaats an Drittländer und -stellen weitergeben.

- (4) Nach Maßgabe der Verordnung (EU) 2016/794 kann Europol den betreffenden Mitgliedstaat um weitere Informationen ersuchen.
- (5) Europol
  - a) unterlässt es unbeschadet der Absätze 3, 4 und 6, Teile des SIS, zu denen sie Zugang hat, oder die hierin gespeicherten Daten, auf die sie Zugriff hat, mit einem von oder bei Europol betriebenen Computersystem 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) beschränkt den Zugriff auf die in das SIS eingegebenen Daten auf die eigens dazu ermächtigten Bediensteten von Europol;
  - c) nimmt die in Artikel 10 und Artikel 11 aufgeführten Maßnahmen an und wendet sie an;
  - d) gestattet dem Europäischen Datenschutzbeauftragten, die Tätigkeiten Europolis bei der Ausübung ihres Rechts auf Zugriff auf die in das SIS eingegebenen Daten und deren Abfrage zu überprüfen.
- (6) Die Daten dürfen nur zu technischen Zwecken vervielfältigt werden, sofern dies zur direkten Abfrage durch die ordnungsgemäß ermächtigten Europol-Bediensteten erforderlich ist. Diese Verordnung findet auf solche Kopien Anwendung. Die technische Kopie wird 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 auszulegen. Europol darf Ausschreibungsdaten oder ergänzende Daten, die von Mitgliedstaaten oder dem CS-SIS übermittelt wurden, nicht in andere Europol-Systeme kopieren.
- (7) Kopien nach Absatz 6, bei denen Off-line-Datenbanken entstehen, dürfen für einen Zeitraum von höchstens 48 Stunden erfasst werden. Diese Frist kann in einer Notsituation bis zu deren Beendigung verlängert werden. Europol meldet diese Verlängerungen dem Europäischen Datenschutzbeauftragten.
- (8) Europol kann Zusatzinformationen zu entsprechenden SIS-Ausschreibungen entgegennehmen und verarbeiten, sofern die in den Absätzen 2 bis 7 genannten Vorschriften für die Datenverarbeitung angemessen angewendet werden.
- (9) Für die Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung und der Sicherstellung der angemessenen Sicherheit und Integrität der Daten sollte Europol über jeden Zugriff auf das SIS und jede Abfrage im SIS Protokolle führen. Diese Protokolle und Dokumentationen sind nicht als das rechtswidrige Herunterladen oder Vervielfältigen eines Teils des SIS anzusehen.

*Artikel 47*  
*Zugriff von Eurojust auf SIS-Daten*

- (1) Die nationalen Mitglieder von Eurojust und die sie unterstützenden Personen haben im Rahmen ihres Mandats Zugriff auf die nach den Artikeln 26, 32, 34, 38 und 40 in das SIS eingegebenen Daten 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 das Mitglied den ausschreibenden Mitgliedstaat davon in Kenntnis.
- (3) Dieser Artikel ist nicht so auszulegen, dass er sich auf die im Beschluss 2002/187/JI enthaltenen Bestimmungen betreffend den Datenschutz und die Haftung wegen unbefugter oder unrichtiger Datenverarbeitung durch die nationalen Mitglieder von Eurojust oder die sie unterstützenden Personen oder auf die Befugnisse der gemäß jenem Beschluss eingesetzten Gemeinsamen Kontrollinstanz auswirkt.
- (4) Jeder Zugriff und jede Abfrage durch ein nationales Mitglied von Eurojust oder durch eine dieses Mitglied unterstützende Person sowie jede Nutzung der von ihnen abgerufenen Daten werden nach Maßgabe von Artikel 12 protokolliert.
- (5) Weder dürfen Teile des SIS mit einem der Erhebung und Verarbeitung von Daten dienenden, von oder bei Eurojust betriebenen Computersystem verbunden werden, noch dürfen die im SIS enthaltenen Daten, auf die die nationalen Mitglieder oder die sie unterstützenden Personen Zugriff haben, an ein solches Computersystem übermittelt werden. Kein Teil des SIS darf heruntergeladen werden. Die Protokollierung von Zugriffen und Abfragen ist nicht als unzulässiges Herunterladen oder Vervielfältigen von SIS-Daten auszulegen.
- (6) Der Zugriff auf die in das SIS eingegebenen Daten ist auf die nationalen Mitglieder und die sie unterstützenden Personen beschränkt und gilt nicht für die Eurojust-Bediensteten.
- (7) Es sind Maßnahmen zur Gewährleistung der Sicherheit und Geheimhaltung wie die in Artikel 10 und Artikel 11 aufgeführten anzunehmen und anzuwenden.

*Artikel 48*  
*Zugang von Mitgliedern der Europäischen Grenz- und Küstenwacheteams, der Teams von mit rückkehrbezogenen Aufgaben betrautem Personal sowie des Teams zur Unterstützung des Migrationsmanagements zu SIS-Daten*

- (1) Nach Artikel 40 Absatz 8 der Verordnung (EU) 2016/1624 haben die Mitglieder der Europäischen Grenz- und Küstenwacheteams, der Teams von mit rückkehrbezogenen Aufgaben betrautem Personal sowie der Teams zur Unterstützung der Migrationssteuerung im Rahmen ihres Mandats das Recht auf Zugang zu den in das SIS eingegebenen Daten und deren Abfrage.
- (2) Für die Mitglieder der Europäischen Grenz- und Küstenwacheteams, der Teams von mit rückkehrbezogenen Aufgaben betrautem Personal sowie der Teams zur Unterstützung der Migrationssteuerung erfolgt der Zugang zu und die Abfrage von in das SIS eingegebenen Daten gemäß Absatz 1 über die nach Artikel 49 Absatz 1 von der Europäischen Agentur für die Grenz- und Küstenwache eingerichtete und gewartete technische Schnittstelle.
- (3) Stellt sich bei der Abfrage durch ein Mitglied der Europäischen Grenz- und Küstenwacheteams, der Teams von mit rückkehrbezogenen Aufgaben betrautem

Personal oder des Teams zur Unterstützung der Migrationssteuerung heraus, dass eine Ausschreibung im SIS vorliegt, wird der ausschreibende Mitgliedstaat hiervon unterrichtet. Nach Artikel 40 der Verordnung (EU) 2016/1624 dürfen die Mitglieder der Teams in Reaktion auf eine Ausschreibung im SIS grundsätzlich nur auf Anweisung und in Gegenwart von Grenzschutzbeamten oder mit rückkehrbezogenen Aufgaben beteiligtem Personal des Einsatzmitgliedstaats handeln, in dem sie tätig sind. Der Einsatzmitgliedstaat kann Teammitglieder ermächtigen, in seinem Namen zu handeln.

- (4) Jeder Zugriff und jede Abfrage durch ein Mitglied der Europäischen Grenz- und Küstenwacheteams, der Teams von mit rückkehrbezogenen Aufgaben betrautem Personal oder des Teams zur Unterstützung der Migrationssteuerung wird nach Artikel 12 protokolliert, und jede Nutzung der von ihnen abgerufenen Daten wird protokolliert.
- (5) Der Zugang zu den in das SIS eingegebenen Daten gilt nur für ein Mitglied der Europäischen Grenz- und Küstenwacheteams, der Teams von mit rückkehrbezogenen Aufgaben betrautem Personal oder des Teams zur Unterstützung der Migrationssteuerung und wird nicht auf andere Teammitglieder ausgeweitet.
- (6) Es sind Maßnahmen zur Gewährleistung der Sicherheit und Geheimhaltung wie die in den Artikeln 10 und 11 aufgeführten anzunehmen und anzuwenden.

#### *Artikel 49*

##### *Zugriff der Europäischen Agentur für die Grenz- und Küstenwache auf SIS-Daten*

- (1) Für die Zwecke von Artikel 48 Absatz 1 und von Absatz 2 dieses Artikels ist die Europäische Agentur für die Grenz- und Küstenwache zuständig für die Einrichtung und Wartung einer technischen Schnittstelle, die eine direkte Verbindung mit dem zentralen SIS ermöglicht.
- (2) Damit sie die ihr durch die Verordnung über die Einrichtung eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS) übertragenen Aufgaben wahrnehmen kann, ist die Europäische Agentur für die Grenz- und Küstenwache berechtigt, im Einklang mit den Artikeln 26, 32, 34, 36 und 38 Absatz 2 Buchstaben j und k auf die in das SIS eingegebenen Daten zuzugreifen und diese abzufragen.
- (3) Stellt sich bei einer Überprüfung durch die Europäische Agentur für die Grenz- und Küstenwache heraus, dass eine Ausschreibung im SIS vorliegt, findet das Verfahren nach Artikel 22 der Verordnung zur Einrichtung eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS) Anwendung.
- (4) Dieser Artikel ist nicht so auszulegen, dass er sich auf die in der Verordnung (EU) 2016/1624 enthaltenen Bestimmungen betreffend den Datenschutz und die Haftung wegen unbefugter oder unrichtiger Datenverarbeitung durch die Europäische Agentur für die Grenz- und Küstenwache auswirkt.
- (5) Jeder Zugriff und jede Abfrage durch die Europäische Agentur für die Grenz- und Küstenwache wird nach Artikel 12 protokolliert und jede Nutzung der von ihr abgerufenen Daten aufgezeichnet.
- (6) Mit Ausnahme der Fälle, in denen es zur Wahrnehmung der Aufgaben für die Zwecke der Verordnung zur Einführung eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS) erforderlich ist, dürfen keine Teile des SIS mit einem der Erhebung und Verarbeitung von Daten dienenden Computersystem

verbunden werden, das von oder bei der Europäischen Agentur für die Grenz- und Küstenwache betrieben wird, noch dürfen die im SIS enthaltenen Daten, auf die die Europäische Agentur für die Grenz- und Küstenwache Zugriff hat, an ein solches System übermittelt werden. Kein Teil des SIS darf heruntergeladen werden. Die Protokollierung von Zugriffen und Abfragen ist nicht als Herunterladen oder Vervielfältigen von SIS-Daten auszulegen.

- (7) Die Europäische Agentur für die Grenz- und Küstenwache nimmt Maßnahmen nach den Artikeln 10 und 11 zur Gewährleistung der Sicherheit und Geheimhaltung an und wendet sie an.

#### *Artikel 50 Umfang des Zugriffs*

Endnutzer einschließlich Europol, die nationalen Mitglieder von Eurojust und die sie unterstützenden Personen sowie die Europäische Agentur für die Grenz- und Küstenwache dürfen nur auf Daten zugreifen, die zur Erfüllung ihrer Aufgaben erforderlich sind.

#### *Artikel 51 Erfassungsdauer von Ausschreibungen*

- (1) Die gemäß dieser Verordnung in das SIS eingegebenen Ausschreibungen werden nicht länger als für den verfolgten Zweck erforderlich gespeichert.
- (2) Der ausschreibende Mitgliedstaat prüft innerhalb von fünf Jahren nach Eingabe einer Ausschreibung in das SIS die Erforderlichkeit der weiteren Speicherung. Ausschreibungen für die Zwecke von Artikel 36 dieser Verordnung werden höchstens ein Jahr gespeichert.
- (3) Ausschreibungen zu amtlichen Blankodokumenten und ausgestellten Ausweispapieren gemäß Artikel 38 werden höchstens zehn Jahre gespeichert. Für Ausschreibungen von Gegenstandskategorien können im Wege gemäß dem Prüfverfahren nach Artikel 72 Absatz 2 angenommener Durchführungsmaßnahmen kürzere Speicherfristen festgelegt werden.
- (4) Jeder Mitgliedstaat bestimmt gegebenenfalls kürzere Prüffristen nach Maßgabe seines nationalen Rechts.
- (5) In den Fällen, in denen Mitarbeiter des SIRENE-Büros, die für die Koordinierung und Überprüfung der Qualität der Daten verantwortlich sind, erkennen, dass eine Personenausschreibung ihren Zweck erfüllt hat und aus dem SIS gelöscht werden sollte, setzen sie die Behörde, die die Ausschreibung eingegeben hat, hiervon in Kenntnis. Die Behörde verfügt über eine Frist von 30 Kalendertagen ab Eingang der Mitteilung, um anzuzeigen, dass die Ausschreibung gelöscht wurde oder wird, oder Gründe für die Beibehaltung der Ausschreibung anzugeben. Läuft die Frist von 30 Tagen ohne entsprechende Antwort ab, wird die Ausschreibung von den Mitarbeitern des SIRENE-Büros gelöscht. SIRENE-Büros melden wiederholt auftretende Probleme in diesem Bereich ihrer nationalen Aufsichtsbehörde.
- (6) Innerhalb der Prüffrist kann der ausschreibende Mitgliedstaat nach einer umfassenden individuellen Bewertung, die zu protokollieren ist, beschließen, die Ausschreibung noch beizubehalten, wenn dies für den der Ausschreibung zugrunde liegenden Zweck erforderlich ist. In diesem Fall gilt Absatz 2 auch für die

Verlängerung. Jede Verlängerung der Ausschreibungsdauer wird der CS-SIS mitgeteilt.

- (7) Die Ausschreibungen werden nach Ablauf der in Absatz 2 genannten Prüffrist automatisch gelöscht, es sei denn, der ausschreibende Mitgliedstaat hat der CS-SIS die Verlängerung der Ausschreibungsdauer nach Absatz 6 mitgeteilt. Die CS-SIS weist die Mitgliedstaaten mit einem Vorlauf von vier Monaten automatisch auf die im System programmierte Löschung hin.
- (8) Die Mitgliedstaaten führen Statistiken über die Zahl der Ausschreibungen, deren Erfassungsdauer nach Absatz 6 verlängert wurde.

## **KAPITEL XIII**

### **LÖSCHUNG VON AUSSCHREIBUNGEN**

#### *Artikel 52*

#### *Löschung von Ausschreibungen*

- (1) Ausschreibungen von Personen zum Zwecke der Übergabe- oder Auslieferungshaft nach Artikel 26 werden gelöscht, sobald die betreffende Person an die zuständigen Behörden des ausstellenden Mitgliedstaats übergeben oder ausgeliefert worden ist. Sie können zudem gelöscht werden, wenn die richterliche Entscheidung, die der Ausschreibung zugrunde lag, von der zuständigen Justizbehörde nach innerstaatlichem Recht aufgehoben worden ist.
- (2) Für die Löschung von Ausschreibungen von vermissten Personen gelten folgende Bestimmungen:
  - a) Ausschreibungen von vermissten Kindern gemäß Artikel 32 werden gelöscht, sobald
    - der betreffende Fall gelöst worden ist, beispielsweise wenn das betreffende Kind rückgeführt wurde oder die zuständigen Behörden im vollziehenden Mitgliedstaat entschieden haben, in wessen Obhut das Kind gegeben wird;
    - die Ausschreibung nach Artikel 51 abgelaufen ist;
    - die zuständige Behörde des ausschreibenden Mitgliedstaats die Löschung beschlossen hat; oder
    - das betreffende Kind ausfindig gemacht wurde.
  - b) Ausschreibungen von vermissten Erwachsenen gemäß Artikel 32, bei denen keine Schutzmaßnahmen ergriffen werden müssen, werden gelöscht, sobald
    - die zu ergreifende Maßnahme ausgeführt (d. h. der Aufenthaltsort vom vollziehenden Mitgliedstaat festgestellt) wurde;
    - die Ausschreibung nach Artikel 51 abgelaufen ist; oder
    - die zuständige Behörde des ausschreibenden Mitgliedstaats die Löschung beschlossen hat.

- c) Ausschreibungen von vermissten Erwachsenen gemäß Artikel 32, bei denen Schutzmaßnahmen ergriffen werden müssen, werden gelöscht, sobald
- die zu ergreifende Maßnahme ausgeführt (d. h. die Person unter Schutz gestellt) wurde;
  - die Ausschreibung nach Artikel 51 abgelaufen ist; oder
  - die zuständige Behörde des ausschreibenden Mitgliedstaats die Löschung beschlossen hat.

Wenn eine Person gemäß einer Entscheidung einer zuständigen Behörde interniert wurde, kann vorbehaltlich des innerstaatlichen Rechts eine Ausschreibung beibehalten werden, bis der Betreffende rückgeführt wurde.

- (3) Für die Löschung von Ausschreibungen von Personen, die im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesucht werden, gelten folgende Bestimmungen:

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. Wenn ein Tätigwerden auf der Grundlage der weitergeleiteten Informationen nicht möglich ist, informiert das SIRENE-Büro des ausschreibenden Mitgliedstaats das SIRENE-Büro des vollziehenden Mitgliedstaats, damit das Problem gelöst wird;
- b) die Ausschreibung nach Artikel 51 abgelaufen ist; oder
- c) die zuständige Behörde des ausschreibenden Mitgliedstaats die Löschung beschlossen hat.

Wenn in einem Mitgliedstaat ein Treffer erzielt wurde und die Adressdaten an den ausschreibenden Mitgliedstaat weitergeleitet wurden und ein anschließender Treffer in diesem Mitgliedstaat dieselben Adressdaten ergibt, wird der Treffer im vollziehenden Mitgliedstaat protokolliert, aber es werden weder die Adressdaten noch ergänzende Daten 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 prüft, ob die Ausschreibung beibehalten werden muss.

- (4) Für die Löschung von Ausschreibungen für verdeckte Kontrollen, Ermittlungsanfragen oder gezielte Kontrollen gelten folgende Bestimmungen:

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

- a) die Ausschreibung nach Artikel 51 abgelaufen ist;
- b) die zuständige Behörde des ausschreibenden Mitgliedstaats die Löschung beschlossen hat.

- (5) Für die Löschung von Sachfahndungsausschreibungen zur Sicherstellung oder Beweissicherung gelten folgende Bestimmungen:

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

- a) der betreffende Gegenstand sichergestellt oder eine entsprechende Maßnahme getroffen wurde und der erforderliche anschließende Austausch von Zusatzinformationen zwischen den SIRENE-Büros stattgefunden hat oder der betreffende Gegenstand einem anderen Gerichts- oder Verwaltungsverfahren unterworfen wird;
  - b) die Ausschreibung abgelaufen ist, oder
  - c) die zuständige Behörde des ausschreibenden Mitgliedstaats die Löschung beschlossen hat.
- (6) Ausschreibungen zu unbekannt gesuchten Personen gemäß Artikel 40 werden gelöscht, sobald
- a) die betreffende Person identifiziert worden ist; oder
  - b) die Ausschreibung abgelaufen ist.

## **KAPITEL XIV**

### **ALLGEMEINE BESTIMMUNGEN FÜR DIE DATENVERARBEITUNG**

#### *Artikel 53*

#### *Verarbeitung von SIS-Daten*

- (1) Die Mitgliedstaaten dürfen die in Artikel 20 genannten Daten nur für die Zwecke der in den Artikeln 26, 32, 34, 36, 38 und 40 genannten Ausschreibungskategorien verarbeiten.
- (2) Die Daten dürfen nur zu technischen Zwecken vervielfältigt werden, sofern dies zur direkten Abfrage durch die in Artikel 43 genannten Behörden erforderlich ist. Diese Verordnung findet auf solche Kopien 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 Off-line-Datenbanken entstehen, dürfen für einen Zeitraum von höchstens 48 Stunden erfasst werden. Diese Frist kann in einer Notsituation bis zu deren Beendigung verlängert werden.
- (4) Die Mitgliedstaaten führen ein aktuelles Verzeichnis dieser Kopien, stellen dieses Verzeichnis ihren nationalen Aufsichtsbehörden zur Verfügung und gewährleisten, dass die Bestimmungen dieser Verordnung, insbesondere Artikel 10, auf diese Kopien angewandt werden.
- (5) Der Zugriff auf die Daten wird nur im Rahmen der Zuständigkeiten der in Artikel 43 genannten nationalen Behörden und nur entsprechend bevollmächtigten Bediensteten gewährt.
- (6) 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 schwerwiegenden und unmittelbar bevorstehenden Gefahr für die öffentliche Sicherheit und Ordnung, aus schwerwiegenden Gründen der nationalen Sicherheit

oder zur Verhütung einer schweren Straftat erforderlich ist. Hierzu wird die vorherige Zustimmung des ausschreibenden Mitgliedstaats eingeholt.

- (7) Jede Nutzung der Daten, die den Absätzen 1 bis 6 nicht entspricht, wird nach dem nationalen Recht des jeweiligen Mitgliedstaats als Missbrauch bewertet.
- (8) Jeder Mitgliedstaat übermittelt der Agentur eine Liste seiner zuständigen Behörden, die nach dieser Verordnung berechtigt sind, die im SIS gespeicherten Daten unmittelbar abzufragen, sowie alle Änderungen dieser Liste. In der Liste wird für jede Behörde angegeben, welche Daten sie für welche Aufgaben abfragen darf. Die Agentur sorgt für die jährliche Veröffentlichung dieser Liste im *Amtsblatt der Europäischen Union*.
- (9) Soweit das Recht der Union keine besondere Regelung enthält, findet das nationale Recht des jeweiligen Mitgliedstaats auf die in sein NS.SIS eingegebenen Daten Anwendung.

#### *Artikel 54*

##### *SIS-Daten und nationale Dateien*

- (1) Artikel 53 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 53 Absatz 2 berührt nicht das Recht eines Mitgliedstaats, Daten zu einer bestimmten Ausschreibung, die dieser Mitgliedstaat im SIS vorgenommen hat, in nationalen Dateien zu speichern.

#### *Artikel 55*

##### *Information im Falle der Nichtausführung einer Ausschreibung*

Kann die erbetene Maßnahme nicht durchgeführt werden, so unterrichtet der ersuchte Mitgliedstaat den ausschreibenden Mitgliedstaat unverzüglich hiervon.

#### *Artikel 56*

##### *Qualität der im SIS verarbeiteten Daten*

- (1) Der ausschreibende Mitgliedstaat ist für die Richtigkeit und Aktualität der Daten sowie die Rechtmäßigkeit der Eingabe in das SIS verantwortlich.
- (2) Jede Änderung, Ergänzung, Berichtigung, Aktualisierung oder Löschung der Daten darf nur durch den ausschreibenden Mitgliedstaat vorgenommen werden.
- (3) Hat ein Mitgliedstaat, der die Ausschreibung nicht selbst vorgenommen hat, Anhaltspunkte dafür, dass Daten unrichtig oder unrechtmäßig gespeichert worden sind, so setzt er den ausschreibenden Mitgliedstaat so rasch wie möglich, spätestens aber zehn Tage, nachdem ihm die Anhaltspunkte bekannt geworden sind, im Wege des Austauschs von Zusatzinformationen davon in Kenntnis. Der ausschreibende Mitgliedstaat prüft die Mitteilung und berichtigt oder löscht erforderlichenfalls die Daten unverzüglich.
- (4) Können die Mitgliedstaaten sich nicht binnen zwei Monaten ab dem Zeitpunkt, zu dem die Anhaltspunkte nach Absatz 3 erstmals bekannt geworden sind, einigen, so

unterbreitet der Mitgliedstaat, der die Ausschreibung nicht vorgenommen hat, die Angelegenheit den betroffenen nationalen Aufsichtsbehörden zur Entscheidung.

- (5) Die Mitgliedstaaten tauschen Zusatzinformationen aus, wenn sich eine Person beschwert, nicht die in einer Ausschreibung gesuchte Person zu sein. Ergibt die Überprüfung, dass es sich tatsächlich um zwei unterschiedliche Personen handelt, so wird der Beschwerdeführer über die Maßnahmen nach Artikel 59 unterrichtet.
- (6) Wurde in Bezug auf eine Person bereits eine Ausschreibung in das SIS eingegeben, so stimmt sich der Mitgliedstaat, der eine weitere Ausschreibung vornimmt, mit dem Mitgliedstaat, der die erste Ausschreibung vorgenommen hat, über die Eingabe der Ausschreibungen ab. Diese Abstimmung erfolgt im Wege des Austauschs von Zusatzinformationen.

#### *Artikel 57*

##### *Sicherheitsvorfälle*

- (1) Jedes Ereignis, das sich auf die Sicherheit des Betriebs des SIS auswirkt bzw. auswirken und SIS-Daten beschädigen oder ihren Verlust herbeiführen kann, ist als Sicherheitsvorfall anzusehen; dies gilt insbesondere, wenn möglicherweise ein 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) Die Mitgliedstaaten setzen die Kommission, die Agentur und die nationale Aufsichtsbehörde von Sicherheitsvorfällen in Kenntnis. Die Agentur setzt die Kommission und den Europäischen Datenschutzbeauftragten von Sicherheitsvorfällen in Kenntnis.
- (4) Informationen über Sicherheitsvorfälle, die sich möglicherweise auf den Betrieb des SIS in einem Mitgliedstaat oder in der Agentur oder auf die Verfügbarkeit, die Integrität und die Geheimhaltung der von anderen Mitgliedstaaten eingegebenen oder übermittelten Daten auswirken, werden den Mitgliedstaaten im Einklang mit dem von der Agentur vorgelegten Sicherheitsvorfallmanagementplan übermittelt.

#### *Artikel 58*

##### *Unterscheidung von Personen mit ähnlichen Merkmalen*

Wird bei der Eingabe einer neuen Ausschreibung festgestellt, dass im SIS bereits eine Person mit denselben Identitätskriterien ausgeschrieben ist, so kommt folgendes Verfahren zur Anwendung:

- a) Das SIRENE-Büro setzt sich mit der ersuchenden Behörde in Verbindung, um zu überprüfen, ob es sich um dieselbe Person handelt.
- b) Stellt sich bei der Überprüfung heraus, dass es sich bei dem neu Ausgeschriebenen tatsächlich um die bereits im SIS ausgeschriebene Person handelt, so wendet das SIRENE-Büro das Verfahren für die Eingabe einer Mehrfachausschreibung nach Artikel 56 Absatz 6 an. Stellt sich bei der Überprüfung heraus, dass es sich hingegen um zwei verschiedene Personen handelt, so billigt das SIRENE-Büro das Ersuchen um Ausschreibung und fügt die erforderlichen Informationen zur Verhinderung einer falschen Identifizierung hinzu.

## Artikel 59

### *Ergänzende Daten zur Behandlung von Fällen des Missbrauchs der Identität einer Person*

- (1) Könnte eine Person, die tatsächlich Gegenstand einer Ausschreibung sein soll, mit einer Person, deren Identität missbraucht wurde, verwechselt werden, so ergänzt der ausschreibende Mitgliedstaat vorbehaltlich der ausdrücklichen Genehmigung der betroffenen Person die Ausschreibung um Daten über diese Person, um negativen Auswirkungen einer falschen Identifizierung vorzubeugen.
- (2) Daten über Personen, deren Identität missbraucht wurde, dürfen ausschließlich dazu verwendet werden,
  - a) der zuständigen Behörde zu ermöglichen, zwischen der Person, deren Identität missbraucht wurde, und der Person, die tatsächlich Gegenstand einer Ausschreibung sein soll, zu unterscheiden;
  - b) 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 dürfen in das SIS nur die folgenden personenbezogenen Daten eingegeben und weiterverarbeitet werden:
  - a) Nachname(n);
  - b) Vorname(n);
  - c) Geburtsname(n);
  - d) frühere Namen und Aliasnamen, gegebenenfalls in einem anderen Datensatz;
  - e) besondere objektive unveränderliche körperliche Merkmale;
  - f) Geburtsort;
  - g) Geburtsdatum;
  - h) Geschlecht
  - i) Lichtbilder und Gesichtsbilder;
  - j) Fingerabdrücke;
  - k) Staatsangehörigkeit(en);
  - l) Kategorie des Ausweispapiers der Person;
  - m) Ausstellungsland des Ausweispapiers der Person;
  - n) Anzahl der Ausweispapiere der Person;
  - o) Ausstellungsdatum des Ausweispapiers der Person;
  - p) Anschrift des Opfers;
  - q) Name des Vaters des Opfers;
  - r) Name der Mutter des Opfers.
- (4) Die technischen Vorschriften für die Eingabe und Weiterverarbeitung der Daten nach Absatz 3 werden im Wege von Durchführungsmaßnahmen nach dem in Artikel 72 Absatz 2 genannten Prüfverfahren festgelegt und weiterentwickelt.
- (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 Behörden, die Zugriff auf die entsprechende Ausschreibung haben, dürfen auf die Daten nach Absatz 3 zugreifen. Dieser Zugriff darf ausschließlich zur Verhinderung einer falschen Identifizierung erfolgen.

#### *Artikel 60*

##### *Verknüpfungen zwischen Ausschreibungen*

- (1) Ein Mitgliedstaat kann von ihm im SIS vorgenommene Ausschreibungen miteinander verknüpfen. Durch eine solche Verknüpfung werden zwei oder mehr Ausschreibungen miteinander verbunden.
- (2) Eine Verknüpfung wirkt sich nicht auf die jeweils zu ergreifende Maßnahme für jede verknüpfte Ausschreibung oder auf die Erfassungsdauer jeder der verknüpften Ausschreibungen aus.
- (3) Die Verknüpfung darf die in dieser Verordnung festgelegten Zugriffsrechte nicht beeinträchtigen. Behörden, die auf bestimmte Ausschreibungskategorien keinen Zugriff 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 technischen Vorschriften für die Verknüpfung von Ausschreibungen werden nach dem in Artikel 72 Absatz 2 genannten Prüfverfahren festgelegt und entwickelt.

#### *Artikel 61*

##### *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 vorgenommen 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 nationale Rechtsvorschriften geregelt.

*Artikel 62*  
*Übermittlung personenbezogener Daten an Dritte*

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

*Artikel 63*  
*Datenaustausch mit Interpol über gestohlene, unterschlagene, auf sonstige Weise abhandengekommene oder für ungültig erklärte Pässe*

- (1) Abweichend von Artikel 62 dürfen die Daten zu Passnummer, Ausstellungsland und Dokumentenart der in das SIS eingegebenen gestohlenen, unterschlagenen, auf sonstige Weise abhandengekommenen oder für ungültig erklärten Pässe mit Mitgliedern von Interpol ausgetauscht werden, indem eine Verbindung zwischen dem SIS und der Interpol-Datenbank für gestohlene, unterschlagene, auf sonstige Weise abhandengekommene oder für ungültig erklärte Reisedokumente hergestellt wird, sofern Interpol und die Europäische Union ein entsprechendes Übereinkommen schließen. In dem Übereinkommen wird vorgesehen, dass die von einem Mitgliedstaat eingegebenen Daten nur mit Zustimmung dieses Mitgliedstaats übermittelt werden dürfen.
- (2) In dem Übereinkommen nach Absatz 1 wird vorgesehen, dass die ausgetauschten Daten nur Interpol-Mitgliedern aus solchen Staaten zugänglich sind, in denen ein angemessener Schutz personenbezogener Daten sichergestellt ist. Vor Abschluss des Übereinkommens ersucht der Rat die Kommission um Stellungnahme in der Frage, ob Interpol und die Staaten, die Mitglieder zu Interpol abgestellt haben, bei der automatischen Verarbeitung personenbezogener Daten für einen angemessenen Schutz dieser Daten und die Wahrung der Grundrechte und der staatsbürgerlichen Freiheiten sorgen.
- (3) In dem Übereinkommen nach Absatz 1 kann ebenfalls vorgesehen werden, den Mitgliedstaaten im Einklang mit den einschlägigen Bestimmungen dieser Verordnung über im SIS erfasste Ausschreibungen von gestohlenen, unterschlagenen, auf sonstige Weise abhandengekommenen oder für ungültig erklärten Pässen über das SIS Zugriff auf Daten aus der Interpol-Datenbank für gestohlene oder auf sonstige Weise abhandengekommene Reisedokumente zu gewähren.

## **KAPITEL XV**

### **DATENSCHUTZ**

*Artikel 64*  
*Anwendbares Recht*

- (1) Die Verordnung (EG) Nr. 45/2001 gilt für die Verarbeitung personenbezogener Daten durch die Agentur im Rahmen dieser Verordnung.

- (2) Die Verordnung (EU) 2016/679 gilt für die Verarbeitung personenbezogener Daten, sofern nationale Vorschriften zur Umsetzung der Richtlinie (EU) 2016/680 keine Anwendung finden.
- (3) Auf die Verarbeitung von Daten durch die zuständigen nationalen Behörden für die Zwecke der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, finden die nationalen Vorschriften zur Umsetzung der Richtlinie (EU) 2016/680 Anwendung.

#### *Artikel 65*

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

- (1) Das Recht der betroffenen Personen, über die zu ihrer Person im SIS gespeicherten Daten Auskunft zu erhalten oder diese Daten berichtigen oder löschen zu lassen, richtet sich nach dem Recht des Mitgliedstaats, in dessen Hoheitsgebiet das Auskunftsrecht beansprucht wird.
- (2) Soweit es das nationale Recht vorsieht, entscheidet die nationale Aufsichtsbehörde, ob und in welcher Weise Auskunft erteilt wird.
- (3) Ein Mitgliedstaat, der die Ausschreibung nicht vorgenommen hat, darf Auskunft zu diesen Daten nur erteilen, wenn er vorher dem ausschreibenden Mitgliedstaat Gelegenheit zur Stellungnahme gegeben hat. Dies erfolgt im Wege des Austauschs von Zusatzinformationen.
- (4) Ein Mitgliedstaat trifft eine Entscheidung, das Auskunftsrecht der betroffenen Person vollständig oder teilweise einzuschränken, nach Maßgabe seiner nationalen Rechtsvorschriften, soweit und solange diese teilweise oder vollständige Einschränkung in einer demokratischen Gesellschaft erforderlich und notwendig ist und den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird,
  - a) zur Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden,
  - b) zur Gewährleistung, dass die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,
  - c) zum Schutz der öffentlichen Sicherheit,
  - d) zum Schutz der nationalen Sicherheit,
  - e) zum Schutz der Rechte und Freiheiten anderer.
- (5) Jeder hat das Recht, auf seine Person bezogene sachlich unrichtige Daten berichtigen oder unrechtmäßig gespeicherte Daten löschen zu lassen.
- (6) Die betroffene Person wird so schnell wie möglich informiert, spätestens jedoch 60 Tage nach Stellung ihres Antrags auf Auskunft oder früher, wenn die nationalen Rechtsvorschriften dies vorsehen.
- (7) Die betroffene Person wird so schnell wie möglich, spätestens jedoch drei Monate nach Stellung ihres Antrags auf Berichtigung oder Löschung, oder früher, wenn die nationalen Rechtsvorschriften dies vorsehen, davon in Kenntnis gesetzt, welche

Maßnahmen zur Wahrung ihres Rechts auf Berichtigung oder Löschung getroffen wurden.

*Artikel 66  
Rechtsbehelf*

- (1) Jeder hat das Recht, einen Rechtsbehelf wegen einer seine Person betreffenden Ausschreibung auf Auskunft, Berichtigung, Löschung oder Schadenersatz bei dem Gericht oder der Behörde einzulegen, das bzw. die nach dem Recht eines Mitgliedstaats zuständig ist.
- (2) Unbeschadet des Artikels 70 verpflichten sich die Mitgliedstaaten, unanfechtbare Entscheidungen der Gerichte oder Behörden nach Absatz 1 zu vollziehen.
- (3) Um einen umfassenden Überblick über die Funktionsweise von Rechtsbehelfen zu erhalten, entwickeln die nationalen Behörden ein statistisches Standardssystem für die jährliche Berichterstattung über
  - a) die Zahl der dem Verantwortlichen übermittelten Anträge betroffener Personen sowie die Zahl der Fälle, in denen der Zugang zu den Daten gewährt wurde;
  - b) die Zahl der der nationalen Aufsichtsbehörde übermittelten Anträge betroffener Personen sowie die Zahl der Fälle, in denen der Zugang zu den Daten gewährt wurde;
  - c) die Zahl der dem Verantwortlichen übermittelten Anträge auf Berichtigung unrichtiger Daten und Löschung unrechtmäßig gespeicherter Daten sowie die Zahl der Fälle, in denen die Daten berichtigt oder gelöscht wurden;
  - d) die Zahl der der nationalen Aufsichtsbehörde übermittelten Anträge auf Berichtigung unrichtiger Daten und Löschung unrechtmäßig gespeicherter Daten;
  - e) die Zahl der Fälle, in denen Klage vor Gericht erhoben wurde;
  - f) die Zahl der Fälle, in denen das Gericht teilweise oder vollständig zugunsten des Antragstellers entschied;
  - g) Bemerkungen zu Fällen der gegenseitigen Anerkennung rechtskräftiger Urteile der Gerichte oder Behörden anderer Mitgliedstaaten zu Ausschreibungen des ausschreibenden Mitgliedstaats.

Die Berichte der nationalen Aufsichtsbehörden werden an den Mechanismus der Zusammenarbeit nach Artikel 69 weitergeleitet.

*Artikel 67  
Überwachung der N.SIS*

- (1) Jeder Mitgliedstaat stellt sicher, dass die von ihm benannte(n), mit den Befugnissen nach Kapitel VI der Richtlinie (EU) 2016/680 oder Kapitel VI der Verordnung (EU) 2016/679 ausgestattete(n) nationale(n) Aufsichtsbehörde(n) unabhängig die Rechtmäßigkeit der Verarbeitung personenbezogener SIS-Daten in ihrem Hoheitsgebiet und deren Übermittlung aus ihrem Hoheitsgebiet sowie den Austausch und die Weiterverarbeitung von Zusatzinformationen überwacht beziehungsweise überwachen.

- (2) Die nationale Aufsichtsbehörde gewährleistet, dass die Datenverarbeitungsvorgänge in ihrem N.SIS mindestens alle vier Jahre nach internationalen Prüfungsstandards überprüft werden. Die Prüfung wird entweder von der nationalen Aufsichtsbehörde durchgeführt, oder die nationale Aufsichtsbehörde gibt die Prüfung unmittelbar bei einem unabhängigen Datenschutzprüfer in Auftrag. Der unabhängige Prüfer arbeitet jederzeit unter der Kontrolle und der Verantwortung der nationalen Aufsichtsbehörde.
- (3) Die Mitgliedstaaten gewährleisten, dass die nationale Aufsichtsbehörde über ausreichende Mittel zur Erfüllung der ihr nach dieser Verordnung übertragenen Aufgaben verfügt.

*Artikel 68*  
*Überwachung der Agentur*

- (1) Der Europäische Datenschutzbeauftragte stellt sicher, dass die Verarbeitung personenbezogener Daten durch die Agentur im Einklang mit dieser Verordnung erfolgt. Die Pflichten und Befugnisse nach den Artikeln 46 und 47 der Verordnung (EG) Nr. 45/2001 finden entsprechend Anwendung.
- (2) Der Europäische Datenschutzbeauftragte trägt dafür Sorge, dass die Agentur mindestens alle vier Jahre die Verarbeitung personenbezogener Daten nach internationalen Prüfungsstandards überprüft. Der Prüfbericht wird dem Europäischen Parlament, dem Rat, der Agentur, der Kommission und den nationalen Aufsichtsbehörden übermittelt. Die Agentur erhält Gelegenheit, vor der Annahme des Berichts eine Stellungnahme abzugeben.

*Artikel 69*  
*Zusammenarbeit zwischen den nationalen Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten*

- (1) Die nationalen Aufsichtsbehörden und der Europäische Datenschutzbeauftragte arbeiten im Rahmen ihrer jeweiligen Zuständigkeiten aktiv zusammen und gewährleisten eine koordinierte Überwachung des SIS.
- (2) Im Rahmen ihrer jeweiligen Zuständigkeiten tauschen sie einschlägige Informationen aus, unterstützen sich gegenseitig bei Überprüfungen und Inspektionen, prüfen Schwierigkeiten bei der Auslegung oder Anwendung dieser Verordnung oder anderer anwendbarer Rechtsakte der Union, gehen Problemen nach, die im Zuge der Wahrnehmung der unabhängigen Überwachung oder der Ausübung der Rechte betroffener Personen aufgetreten sind, arbeiten harmonisierte Vorschläge im Hinblick auf gemeinsame Lösungen für etwaige Probleme aus und fördern erforderlichenfalls die Sensibilisierung für die Datenschutzrechte.
- (3) Für die Zwecke des Absatzes 2 kommen die nationalen Aufsichtsbehörden und der Europäische Datenschutzbeauftragte mindestens zweimal jährlich zu einer Sitzung im Rahmen des mit der Verordnung (EU) 2016/679 eingerichteten Europäischen Datenschutzausschusses zusammen. Die Kosten und die Ausrichtung dieser Sitzungen übernimmt der mit der Verordnung (EU) 2016/679 eingerichtete Ausschuss. In der ersten Sitzung wird eine Geschäftsordnung angenommen. Weitere Arbeitsverfahren werden je nach Bedarf gemeinsam festgelegt.

- (4) Der mit der Verordnung (EU) 2016/679 eingerichtete Ausschuss übermittelt dem Europäischen Parlament, dem Rat und der Kommission alle zwei Jahre einen gemeinsamen Tätigkeitsbericht über die koordinierte Aufsicht.

## KAPITEL XVI

### HAFTUNG

#### *Artikel 70*

#### *Haftung*

- (1) Wird jemand beim Betrieb des N.SIS geschädigt, so haftet der betreffende Mitgliedstaat hierfür. Dies gilt auch, wenn der Schaden durch den ausschreibenden Mitgliedstaat verursacht worden ist, indem dieser sachlich unrichtige Daten eingegeben oder die Daten unrechtmäßig gespeichert hat.
- (2) Ist der in Anspruch genommene Mitgliedstaat nicht der ausschreibende Mitgliedstaat, so hat letzterer den geleisteten Ersatz auf Anforderung zu erstatten, es sei denn, die Nutzung der Daten durch den die Erstattung beantragenden Mitgliedstaat verstößt gegen diese Verordnung.
- (3) Für Schäden im SIS, die darauf zurückzuführen sind, dass ein Mitgliedstaat seinen aus dieser Verordnung erwachsenden Pflichten nicht nachgekommen ist, haftet der betreffende Mitgliedstaat, es sei denn, die Agentur oder andere am SIS beteiligte Mitgliedstaaten haben keine angemessenen Schritte unternommen, um den Schaden abzuwenden oder zu minimieren.

## KAPITEL XVII

### SCHLUSSBESTIMMUNGEN

#### *Artikel 71*

#### *Kontrolle und Statistiken*

- (1) Die Agentur 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 und Statistiken hat die Agentur Zugang zu den erforderlichen Informationen über die Verarbeitungsvorgänge im zentralen SIS.
- (3) Außerdem erstellt die Agentur tägliche, monatliche und jährliche Statistiken über die Zahl der Datensätze pro Ausschreibungskategorie, die jährliche Zahl der Treffer pro Ausschreibungskategorie und darüber, wie oft das SIS abgefragt und wie oft zwecks Eingabe, Aktualisierung oder Löschung einer Ausschreibung – insgesamt und nach Mitgliedstaaten aufgeschlüsselt – auf das System zugegriffen wurde. Die erstellten Statistiken dürfen keine personenbezogenen Daten enthalten. Der jährliche Statistikbericht wird veröffentlicht. Die Agentur erstellt zudem - für die

Mitgliedstaaten insgesamt sowie nach Mitgliedstaat aufgeschlüsselt - jährliche Statistiken über die Verwendung der Funktion, eine Ausschreibung nach Artikel 26 der vorliegenden Verordnung vorübergehend nicht abfragbar zu machen, einschließlich etwaiger Verlängerungen der Speicherfrist von 48 Stunden.

- (4) Die Mitgliedstaaten sowie Europol, Eurojust und die Europäische Agentur für die Grenz- und Küstenwache stellen der Agentur und der Kommission die Informationen zur Verfügung, die für die Erstellung der in den Absätzen 3, 7 und 8 genannten Berichte erforderlich sind. Diese Informationen umfassen separate Statistiken über die Zahl der Durchsuchungen 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 Bootsmotoren), Luftfahrzeuge und Container oder deren Verkehrsmanagement zuständig sind. In diesen Statistiken wird auch die Zahl der Treffer pro Ausschreibungskategorie ausgewiesen.
- (5) Die Agentur stellt den Mitgliedstaaten, der Kommission, Europol, Eurojust und der Europäischen Agentur für die Grenz- und Küstenwache alle von ihr erstellten Statistikberichte zur Verfügung. Um die Umsetzung der Rechtsakte der Union zu überwachen, kann die Kommission die Agentur ersuchen, regelmäßig oder ad hoc zusätzliche spezifische Statistikberichte über die Leistung oder die Nutzung der SIS- und der SIRENE-Kommunikation bereitzustellen.
- (6) Für die Zwecke der Absätze 3, 4 und 5 und des Artikel 15 Absatz 5 sorgt die Agentur an ihren technischen Standorten für die Einrichtung, die Implementierung und das Hosting eines Zentralregisters, das die Daten nach Absatz 3 und nach Artikel 15 Absatz 5 enthält, was eine Identifizierung einzelner Personen nicht ermöglicht und es der Kommission und den Agenturen nach Absatz 5 gestattet, maßgeschneiderte Berichte und Statistiken zu erhalten. Die Agentur gewährt den Mitgliedstaaten, der Kommission, Europol, Eurojust und der Europäischen Agentur für die Grenz- und Küstenwache Zugang zum Zentralregister in Form eines gesicherten Zugangs über die Kommunikationsinfrastruktur mit Zugangskontrollen und spezifischen Nutzerprofilen, die ausschließlich Berichterstattungs- und Statistikzwecken dienen.

Detaillierte Bestimmungen über den Betrieb des Zentralregisters und die für das Zentralregister geltenden Datenschutz- und Sicherheitsvorschriften werden im Wege von gemäß dem Prüfverfahren nach Artikel 72 Absatz 2 erlassenen Durchführungsmaßnahmen erlassen.

- (7) Zwei Jahre nach Inbetriebnahme des SIS und danach alle zwei Jahre unterbreitet die Agentur dem Europäischen Parlament und dem Rat einen Bericht über die technische Funktionsweise des zentralen SIS und der Kommunikationsinfrastruktur, einschließlich ihrer Sicherheit, und über den bilateralen und multilateralen Austausch von Zusatzinformationen zwischen den Mitgliedstaaten.
- (8) Drei Jahre nach Inbetriebnahme des SIS 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. Die Kommission übermittelt die Bewertung dem Europäischen Parlament und dem Rat.

*Artikel 72*  
*Ausschussverfahren*

- (1) Die Kommission wird von einem Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011 unterstützt.
- (2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

*Artikel 73*  
*Änderung der Verordnung (EU) Nr. 515/2014*

Die Verordnung (EU) Nr. 515/2014<sup>76</sup> wird wie folgt geändert:

In Artikel 6 wird folgender Absatz 6 angefügt:

„(6) Während der Entwicklungsphase erhalten die Mitgliedstaaten zusätzlich zu ihrem Grundbetrag eine pauschale Mittelzuweisung in Höhe von 36,8 Mio. EUR, die sie gänzlich zur Finanzierung ihrer nationalen SIS-Systeme verwenden, um deren rasche und effiziente Aktualisierung in Übereinstimmung mit der Implementierung des zentralen SIS gemäß der Verordnung (EU) 2018/...<sup>\*</sup> und der Verordnung (EU) 2018/...<sup>\*\*</sup> sicherzustellen.

<sup>\*</sup>Verordnung über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (ABl. ...).

<sup>\*\*</sup>Verordnung (EU) 2018/... über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen (ABl. ...).“

*Artikel 74*  
*Aufhebung*

Ab dem Tag des Beginns der Anwendung dieser Verordnung werden folgende Rechtsakte aufgehoben:

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);

Beschluss 533/2007/JI des Rates vom 12. Juli 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II);

Beschluss 2010/261/EU der Kommission vom 4. Mai 2010 über den Sicherheitsplan für das zentrale SIS II und die Kommunikationsinfrastruktur<sup>77</sup>.

---

<sup>76</sup> Verordnung (EU) Nr. 515/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 zur Schaffung eines Instruments für die finanzielle Unterstützung für Außengrenzen und Visa im Rahmen des Fonds für die innere Sicherheit und zur Aufhebung der Entscheidung Nr. 574/2007/EG (ABl. L 150 vom 20.5.2014, S. 143).

<sup>77</sup> 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).

*Artikel 75*  
*Inkrafttreten und Anwendbarkeit*

- (1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.
- (2) Sie gilt ab dem Zeitpunkt, der von der Kommission festgelegt wird, sobald
  - a) die erforderlichen Durchführungsbestimmungen erlassen wurden,
  - b) die Mitgliedstaaten der Kommission mitgeteilt haben, dass sie die erforderlichen technischen und rechtlichen Vorkehrungen zur Verarbeitung von SIS-Daten und zum Austausch von Zusatzinformationen gemäß dieser Verordnung getroffen haben,
  - c) die Agentur der Kommission mitgeteilt hat, dass sämtliche Tests im Hinblick auf die CS-SIS und die Interaktion zwischen N.SIS und CS-SIS abgeschlossen sind.
- (3) Diese Verordnung ist in allen ihren Teilen verbindlich und gilt gemäß dem Vertrag über die Arbeitsweise der Europäischen Union unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am [...]

*Im Namen des Europäischen Parlaments*  
*Der Präsident*

*Im Namen des Rates*  
*Der Präsident*

## FINANZBOGEN ZU RECHTSAKTEN

### **1. RAHMEN DES VORSCHLAGS/DER INITIATIVE**

- 1.1. Bezeichnung des Vorschlags/der Initiative
- 1.2. Politikbereich(e) in der ABM/ABB-Struktur
- 1.3. Art des Vorschlags/der Initiative
- 1.4. Ziel(e)
- 1.5. Begründung des Vorschlags/der Initiative
- 1.6. Laufzeit der Maßnahme und Dauer ihrer finanziellen Auswirkungen
- 1.7. Vorgeschlagene Methode(n) der Mittelverwaltung

### **2. VERWALTUNGSMASSNAHMEN**

- 2.1. Monitoring und Berichterstattung
- 2.2. Verwaltungs- und Kontrollsystem
- 2.3. Prävention von Betrug und Unregelmäßigkeiten

### **3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE**

- 3.1. Betroffene Rubrik(en) des mehrjährigen Finanzrahmens und Ausgabenlinie(n)
- 3.2. Geschätzte Auswirkungen auf die Ausgaben
  - 3.2.1. *Übersicht*
  - 3.2.2. *Geschätzte Auswirkungen auf die operativen Mittel*
  - 3.2.3. *Geschätzte Auswirkungen auf die Verwaltungsmittel*
  - 3.2.4. *Vereinbarkeit mit dem mehrjährigen Finanzrahmen*
  - 3.2.5. *Finanzierungsbeteiligung Dritter*
- 3.3. Geschätzte Auswirkungen auf die Einnahmen

## FINANZBOGEN ZU RECHTSAKTEN

### 1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

#### 1.1. Bezeichnung des Vorschlags/der Initiative

Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES 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 der Verordnung (EU) Nr. 515/2014 und zur Aufhebung der Verordnung (EG) Nr. 1986/2006, des Beschlusses 2007/533/JI des Rates und des Beschlusses 2010/261/EU der Kommission.

#### 1.2. Politikbereich(e) in der ABM/ABB-Struktur<sup>78</sup>

Politikbereich: Migration und Inneres (Titel 18)

#### 1.3. Art des Vorschlags/der Initiative

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

Der Vorschlag/Die Initiative betrifft **eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**<sup>79</sup>

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

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

#### 1.4. Ziel(e)

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

Ziel – Zerschlagung organisierter Kriminalität

Ziel – Eine starke EU-Reaktion zur Bekämpfung von Terrorismus und zur Verhinderung von Radikalisierung

Die Kommission hat mehrfach darauf hingewiesen, dass die Rechtsgrundlage des SIS überarbeitet werden muss, um die neuen Sicherheits- und Migrationsherausforderungen anzugehen. So kündigte die Kommission in der „Europäischen Sicherheitsagenda“<sup>80</sup> ihre Absicht an, das SIS 2015-2016 zu bewerten und zu prüfen, ob es neue operative Erfordernisse gibt, die Änderungen an der Rechtsgrundlage erforderlich machen. Zudem wurde in der Sicherheitsagenda betont, dass das SIS das Kernstück des polizeilichen Informationsaustauschs bildet und weiter gestärkt werden sollte. Jüngst erklärte die Kommission in ihrer Mitteilung „Solidere und intelligenter Informationssysteme für das Grenzmanagement und mehr Sicherheit“<sup>81</sup>, dass auf der Grundlage des Berichts über die Gesamtbewertung zusätzliche Funktionen des Systems im Hinblick auf die Vorlage von Vorschlägen

<sup>78</sup> ABM: Activity Based Management: maßnahmenbezogenes Management; ABB: Activity Based Budgeting: maßnahmenbezogene Budgetierung.

<sup>79</sup> Im Sinne des Artikels 54 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

<sup>80</sup> COM(2015) 185 final.

<sup>81</sup> COM(2016) 205 final.

zur Überarbeitung der Rechtsgrundlage des SIS erwogen werden. Schließlich schlug die Kommission am 20. April 2016 in ihrer Mitteilung „Umsetzung der Europäischen Sicherheitsagenda im Hinblick auf die Bekämpfung des Terrorismus und die Weichenstellung für eine echte und wirksame Sicherheitsunion“<sup>82</sup> eine Reihe von Änderungen am SIS vor, um dessen zusätzlichen Nutzen zu Gefahrenabwehr- und Strafverfolgungszwecken zu erhöhen.

Die von der Kommission durchgeführte Gesamtbewertung bestätigte, dass das SIS einen operativen Erfolg darstellt. Trotz der vielen mit dem System erzielten Erfolge wurden in der Bewertung jedoch eine Reihe von Empfehlungen zur Verbesserung der technischen und operativen Wirksamkeit und Effizienz des Systems gegeben.

Auf der Grundlage der Empfehlungen im Bericht über die Gesamtbewertung und in völliger Übereinstimmung mit den Zielen der Kommission, die in den oben genannten Mitteilungen und im Strategischen Plan 2016–2020 der GD Migration und Inneres<sup>83</sup> dargelegt werden, zielt dieser Vorschlag auf die Umsetzung von Folgendem:

- Ankündigung der Kommission, den Mehrwert des SIS zu Gefahrenabwehr- und Strafverfolgungszwecken im Hinblick auf die Reaktion auf neue Bedrohungen zu erhöhen;
- Empfehlungen für technische und verfahrensorientierte Änderungen, die aus der umfassenden Bewertung des SIS abgeleitet werden;
- Ersuchen von Endnutzern um technische Verbesserungen;
- vorläufige Erkenntnisse der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität in Bezug auf die Datenqualität.

#### 1.4.2. Einzelziel(e) und ABM/ABB-Tätigkeit(en)

##### Einzelziel Nr.

Managementplan der GD Migration und Inneres für 2017

Einzelziel Nr. 2.1 – Eine starke EU-Reaktion zur Bekämpfung von Terrorismus und zur Verhinderung von Radikalisierung

Einzelziel Nr. 2.2 – Zerschlagung von grenzübergreifender schwerer und organisierter Kriminalität

##### ABM/ABB-Tätigkeit(en):

Kapitel 18 02 – Innere Sicherheit

<sup>82</sup> COM(2016) 230 final.

<sup>83</sup> Ares(2016) 2231546 vom 12.5.2016.

### 1.4.3. Erwartete Ergebnisse und Auswirkungen

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

Hauptziel der geplanten rechtlichen und technischen Änderungen am SIS ist die höhere operative Wirksamkeit des Systems. Im Zuge der von der GD HOME im Zeitraum 2015-2016 durchgeführten Gesamtbewertung des SIS wurde empfohlen, das System technisch weiterzuentwickeln und die nationalen Verfahren für die Zusammenarbeit im Bereich Strafverfolgung zu harmonisieren.

Der neue Vorschlag enthält Maßnahmen, die den operativen und technischen Bedürfnissen der Endnutzer Rechnung tragen. Insbesondere werden durch neue Datenfelder für bereits bestehende Ausschreibungen Polizeibeamten alle für die wirksame Wahrnehmung ihrer Aufgaben notwendigen Informationen zur Verfügung stehen. Darüber hinaus wird in dem Vorschlag besonders hervorgehoben, wie wichtig die ununterbrochene Verfügbarkeit des SIS ist, da Ausfallzeiten die Arbeit von Bediensteten von Strafverfolgungsbehörden erheblich beeinträchtigen können. Zudem enthält der Vorschlag technische Änderungen, die das System wirksamer und einfacher gestalten.

Nach ihrer Verabschiedung und Umsetzung werden diese Vorschläge zudem zur Verbesserung der Betriebskontinuität beitragen, denn die Mitgliedstaaten werden verpflichtet sein, eine vollständige nationale Kopie oder eine Teilkopie sowie eine entsprechende Sicherungskopie zu erstellen. Hierdurch wird die dauerhafte volle Funktions- und Einsatzfähigkeit des Systems für Beamte vor Ort gewährleistet.

Mit dem Vorschlag werden neue biometrische Identifikatoren – Handballenabdrücke, Gesichtsbilder und DNA-Profile – für bestimmte Fälle eingeführt. Gemeinsam mit den geplanten Änderungen an den Artikeln 32 und 33 (Vermisstenausschreibungen), die die Eingabe präventiver Ausschreibungen und die Kategorisierung von vermissten Personen erlauben, wird dies erstens den Schutz unbegleiteter Minderjähriger erheblich stärken und zweitens ihre Identifizierung auf der Grundlage ihrer DNA-Profile oder der DNA-Profile ihrer Eltern und/oder Geschwister (nach deren Zustimmung) ermöglichen.

Die Behörden der Mitgliedstaaten werden dadurch auch in der Lage sein, Ausschreibungen zu unbekanntem im Zusammenhang mit einer Straftat gesuchten Personen lediglich auf der Grundlage von am Tatort hinterlassenen Fingerabdruckspuren oder Handballenabdrücken einzugeben. Dies ist aufgrund der derzeitigen rechtlichen und technischen Rahmenbedingungen nicht möglich und stellt daher eine bedeutende Entwicklung dar.

### 1.4.4. Leistungs- und Erfolgsindikatoren

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

Während der Aufrüstung des Systems:

Nach der Annahme des Vorschlags und der Verabschiedung der technischen Spezifikationen wird das SIS aufrüstet, um die nationalen Verfahren für die Nutzung des Systems besser zu harmonisieren, den Anwendungsbereich des Systems durch Hinzufügen neuer Elemente zu bestehenden Ausschreibungskategorien auszuweiten und technische Änderungen einzuführen, um für mehr Sicherheit und weniger Verwaltungsaufwand zu sorgen. Die Agentur eu-LISA wird für das Projektmanagement verantwortlich sein und die Aufrüstung des Systems

koordinieren. Sie wird eine Projektmanagementstruktur schaffen und einen detaillierten Zeitplan mit Etappenzielen für die Umsetzung der vorgeschlagenen Änderungen festlegen, anhand dessen die Kommission die Umsetzung des Vorschlags genau überwachen kann.

Einzelziel – Inbetriebnahme der aktualisierten Funktionen des SIS im Jahr 2020.

Indikator – erfolgreicher Abschluss umfassender Tests des überarbeiteten Systems vor seiner Einführung.

Nach Inbetriebnahme des Systems:

Nach Inbetriebnahme des Systems stellt eu-LISA sicher, dass Verfahren vorhanden sind, mit denen der Betrieb des Schengener Informationssystems anhand von Leistungs-, Kostenwirksamkeits-, Sicherheits- und Dienstqualitätszielen überwacht werden kann. Zwei Jahre nach Inbetriebnahme des SIS und danach alle zwei Jahre hat eu-LISA dem Europäischen Parlament und dem Rat einen Bericht über die technische Funktionsweise des zentralen SIS und der Kommunikationsinfrastruktur, einschließlich ihrer Sicherheit, sowie über den bilateralen und multilateralen Austausch von Zusatzinformationen zwischen den Mitgliedstaaten zu unterbreiten. Außerdem erstellt eu-LISA tägliche, monatliche und jährliche Statistiken über die Anzahl der Datensätze pro Ausschreibungskategorie, die jährliche Anzahl der Treffer pro Ausschreibungskategorie und darüber, wie oft das SIS abgefragt und wie oft darauf zwecks Eingabe, Aktualisierung oder Löschung einer Ausschreibung – insgesamt und nach Mitgliedstaaten aufgeschlüsselt – zugegriffen wurde. Darüber hinaus erstellt die Agentur – für die Mitgliedstaaten insgesamt sowie nach Mitgliedstaaten aufgeschlüsselt – jährliche Statistiken über die Nutzung der Funktion, eine Ausschreibung nach Artikel 26 der vorgeschlagenen Verordnung vorübergehend nicht abfragbar zu machen, einschließlich etwaiger Verlängerungen der Erfassungsdauer von 48 Stunden.

Drei Jahre nach der Inbetriebnahme des SIS und danach alle vier Jahre nimmt die Kommission eine Gesamtbewertung des zentralen SIS sowie des bilateralen und multilateralen Austausches 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. Die Kommission übermittelt die Bewertung dem Europäischen Parlament und dem Rat.

Einzelziel 1 – Zerschlagung organisierter Kriminalität.

Indikator – Inanspruchnahme des EU-Verfahrens zum Informationsaustausch. Dies lässt sich anhand einer höheren Zahl von Treffern im SIS messen. Indikatoren sind die statistischen Berichte, die von eu-LISA und den Mitgliedstaaten vorgelegt werden. Sie ermöglichen der Kommission zu bewerten, wie die neuen Funktionen des Systems genutzt werden.

Einzelziel Nr. 2 – Eine starke EU-Reaktion zur Bekämpfung von Terrorismus und zur Verhinderung von Radikalisierung.

Indikator – Erhöhung der Zahl der Ausschreibungen und Treffer, insbesondere in Bezug auf Artikel 36 Absatz 3 der vorgeschlagenen Verordnung bei Ausschreibungen von Personen und Gegenständen für verdeckte Kontrollen, Ermittlungsanfragen oder gezielte Kontrollen.

## 1.5. Begründung des Vorschlags/der Initiative

### 1.5.1. Kurz- oder langfristig zu deckender Bedarf

1. Beitrag zur Aufrechterhaltung eines hohen Maßes an Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts in der EU;
2. bessere Harmonisierung der nationalen Verfahren für die Nutzung des SIS;
3. Erweiterung der Liste institutioneller Nutzer mit Zugang zu SIS-Daten, indem Europol und der neuen Europäischen Agentur für die Grenz- und Küstenwache uneingeschränkter Zugang zu dem System gewährt wird;
4. Ergänzung der SIS-Ausschreibungen durch neue Elemente und neue Funktionen, um den Anwendungsbereich des Systems auszuweiten, eine Ausrichtung des Systems auf die derzeitige Sicherheitsumgebung zu ermöglichen, die Zusammenarbeit zwischen den Strafverfolgungs- und Sicherheitsbehörden der Mitgliedstaaten zu verbessern und den Verwaltungsaufwand zu reduzieren;
5. Beitrag zur vollständigen End-to-End-Nutzung des SIS, wozu nicht nur das zentrale System und die nationalen Systeme gehören; zudem ist nämlich zu gewährleisten, dass die Endnutzer alle zur Ausübung ihrer Aufgaben notwendigen Daten erhalten;
6. Verbesserung der Betriebskontinuität und Gewährleistung eines ununterbrochenen Betriebs des SIS auf zentraler und nationaler Ebene;
7. wirksamere Bekämpfung von internationaler Kriminalität, Terrorismus und Cyberkriminalität als direkt miteinander verbundene Bereiche mit stark grenzübergreifender Dimension.

### 1.5.2. Mehrwert aufgrund des Tätigwerdens der EU

Das SIS ist die wichtigste Sicherheitsdatenbank in Europa. Da keine Binnengrenzkontrollen stattfinden, können Verbrechen und Terrorismus nur auf europäischer Ebene wirksam bekämpft werden. Die Ziele dieses Vorschlags betreffen technische Verbesserungen zur Steigerung der Effizienz und der Wirksamkeit des Systems und zur Harmonisierung seiner Nutzung in allen teilnehmenden Mitgliedstaaten. Aufgrund des grenzübergreifenden Charakters dieser Ziele und der Herausforderungen bei der Gewährleistung eines wirksamen Informationsaustauschs zur Bewältigung der immer vielfältigeren Bedrohungen ist die EU am besten aufgestellt, um Lösungen für diese Probleme vorzuschlagen. Die angestrebte verbesserte Effizienz und harmonisierte Nutzung des SIS, d. h. die Erhöhung der Menge, der Qualität und der Geschwindigkeit des Informationsaustauschs über ein zentrales IT-Großsystem, das von einer Regulierungsagentur (eu-LISA) verwaltet wird, sind Ziele, die nicht von den Mitgliedstaaten allein erreicht werden können und ein Tätigwerden auf EU-Ebene erfordern. Wenn die gegenwärtigen Probleme nicht angegangen werden, erfolgt der Betrieb des SIS weiterhin im Einklang mit den derzeit geltenden Vorschriften; somit blieben Möglichkeiten zur Maximierung der Effizienz und des Mehrwerts für die EU, wie sie im Zuge der Bewertung des SIS und seiner Nutzung durch die Mitgliedstaaten festgestellt wurden, ungenutzt.

Allein im Jahr 2015 griffen die zuständigen Behörden der Mitgliedstaaten fast 2,9 Milliarden Mal auf das System zu, was ein eindeutiger Beweis für den entscheidenden Beitrag des Systems zur Zusammenarbeit im Bereich der

Strafverfolgung im Schengen-Raum ist. Dieser intensive Informationsaustausch zwischen Mitgliedstaaten wäre durch dezentrale nationale Lösungen nicht erreicht worden; zudem wäre es unmöglich gewesen, diese Ergebnisse auf Ebene der Mitgliedstaaten zu erzielen. Hinzu kommt, dass das SIS für die Zwecke der Terrorismusbekämpfung erwiesenermaßen das wirksamste Instrument des Informationsaustauschs ist und einen EU-Mehrwert bietet, da es den nationalen Sicherheitsdiensten ermöglicht, rasch, vertraulich und effizient zusammenzuarbeiten. Die neuen Vorschläge werden den Informationsaustausch und die Zusammenarbeit zwischen den EU-Mitgliedstaaten weiter erleichtern. Zudem erhalten Europol und die neue Europäische Agentur für die Grenz- und Küstenwache im Rahmen ihrer Zuständigkeiten uneingeschränkten Zugang zu dem System, was ein eindeutiger Hinweis auf den Mehrwert aufgrund des Tätigwerdens der EU ist.

### 1.5.3. *Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse*

1. Die Entwicklungsphase sollte erst beginnen, nachdem die Betriebsanforderungen und die Anforderungen der Endnutzer in vollem Umfang bestimmt wurden. Die Entwicklung kann nur erfolgen, wenn die zugrunde liegenden Rechtsinstrumente, in denen Zweck, Anwendungsbereich, Funktionen und technische Einzelheiten festgelegt sind, endgültig angenommen wurden.

2. Die Kommission konsultierte (und konsultiert) regelmäßig die Beteiligten, darunter auch die Vertreter der Mitgliedstaaten im SIS/VIS-Ausschuss im Rahmen des Ausschussverfahrens. Diesem Ausschuss gehören Vertreter der Mitgliedstaaten an, die sowohl mit operativen SIRENE-Fragen (grenzübergreifende Zusammenarbeit in Bezug auf das SIS) als auch mit technischen Fragen zur Entwicklung und Wartung des SIS und der betreffenden SIRENE-Anwendung befasst sind. Die in dieser Verordnung vorgeschlagenen Änderungen wurden sehr transparent und umfassend in speziellen Sitzungen und Workshops erörtert. Intern richtete die Kommission eine dienststellenübergreifende Lenkungsgruppe ein, der Mitarbeiter des Generalsekretariats und der Generaldirektionen Migration und Inneres, Justiz und Verbraucher, Humanressourcen und Sicherheit sowie Informatik angehörten. Diese Lenkungsgruppe begleitete den Bewertungsprozess und bot erforderlichenfalls Orientierungshilfe.

3. Die Kommission holte auch externes Expertenwissen durch zwei Studien ein, deren Ergebnisse bei der Ausarbeitung dieses Vorschlags Berücksichtigung fanden:

- „SIS Technical Assessment“ (Technische Beurteilung des SIS) – in dieser Studie wurden die wichtigsten Probleme des SIS und der künftige zu berücksichtigende Bedarf ermittelt; dabei wurden Bedenken im Hinblick auf die Maximierung der Betriebskontinuität und die Anpassungsfähigkeit der gesamten Architektur im Zusammenhang mit den wachsenden Kapazitätserfordernissen formuliert.

- „ICT Impact Assessment of Possible Improvements to the SIS II Architecture“ (Informations- und kommunikationstechnologische Folgenabschätzung möglicher Verbesserungen an der Architektur des SIS II) – in dieser Studie wurden die aktuellen Betriebskosten des SIS auf nationaler Ebene beurteilt und drei mögliche technische Szenarien zur Verbesserung des Systems bewertet. Sämtliche Szenarien beinhalten eine Reihe von technischen Vorschlägen für Verbesserungen des zentralen Systems und der Gesamtarchitektur.

#### 1.5.4. Vereinbarkeit mit anderen Finanzierungsinstrumenten sowie mögliche Synergieeffekte

Mit diesem Vorschlag sollen die in der Mitteilung „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“<sup>84</sup> vom 6. April 2016 vorgesehenen Maßnahmen umgesetzt werden, in der dargelegt wird, dass die EU ihre IT-Systeme, ihre Datenarchitektur und den Informationsaustausch im Bereich Strafverfolgung, Terrorismusbekämpfung und Grenzmanagement verstärken und verbessern muss.

Zudem ist dieser Vorschlag mit anderen Bereichen der Unionspolitik eng verbunden und ergänzt diese, nämlich:

- a) die innere Sicherheit wie sie in der Europäischen Sicherheitsagenda<sup>85</sup> hervorgehoben wird, um schwere und terroristische Straftaten zu verhüten, aufzudecken, zu ermitteln und zu verfolgen, indem Strafverfolgungsbehörden ermöglicht wird, personenbezogene Daten von Personen, die unter dem Verdacht stehen, an terroristischen Handlungen oder schweren Straftaten beteiligt zu sein, zu verarbeiten;
- b) den Datenschutz insofern, als dieser Vorschlag den Schutz des Grundrechts auf Achtung des Privatlebens der Personen, deren personenbezogene Daten im SIS verarbeitet werden, gewährleisten muss.

Der Vorschlag steht zudem im Einklang mit den bestehenden Rechtsvorschriften der Europäischen Union betreffend:

- a) die Europäische Grenz- und Küstenwache<sup>86</sup> in Bezug auf erstens die Möglichkeit der Bediensteten der Agentur, Risikoanalysen durchzuführen, und zweitens ihren Zugang zum SIS für die Zwecke des vorgeschlagenen Systems ETIAS. Der Vorschlag zielt auch darauf ab, den Teams der Europäischen Grenz- und Küstenwache, den Teams von mit rückkehrbezogenen Aufgaben betrautem Personal und den Mitgliedern der Teams zur Unterstützung des Migrationsmanagements, die im Rahmen ihres Auftrags berechtigt sind, auf die in das SIS eingegebenen Daten zuzugreifen und diese abzufragen, eine technische Schnittstelle für den Zugang zum SIS bereitzustellen;
- b) Europol, insofern, als mit diesem Vorschlag der Agentur Europol im Rahmen ihres Mandats zusätzliche Rechte auf Zugang zu den in das SIS eingegebenen Daten und deren Abfrage gewährt werden;
- c) Prüm<sup>87</sup>, insofern, als die in diesem Vorschlag vorgesehenen Maßnahmen, die die Identifizierung von Personen auf der Grundlage von Fingerabdrücken (sowie von

<sup>84</sup> COM(2016) 205 final.

<sup>85</sup> COM(2015) 185 final.

<sup>86</sup> 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).

<sup>87</sup> Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6.8.2008, S. 1) und Beschluss 2008/616/JI des Rates vom 23. Juni 2008 zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden

Gesichtsbildern und DNA-Profilen) ermöglichen, die geltenden Prümer Bestimmungen über den grenzüberschreitenden Online-Zugriff auf die benannten nationalen DNA-Datenbanken und automatisierte daktyloskopische Identifizierungssysteme ergänzen.

Der Vorschlag steht zudem im Einklang mit künftigen Rechtsvorschriften der Europäischen Union in Bezug auf:

- a) den Grenzschutz an den Außengrenzen. Der Vorschlag ergänzt das geplante neue Prinzip im Schengener Grenzkodex, wonach alle Reisenden, einschließlich der Unionsbürger, bei der Einreise in den und der Ausreise aus dem Schengen-Raum systematischen Kontrollen anhand der einschlägigen Datenbanken unterzogen werden, das als Reaktion auf das Phänomen ausländischer terroristischer Kämpfer eingeführt wurde;
- b) das Einreise-/Ausreisensystem<sup>88</sup> (EES), insofern, als in dem Vorschlag die vorgeschlagene Nutzung einer Kombination aus Fingerabdruck und Gesichtsbild als biometrische Identifikatoren für den Betrieb des EES berücksichtigt wird;
- c) das ETIAS, insofern, als der Vorschlag dem vorgeschlagenen System ETIAS Rechnung trägt, das eine umfassende Sicherheitsbeurteilung vorsieht, einschließlich einer Überprüfung von Drittstaatsangehörigen im SIS, die in die Europäische Union einreisen möchten.

---

Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6.8.2008, S. 12).

<sup>88</sup>

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Einreise-/Ausreisensystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten der Europäischen Union und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung der Verordnung (EG) Nr. 767/2008 (COM(2016) 194 final).

## 1.6. Laufzeit der Maßnahme und Dauer ihrer finanziellen Auswirkungen

- Vorschlag/Initiative mit **befristeter Laufzeit**
  - Laufzeit: [TT/MM]JJJJ bis [TT/MM]JJJJ
  - Finanzielle Auswirkungen: JJJJ bis JJJJ
- Vorschlag/Initiative mit **unbefristeter Laufzeit**
  - Vorbereitungszeitraum 2017
  - Anlaufphase von 2018 bis 2020,
  - anschließend reguläre Umsetzung.

## 1.7. Vorgeschlagene Methode(n) der Mittelverwaltung<sup>89</sup>

- Direkte Verwaltung** durch die Kommission
  - durch ihre Dienststellen, einschließlich ihres Personals in den Delegationen der Union;
  - durch Exekutivagenturen.
- Geteilte Verwaltung** mit Mitgliedstaaten
- Indirekte Verwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:
  - Drittländer oder die von ihnen benannten Einrichtungen;
  - internationale Einrichtungen und deren Agenturen (bitte angeben);
  - die EIB und den Europäischen Investitionsfonds;
  - Einrichtungen im Sinne der Artikel 208 und 209 der Haushaltsordnung;
  - öffentlich-rechtliche Körperschaften;
  - privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern sie ausreichende Finanzsicherheiten bieten;
  - privatrechtliche Einrichtungen eines Mitgliedstaats, die mit der Einrichtung einer öffentlich-privaten Partnerschaft betraut werden und die ausreichende Finanzsicherheiten bieten;
  - Personen, die mit der Durchführung bestimmter Maßnahmen im Bereich der GASP im Rahmen des Titels V EUV betraut und in dem maßgeblichen Basisrechtsakt benannt sind.
  - *Falls mehrere Methoden der Mittelverwaltung angegeben werden, ist dies unter „Bemerkungen“ näher zu erläutern.*

### Bemerkungen

Die Kommission wird für die Gesamtverwaltung der Maßnahme, eu-LISA für die Entwicklung, den Betrieb und die Wartung des Systems zuständig sein.

**Das SIS stellt ein einziges Informationssystem dar. Folglich sollten die in den beiden Vorschlägen (also in dem vorliegenden und dem Vorschlag für eine Verordnung über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems**

<sup>89</sup> Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb (in französischer und englischer Sprache): [http://www.cc.cec/budg/man/budgmanag/budgmanag\\_en.html](http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html)

**(SIS) im Bereich der Grenzkontrollen) vorgesehenen Ausgaben nicht als zwei separate Beträge sondern als ein einziger Betrag betrachtet werden. Die Auswirkungen der für die Umsetzung der beiden Vorschläge erforderlichen Änderungen auf den Haushalt sind in einem einzigen Finanzbogen enthalten.**

## 2. VERWALTUNGSMASSNAHMEN

### 2.1. Monitoring und Berichterstattung

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

Die Kommission, die Mitgliedstaaten und die Agentur werden die Nutzung des SIS regelmäßig überprüfen und kontrollieren, um sicherzustellen, dass das System weiterhin wirksam und effizient funktioniert. Wie in diesem Vorschlag vorgesehen, wird die Kommission bei der Durchführung der technischen und operativen Maßnahmen von einem Ausschuss unterstützt.

Die vorgeschlagene Verordnung sieht zudem in Artikel 71 Absätze 7 und 8 ein formelles, regelmäßiges Überprüfungs- und Bewertungsverfahren vor.

Alle zwei Jahre hat eu-LISA dem Europäischen Parlament und dem Rat einen Bericht über die technische Funktionsweise – einschließlich der Sicherheit – des SIS und der diesbezüglichen Kommunikationsinfrastruktur sowie über den bilateralen und multilateralen Austausch von Zusatzinformationen zwischen den Mitgliedstaaten zu unterbreiten.

Darüber hinaus hat die Kommission alle vier Jahre eine Gesamtbewertung des SIS und des Informationsaustauschs zwischen den Mitgliedstaaten vorzunehmen, die sie dem Parlament und dem Rat übermittelt. Dabei

- a) misst sie die Ergebnisse an den Zielen,
- b) überprüft sie, ob die grundlegenden Prinzipien des Systems weiterhin Gültigkeit haben,
- c) prüft sie, inwieweit die Verordnung auf das zentrale System angewandt wird,
- d) bewertet sie die Sicherheit des zentralen Systems,
- e) untersucht sie die Auswirkungen auf den künftigen Betrieb des Systems.

Des Weiteren ist eu-LISA nunmehr gehalten, tägliche, monatliche und jährliche Statistiken über die Nutzung des SIS zu erstellen und somit für eine kontinuierliche Überwachung des Systems und seiner Funktionsweise anhand von Zielen zu sorgen.

### 2.2. Verwaltungs- und Kontrollsystem

#### 2.2.1. Ermittelte Risiken

Folgende Risiken wurden ermittelt:

1. Schwierigkeiten, die sich insofern für eu-LISA ergeben könnten, als zum einen die im vorliegenden Vorschlag dargelegten Systementwicklungen zeitgleich mit anderen laufenden Entwicklungen (z. B. Implementierung des AFIS im SIS) und zum anderen künftige Entwicklungen (z. B. Einreise-/Ausreisensystem, ETIAS und Aufrüstung von Eurodac) umgesetzt werden müssen. Dieses Risiko könnte eingedämmt werden, indem sichergestellt wird, dass eu-LISA über ausreichend Personal und Ressourcen verfügt, um diese Aufgaben auszuführen und für die laufende Verwaltung im Zusammenhang mit dem für die Wartung des Systems zuständigen Auftragnehmer zu sorgen.

2. Schwierigkeiten für die Mitgliedstaaten:

2.1 Hierbei handelt es sich vorwiegend um finanzielle Schwierigkeiten. Die Legislativvorschläge enthalten beispielsweise die Verpflichtung, eine nationale

Teilkopie in jedem N.SIS II zu erstellen. Mitgliedstaaten, die diese Kopie noch nicht erstellt haben, werden die betreffende Investition vornehmen müssen. Außerdem muss das Schnittstellenkontrolldokument vollständig auf nationaler Ebene umgesetzt werden. Mitgliedstaaten, die dies noch nicht getan haben, müssen die betreffenden Ausgaben in den Haushalten der entsprechenden Ministerien einplanen. Dieses Risiko könnte eingedämmt werden, indem den Mitgliedstaaten EU-Mittel bereitgestellt werden, beispielsweise aus dem Fonds für die innere Sicherheit (ISF).

2.2 Die nationalen Systeme müssen mit den Anforderungen auf zentraler Ebene in Einklang gebracht werden; die diesbezüglichen Gespräche mit den Mitgliedstaaten könnten zu Entwicklungsverzögerungen führen. Dieses Risiko könnte eingedämmt werden, indem dieser Punkt frühzeitig mit den Mitgliedstaaten erörtert wird, um sicherzustellen, dass die entsprechenden Maßnahmen zum richtigen Zeitpunkt getroffen werden können.

#### 2.2.2. *Angaben zum Aufbau des Systems der internen Kontrolle*

Die Zuständigkeit für die zentralen Komponenten des SIS liegt bei eu-LISA. Um eine bessere Überwachung der Nutzung des SIS für die Analyse von Trends im Zusammenhang mit Migrationsdruck, Grenzmanagement und Straftaten zu ermöglichen, sollte eu-LISA in der Lage sein, ein dem neuesten Stand der Technik entsprechendes System für die statistische Berichterstattung gegenüber den Mitgliedstaaten und der Kommission zu entwickeln.

Die Rechnungsführung von eu-LISA wird dem Rechnungshof zur Genehmigung vorgelegt und ist Gegenstand des Entlastungsverfahrens. Der Interne Auditdienst der Kommission führt in Absprache mit dem internen Prüfer von eu-LISA Prüfungen durch.

#### 2.2.3. *Abschätzung der Kosten und des Nutzens der Kontrollen sowie Bewertung des voraussichtlichen Fehlerrisikos*

entfällt

### 2.3. **Prävention von Betrug und Unregelmäßigkeiten**

*Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen vorhanden oder vorgesehen sind.*

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

1. Zur Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen findet die Verordnung (EG) Nr. 1073/1999 Anwendung.
2. Die Agentur tritt der Interinstitutionellen Vereinbarung über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) bei und erlässt unverzüglich die für alle Beschäftigten der Agentur geltenden einschlägigen Vorschriften.
3. Die Finanzierungsbeschlüsse sowie die sich daraus ergebenden Durchführungsvereinbarungen und -instrumente sehen ausdrücklich vor, dass der Rechnungshof und das OLAF erforderlichenfalls Vor-Ort-Kontrollen bei den Empfängern der Mittel der Agentur und bei den verteilenden Stellen durchführen können.

Gemäß diesen Bestimmungen fasste der Verwaltungsrat der Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der

Sicherheit und des Rechts am 28. Juni 2012 den Beschluss über die Bedingungen und Modalitäten der internen Untersuchungen zur Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen zum Nachteil der Interessen der Union.

Es gilt die Strategie für die Betrugsaufdeckung und -bekämpfung der GD HOME.

### 3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

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

- Bestehende Haushaltslinien

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

Rubrik des mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
			von EFTA-Ländern <sup>91</sup>	von Kandidatenländern <sup>92</sup>	von Drittländern	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
	Rubrik 3 –Sicherheit und Unionsbürgerschaft	GM/NGM <sup>90</sup>				
	18 02 08 – Schengener Informationssystem	GM	NEIN	NEIN	JA	NEIN
	18 02 01 01 – Unterstützung des Grenzmanagements und der gemeinsamen Visumpolitik zur Erleichterung legaler Reisen	GM	NEIN	NEIN	JA	NEIN
	18 02 07 – Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA)	GM	NEIN	NEIN	JA	NEIN

<sup>90</sup> GM = Getrennte Mittel/NGM = Nichtgetrennte Mittel.

<sup>91</sup> EFTA: Europäische Freihandelsassoziation.

<sup>92</sup> Kandidatenländer und gegebenenfalls potenzielle Kandidatenländer des Westbalkans.

### 3.2. Geschätzte Auswirkungen auf die Ausgaben

#### 3.2.1. Übersicht

<b>Rubrik des mehrjährigen Finanzrahmens</b>	3	Sicherheit und Unionsbürgerschaft
--	---	-----------------------------------

GD HOME			Jahr 2018	Jahr 2019	Jahr 2020	INSGESAMT
• Operative Mittel						
18 02 08 Schengener Informationssystem	Verpflichtungen	(1)	6,234	1,854	1,854	<b>9,942</b>
	Zahlungen	(2)	6,234	1,854	1,854	<b>9,942</b>
18 02 01 01 Grenzen und Visa	Verpflichtungen	(1)		18,405	18,405	<b>36,810</b>
	Zahlungen	(2)		18,405	18,405	<b>36,810</b>
<b>Mittel INSGESAMT für die GD HOME</b>	Verpflichtungen	=1+1a +3	6,234	20,259	20,259	<b>46,752</b>
	Zahlungen	=2+2a +3	6,234	20,259	20,259	<b>46,752</b>

<b>Rubrik des mehrjährigen Finanzrahmens</b>	3	Sicherheit und Unionsbürgerschaft
--	---	-----------------------------------

eu-LISA			Jahr 2018	Jahr 2019	Jahr 2020	INSGESAMT
• Operative Mittel						
Titel 1: Personalausgaben	Verpflichtungen	(1)	0,210	0,210	0,210	<b>0,630</b>
	Zahlungen	(2)	0,210	0,210	0,210	<b>0,630</b>
Titel 2: Infrastruktur- und Betriebsausgaben	Verpflichtungen	(1a)	0	0	0	<b>0</b>
	Zahlungen	(2a)	0	0	0	<b>0</b>
Titel 3: Operative Ausgaben	Verpflichtungen	(1a)	12,893	2,051	1,982	<b>16,926</b>
	Zahlungen	(2a)	2,500	7,893	4,651	<b>15,044</b>
<b>Mittel INSGESAMT für eu-LISA</b>	Verpflichtungen	=1+1a +3	13,103	2,261	2,192	<b>17,556</b>
	Zahlungen	=2+2a +3	2,710	8,103	4,861	<b>15,674</b>

### 3.2.2. Geschätzte Auswirkungen auf die operativen Mittel

• Operative Mittel INSGESAMT	Verpflichtungen	(4)							
	Zahlungen	(5)							
• Aus der Dotation bestimmter Programme finanzierte Verwaltungsausgaben INSGESAMT		(6)							
<b>Mittel INSGESAMT unter der RUBRIK &lt;...&gt; des mehrjährigen Finanzrahmens</b>	Verpflichtungen	=4+ 6							
	Zahlungen	=5+ 6							

**Wenn der Vorschlag/die Initiative mehrere Rubriken betrifft:**

• Operative Mittel INSGESAMT	Verpflichtungen	(4)							
	Zahlungen	(5)							
• Aus der Dotation bestimmter Programme finanzierte Verwaltungsausgaben INSGESAMT		(6)							
<b>Mittel INSGESAMT unter den RUBRIKEN 1 bis 4 des mehrjährigen Finanzrahmens (Referenzbetrag)</b>	Verpflichtungen	=4+ 6	19,337	22,520	22,451				<b>64,308</b>
	Zahlungen	=5+ 6	8,944	28,362	25,120				<b>62,426</b>

3.2.3. *Geschätzte Auswirkungen auf die Verwaltungsmittel*

<b>Rubrik des mehrjährigen Finanzrahmens</b>	<b>5</b>	Verwaltungsausgaben
--	----------	---------------------

		Jahr N	Jahr N+1	Jahr N+2	Jahr N+3	Bei länger andauernden Auswirkungen (siehe 1.6) bitte weitere Spalten einfügen	INSGESAMT
GD <.....>							
• Personalausgaben							
• Sonstige Verwaltungsausgaben							
<b>GD &lt;.....&gt;INSGESAMT</b>	Mittel						

in Mio. EUR (3 Dezimalstellen)

<b>Mittel INSGESAMT unter der RUBRIK 5 des mehrjährigen Finanzrahmens</b>	(Verpflichtungen insges. = Zahlungen insges.)								

in Mio. EUR (3 Dezimalstellen)

<b>Mittel INSGESAMT unter den RUBRIKEN 1 bis 5 des mehrjährigen Finanzrahmens</b>		Jahr N <sup>93</sup>	Jahr N+1	Jahr N+2	Jahr N+3	Bei länger andauernden Auswirkungen (siehe 1.6) bitte weitere Spalten einfügen			Insgesamt
		Verpflichtungen							
Zahlungen									

<sup>93</sup> Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird.

### 3.2.3.1. Geschätzte Auswirkungen auf die Mittel der GD HOME

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

Ziele und Ergebnisse angeben  ↓			Jahr 2018		Jahr 2019		Jahr 2020		Bei länger andauernden Auswirkungen (siehe 1.6) bitte weitere Spalten einfügen						INSGESAMT					
	ERGEBNISSE																			
	Art <sup>94</sup>	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1 <sup>95</sup> Entwicklung nationales System		1		1	1,221	1	1,221													2,442
EINZELZIEL Nr. 2 Infrastruktur		1		1	17,184	1	17,184													34,368
<b>GESAMTKOSTEN</b>					18,405		18,405													36,810

<sup>94</sup> Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B. Zahl der Austauschstudenten, gebaute Straßenkilometer).

<sup>95</sup> Wie in Punkt 1.4.2 beschrieben „Einzelziel(e)...“.

### 3.2.3.2. Geschätzte Auswirkungen auf die operativen Mittel von eu-LISA

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

Mittel für Verpflichtungen in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse angeben  ↓			Jahr 2018		Jahr 2019		Jahr 2020		Bei länger andauernden Auswirkungen (siehe 1.6) bitte weitere Spalten einfügen						INSGESAMT				
	ERGEBNISSE																		
	Art <sup>96</sup>	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl
EINZELZIEL Nr. 1 <sup>97</sup> Entwicklung des zentralen Systems																			
- Auftragnehmer			1	5,013															5,013
- Software			1	4,050															4,050
- Hardware			1	3,692															3,692
Zwischensumme für Einzelziel Nr. 1				12,755															12,755
EINZELZIEL Nr. 2 Wartung des zentralen Systems																			
- Auftragnehmer			1	0	1	0,365	1	0,365											0,730
Software			1	0	1	0,810	1	0,810											1,620
Hardware			1	0	1	0,738	1	0,738											1,476
Zwischensumme für Einzelziel						1,913		1,913											3,826

<sup>96</sup> Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B. Zahl der Austauschstudenten, gebaute Straßenkilometer).

<sup>97</sup> Wie in Punkt 1.4.2 beschrieben „Einzelziel(e)...“.

Nr. 2															
EINZELZIEL Nr. 3 Sitzungen/Schulungen															
Schulungsmaßnahmen	1	0,138	1	0,138	1	0,069									0,345
Zwischensumme für Einzelziel Nr. 3		0,138		0,138		0,069									0,345
<b>GESAMTKOSTEN</b>		12,893		2,051		1,982									16,926

### 3.2.3.3. Geschätzte Auswirkung auf das Personal von eu-LISA

#### Übersicht

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

in Mio. EUR (3 Dezimalstellen)

	Jahr 2018	Jahr 2019	Jahr 2020	INSGE- SAMT
--	--------------	--------------	--------------	----------------

Beamte der Funktionsgruppe AD				
Beamte der Funktionsgruppe AST				
Vertragsbedienstete	0,210	0,210	0,210	0,630
Zeitbedienstete				
Abgeordnete nationale Sachverständige				

<b>INSGESAMT</b>	<b>0,210</b>	<b>0,210</b>	<b>0,210</b>	<b>0,630</b>
------------------	--------------	--------------	--------------	--------------

Einstellungen sind für Januar 2018 geplant. Das gesamte Personal muss ab Anfang 2018 verfügbar sein, damit die Entwicklung rechtzeitig beginnen und die Neuversion des SIS II 2020 in Betrieb genommen werden kann. Die drei neuen Vertragsbediensteten werden für die Durchführung des Projekts sowie nach Inbetriebnahme des Systems für die operative Unterstützung und Wartung benötigt. Diese Bediensteten übernehmen folgende Aufgaben:

- Unterstützung der Projektdurchführung als Projektteammitglieder, u. a. bei folgenden Tätigkeiten: Festlegung der Anforderungen und technischen Spezifikationen, Zusammenarbeit mit den Mitgliedstaaten und deren Unterstützung während der Projektdurchführung, Aktualisierung des Schnittstellenkontrolldokuments (Interface Control Document – ICD), Überwachung der vertraglich vereinbarten Leistungen, Bereitstellung von Dokumentation und Aktualisierungen usw.
- Unterstützung der Übergangsmaßnahmen zur Inbetriebnahme des Systems in Zusammenarbeit mit dem Auftragnehmer (Follow-up der einzelnen Versionen, Aktualisierung des Betriebsprozesses, Schulungen (einschließlich Fortbildungsmaßnahmen in den Mitgliedstaaten) usw.).
- Unterstützung der längerfristigen Maßnahmen, Festlegung von Spezifikationen, Vertragsvorbereitung im Fall einer Umstellung des Systems (z. B. aufgrund der Bilderkennung) oder, falls der neue Vertrag über die Wartung des SIS II geändert werden muss, um zusätzlichen (technischen oder budgetären) Änderungen Rechnung zu tragen.

- Unterstützung des Second-Level-Support nach der Inbetriebnahme bei kontinuierlichen Wartungsarbeiten sowie bei Tätigkeiten, die während des laufenden Betriebs anfallen.

Es ist darauf hinzuweisen, dass die drei neuen Vertragsbediensteten (VZÄ VB) die internen Ressourcen der Teams ergänzen werden, die auch für das Follow-up und die operativen Aufgaben im Zusammenhang mit dem Projekt und den vertraglichen und finanziellen Aspekten eingesetzt werden. Durch den Einsatz von Vertragsbediensteten wird eine angemessene Vertragsdauer und -kontinuität gewährleistet, um den laufenden Dienstbetrieb sicherzustellen und nach Abschluss des Projekts dieselben Fachkräfte für operative Unterstützungsaufgaben einsetzen zu können. Darüber hinaus ist für die operativen Unterstützungstätigkeiten ein Zugang zur Betriebsumgebung erforderlich, der Auftragnehmern oder externen Mitarbeitern nicht gewährt werden kann.



### 3.2.4. Vereinbarkeit mit dem mehrjährigen Finanzrahmen

- Der Vorschlag/Die Initiative ist mit dem mehrjährigen Finanzrahmen vereinbar.
- Der Vorschlag/Die Initiative erfordert eine Anpassung der betreffenden Rubrik des mehrjährigen Finanzrahmens.

Eine Neuprogrammierung des Restbetrags der Mittel, die für das Paket „Intelligente Grenzen“ im Rahmen des Fonds für die innere Sicherheit bereitgestellt wurden, ist geplant, um die in diesen beiden Vorschlägen vorgesehenen Funktionen und Änderungen umzusetzen. Die Verordnung ISF – Grenzen ist das Finanzierungsinstrument, das die Mittel für die Umsetzung des Pakets „Intelligente Grenzen“ enthält. Artikel 5 dieser Verordnung sieht vor, dass 791 Mio. EUR für ein Programm zur Einführung von IT-Systemen verwendet werden, die die Steuerung von Migrationsströmen über die Außengrenzen gemäß den in Artikel 15 festgelegten Bedingungen unterstützen. Von den vorgenannten 791 Mio. EUR sind 480 Mio. EUR für die Entwicklung des Einreise-/Ausreisystems und 210 Mio. EUR für die Entwicklung des Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) vorgesehen. Der Restbetrag von 100,828 Mio. EUR wird teilweise verwendet, um die Kosten der in den beiden Vorschlägen vorgesehenen Änderungen im Zusammenhang mit der Aufrüstung der SIS-II-Funktionen zu decken.

- Der Vorschlag/Die Initiative erfordert eine Inanspruchnahme des Flexibilitätsinstruments oder eine Änderung des mehrjährigen Finanzrahmens.

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

### 3.2.5. Finanzierungsbeteiligung Dritter

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

Mittel in Mio. EUR (3 Dezimalstellen)

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

### 3.3. Geschätzte Auswirkungen auf die Einnahmen

- Der Vorschlag/Die Initiative wirkt sich nicht auf die Einnahmen aus.
- Der Vorschlag/Die Initiative wirkt sich auf die Einnahmen aus, und zwar:
  - auf die Eigenmittel
  - auf die sonstigen Einnahmen

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Für das laufende Haushaltsjahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative <sup>100</sup>					Bei länger andauernden Auswirkungen (siehe 1.6) bitte weitere Spalten einfügen		
		2018	2019	2020	2021				
Artikel 63 13 – Beitrag der assoziierten Schengen-Länder (CH, NO, LI, IS)		p.m	p.m	p.m	p.m				

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

18 02 08 (Schengener Informationssystem), 18 02 07 (eu-LISA)

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

Der Haushalt enthält einen Beitrag von Ländern, die bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands assoziiert sind.

<sup>100</sup> Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d. h. abzüglich 25 % für Erhebungskosten, anzugeben.