Rat der
Europäischen Union

Brüssel, den 5. September 2019
(OR. en)

9364/19

DAPIX 184
ENFOPOL 252
CT 53
ENFOCUSTOM 105
CRIMORG 81
SCHENGEN 23
VISA 116
SIRIS 97
COPEN 219
ASIM 62
FRONT 190
COMIX 273
JAI 529

VERMERK

Absender:	Generalsekretariat des Rates
Empfänger:	Gruppe "Informationsaustausch und Datenschutz" (DAPIX)
Nr. Vordok.:	6727/18
Betr.:	Leitfaden für den Austausch von strafverfolgungsrelevanten Informationen

1. Einleitung

Mit dem Leitfaden für den Austausch von strafverfolgungsrelevanten Informationen soll das Handbuch für grenzüberschreitende Einsätze (Dok. 10505/4/09 REV 4) ergänzt werden. Sowohl der Inhalt als auch die Struktur des Leitfadens und der nationalen Merkblätter sind im Rahmen der Strategie für das Informationsmanagement (IMS) für die innere Sicherheit in der EU von der DAPIX-Gruppe im Hinblick auf die Unterstützung, Straffung und Förderung des grenzüberschreitenden Informationsaustauschs gebilligt worden.

Übersetzungen in alle Amtssprachen der Union werden zur Verfügung gestellt, um den praktischen Nutzen des Leitfadens zu steigern. Darüber hinaus wird der Leitfaden zweimal jährlich aktualisiert, wobei gegebenenfalls neue Rechtsvorschriften oder Erfahrungen aus der Praxis berücksichtigt werden.

Die gegenwärtige Fassung trägt insbesondere der Europol-Verordnung und den Kontaktangaben Rechnung. Diese Kontaktangaben werden von den Mitgliedstaaten regelmäßig aktualisiert und sind in den nationalen Merkblättern, die von nun an als Addendum (ADD1) zum Leitfaden herausgegeben werden, aufgeführt. Dieses Addendum enthält sensible Informationen und darf nicht ohne Konsultation des Generalsekretariats des Rates nach Maßgabe der Verordnung (EG) Nr. 1049/2001 verbreitet werden[1]. Ein neues Element ist der praktische Ratgeber (ADD 2), der eine Gegenüberstellung der Anforderungen an den Informationsaustausch über die verschiedenen Kanäle enthält.

2. Zweck des Leitfadens

Der Leitfaden ist in erster Linie als ein Werkzeug für die als internationale Verbindungsbeamte tätigen Polizeibeamten – insbesondere für die in den sogenannten "**einzigen Anlaufstellen" (Single Point of Contact/SPOC) als "Operator" eingesetzten Beamten** – gedacht. Daher sollte er möglichst nutzerfreundlich und umfassend gehalten sein.

Der Leitfaden soll die **alltägliche praktische Zusammenarbeit** zwischen den verschiedenen am Austausch polizeilicher Informationen sowohl auf nationaler als auch auf internationaler Ebene beteiligten Behörden der Mitgliedstaaten auf solide Grundlagen stellen und erleichtern, Ausbildungszwecken dienen und gewährleisten, dass in Bezug auf Informationsbeschaffung und -austausch über Grenzen hinweg fundiertere Entscheidungen getroffen werden.

Der Leitfaden enthält einen **Überblick über alle EU-Systeme, EU-Rechtsgrundlagen und EU-Instrumente für den Informationsaustausch**, die den Strafverfolgungsbehörden der Mitgliedstaaten zur Verfügung stehen. Somit wird der Nutzer umfassend darüber unterrichtet, welche Optionen ihm für die Entscheidung in der Frage zur Verfügung stehen, wie Informationen grenzüberschreitend beschafft oder bereitgestellt werden sollen.

Der Leitfaden wird durch **nationale Merkblätter** ergänzt, die die für den grenzüberschreitenden Austausch relevanten Kontaktangaben und Informationen enthalten. Mit der regelmäßigen Aktualisierung dieser Merkblätter kommen die Mitgliedstaaten den zahlreichen Mitteilungspflichten gemäß den einzelnen Rechtsinstrumenten nach. Die nationalen Merkblätter dürften die Verwaltung und Beschaffung der erforderlichen Informationen vereinfachen.

---

[1] Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission. Diese Verordnung legt die allgemeinen Grundsätze und Einschränkungen für den Zugang fest.

Der Leitfaden enthält diese nationalen Merkblätter sowie die wesentlichen praktischen Informationen über den Rahmenbeschluss 2006/960/JI des Rates ("schwedischer Rahmenbeschluss"); ferner ersetzt er die früheren Leitlinien für die Umsetzung des "schwedischen Rahmenbeschlusses" (9512/10 CRIMORG 90 ENFOPOL 125 ENFOCUSTOM 36 COMIX 346).

3. Inhalt des Leitfadens

Der Leitfaden gliedert sich in drei Teile, die je nach Bedarf des Lesers unabhängig voneinander konsultiert werden können.

Der erste Teil des Leitfadens besteht aus **Checklisten**, die einen praxisorientierten Überblick über die Optionen für den Informationsaustausch und diesbezügliche praktische Aspekte vermitteln. Diese Checklisten sind dabei behilflich, den Nutzer anhand von Listen der verfügbaren Systeme und Methoden bei folgenden Haupteinsatzsituationen zu der entsprechenden Anlaufstelle zu leiten:

– Verhütung und Untersuchung von Straftaten (sowie der illegalen Einwanderung);

– Terrorismusbekämpfung;

– Aufrechterhaltung der öffentlichen Ordnung und Sicherheit.

Im zweiten Teil werden mit einer **allgemeinen** Beschreibung sowohl die am Informationsaustausch beteiligten nationalen Stellen als auch die Instrumente für den Informationsaustausch vorgestellt. Im Leitfaden wird auf die zentrale Rolle des Rahmenbeschlusses 2006/960/JI des Rates ("schwedischer Rahmenbeschluss") und des Beschlusses 2008/615/JI ("Prüm-Beschluss") für den umfassenderen Kontext des Informationsaustauschs in der EU hingewiesen. Der Leitfaden beschränkt sich aber nicht auf diese Instrumente.

Im Addendum wird der Leitfaden ergänzt durch

a) eine Sammlung der **nationalen Merkblätter** zu den einzelnen Mitgliedstaaten mit **praktischen Angaben** zu den für den grenzübergreifenden Informationsaustausch zuständigen **Anlaufstellen**, und

b) die Anforderungen an den Informationsaustausch im Hinblick auf die jeweils verwendeten Kanäle (Interpol /Europol /SIRENE / Verbindungsbeamte / Zentrum für die Zusammenarbeit von Polizei und Zoll) und praktische Hinweise, die nutzerfreundlich dargestellt werden.

4. Überblick und Ausblick

Die Ausarbeitung des vorgeschlagenen Leitfadens war als Maßnahme im dritten Maßnahmenkatalog der Strategie für das Informationsmanagement (IMS) enthalten; die erste Fassung des Leitfadens wurde unter irischem, zyprischem, griechischem, italienischem und lettischem Vorsitz erstellt.

Um die Verwendung des Leitfadens für den Austausch von strafverfolgungsrelevanten Informationen noch einfacher zu gestalten, legt der Vorsitz die vorliegende aktualisierte Fassung den Delegationen mit der Bitte vor, sie entsprechend ihren Bedürfnissen in geeigneter Weise zu verbreiten.

Rat der Europäischen Union
Generalsekretariat
Generaldirektion Justiz und Inneres
Direktion Inneres
Referat 1C Polizeiliche und zollbehördliche Zusammenarbeit

Leitfaden für den Austausch von strafverfolgungsrelevanten Informationen

Inhalt

Einleitung 10

CHECKLISTE A: INFORMATIONSAUSTAUSCH FÜR DIE ZWECKE DER VERHÜTUNG UND UNTERSUCHUNG VON STRAFTATEN 14

CHECKLISTE B: INFORMATIONSAUSTAUSCH FÜR DIE ZWECKE DER BEKÄMPFUNG TERRORISTISCHER STRAFTATEN 21

CHECKLISTE C: INFORMATIONSAUSTAUSCH FÜR DIE ZWECKE DER AUFRECHTERHALTUNG DER ÖFFENTLICHEN ORDNUNG UND SICHERHEIT 29

TEIL II – Allgemeine Informationen 32

1. KONTAKTKANÄLE 33

1.1. Einzige Anlaufstellen (Single Point of Contact/SPOC) 33

1.2. SIRENE-Büros 37

1.3. Nationale Europol-Stellen (ENU) 38

1.4. INTERPOL – Nationale Zentralbüros (NZB) 39

1.5. Nationale Prüm-Kontaktstellen 40

1.5.1. Nationale Prüm-Kontaktstelle – DNA und Fingerabdrücke 40

1.5.2. Nationale Prüm-Kontaktstelle – Fahrzeugregisterdaten (VRD) 42

1.5.3. Nationale Prüm-Kontaktstelle – Terrorismusprävention 43

1.5.4. Nationale Prüm-Kontaktstelle – Großveranstaltungen 43

1.6. Nationale Fußballinformationsstellen (der Polizei) (NFIP) 44

1.6.1. Fußballhandbuch 45

1.7. Zentren für die Zusammenarbeit von Polizei und Zoll (PCCC) 45

1.8. Verbindungsbeamte 48

1.9. Vermögensabschöpfungsstellen (ARO) der Mitgliedstaaten 50

1.10. Geldwäsche – Zusammenarbeit zwischen den Zentralstellen für Geldwäsche-Verdachtsanzeigen (FIU) 51

1.11. Neapel-II-Übereinkommen 53

1.12. PNR-Zentralstelle 54

1.13. Nationale Zugangsstellen – EES 57

1.14. Nationale ETIAS-Stellen 59

1.15. Interoperabilität 62

1.16. Wahl des Kommunikationskanals – allgemein verwendete Kriterien 64

2. INFORMATIONSSYSTEME 66

2.1. Schengener Informationssystem der zweiten Generation (SIS II) 66

2.2. EIS – Europol-Informationssystem 68

2.3. SIENA – die Europol-Netzanwendung für sicheren Datenaustausch 69

2.4. I-24/7 – das globale Polizeikommunikationssystem von Interpol 70

2.4.1. Interpol: DNA-Gateway 71

2.4.2. Interpol-Fingerabdruckdatenbank 71

2.4.3. Interpol-Datenbank gestohlener und verlorener Reisedokumente 72

2.4.4. Datenbank zur Erfassung von Ausschreibungen zugeordneten Reisedokumenten (TDAWN) 72

2.4.5. Referenztabelle für Schusswaffen 72

2.5. Europäisches Strafregisterinformationssystem ECRIS 73

2.5.1. ECRIS für Drittstaatsangehörige 74

2.6. Visa-Informationssystem (VIS) 76

2.7. Eurodac 78

2.8. ZIS – Zollinformationssystem 80

2.9. Gefälschte und echte Dokumente online – FADO 81

2.10. Öffentliches Online-Register echter Identitäts- und Reisedokumente – PRADO 82

2.11. Einreise-/Ausreisesystem (EES) 83

2.12. Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) 85

2.13. Gesamtüberblick über die für den Informationsaustausch auf EU-Ebene verwendeten Informationssysteme 88

3. RECHTSVORSCHRIFTEN – RECHTLICHER KONTEXT SOWIE REGELN UND LEITLINIEN FÜR DIE WICHTIGSTEN KOMMUNIKATIONSVERFAHREN UND -SYSTEME 95

3.1. Datenschutzrichtlinie 95

3.2. "Schwedischer Rahmenbeschluss" 98

3.3. Schengen – SIS- II-Datenaustausch und nicht über SIS II laufender Datenaustausch 109

3.4. Europol 112

3.5. Interpol 114

3.6. Verbindungsbeamte 115

3.7. "Prüm"- Datenaustausch 117

3.8. Visa-Informationssystem (VIS) 118

3.9. Eurodac 120

3.10. Neapel- II-Übereinkommen 121

3.10.1. Zollinformationssystem – ZIS 122

3.11. Nationale Vermögensabschöpfungsstellen (ARO) und CARIN 122

3.12. Zentrale Meldestellen für Geldwäsche-Verdachtsanzeigen (FIU) 124

3.13. Abkommen EU-USA über das Programm zum Aufspüren der Finanzierung des Terrorismus (TFTP-Abkommen) 126

3.14. Austausch von Strafregisterinformationen (ECRIS) 127

3.14.1. Austausch von Strafregisterinformationen zu Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) 128

3.15. Vorratsspeicherung von Telekommunikationsdaten 130

3.16. PNR (Fluggastdatensätze)-Richtlinie 131

3.17. Vorab übermittelte Fluggastdaten (API-Daten) 133

3.18. Straßenverkehrsgefährdende Verkehrsdelikte 134

3.19. Einreise-/Ausreisesystem (EES) 135

3.20. Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) 137

3.21. Rechtsvorschriften zur Interoperabilität 140

EINLEITUNG

Zweck des Leitfadens

Die grenzüberschreitende polizeiliche Zusammenarbeit innerhalb der Europäischen Union stützt sich ganz wesentlich auf den Informationsaustausch. Mit diesem Leitfaden soll die diesbezügliche alltägliche Zusammenarbeit erleichtert werden. Wichtigste Zielgruppe sind die jeweiligen nationalen einzigen Anlaufstellen (SPOC), die für die Steuerung des Informationsflusses zwischen den einzelnen Einheiten und benannten Anlaufstellen sowohl auf nationaler als auch auf internationaler Ebene verantwortlich sind.

Das Gesamtbild der Zusammenarbeit bei der Strafverfolgung[2] ist durch die Zunahme und die Beschleunigung des Informationsaustauschs gekennzeichnet. Zum einen wird es durch die kontinuierliche Weiterentwicklung der Informations- und Kommunikationstechnologien unterstützt. Zum anderen ist eine Vielzahl nationaler und internationaler Datenbanken verfügbar.

Dieser Leitfaden soll behilflich sein, wenn in einem konkreten operativen Kontext die richtige Anlaufstelle oder Datenbank gefunden werden muss. Im Leitfaden werden die einschlägigen Rechtsvorschriften kurz dargelegt, ohne dass dabei der Hauptzweck, nämlich die Erleichterung des grenzüberschreitenden Informationsaustauschs, außer Acht gerät.

Struktur des Leitfadens

Der Leitfaden gliedert sich wie folgt:

Teil I – "Operativer Kontext" **–** enthält eine Reihe von Tabellen oder "Checklisten", die die in Teil II und Teil III enthaltenen Informationen entweder mit der einschlägigen Rechtsgrundlage oder mit Informationen über die Anlaufstellen verknüpfen. Diese Checklisten sind nach drei Hauptthemenbereichen gegliedert:

- **Verhütung und Bekämpfung der Kriminalität (und der illegalen Einwanderung) – Checkliste A**
- **Bekämpfung terroristischer Straftaten – Checkliste B**
- **Aufrechterhaltung der öffentlichen Ordnung – Checkliste C**

Diese Checklisten sollen dem Leser den Weg weisen von einem in einem spezifischen operativen Kontext als relevant ausgewählten Informationskanal oder - verfahren hin zu Quellen mit Kontaktangaben oder einschlägigen Rechtsvorschriften, Regelungen und Leitfäden mit bewährten Verfahren.

---

[2] Für die Zwecke dieses Leitfadens bezeichnet "Strafverfolgung" die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten im Sinne der Richtlinie (EU) 2017/541 oder von schweren Straftaten im Sinne von Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI über den Europäischen Haftbefehl (EuHb).

Teil II – "Allgemeine Informationen" – gibt einen Überblick über das Strafverfolgungsumfeld in Bezug auf die verschiedenen den Polizeikräften in der EU zur Verfügung stehenden Kommunikationskanäle und verfahren. Dieser Teil II ist in drei Bereiche untergliedert, die Folgendes betreffen:

- ***Kommunikationskanäle (d. h. Stellen, die mit dem Austausch von strafverfolgungsrelevanten Informationen befasst sind)***
- ***für den grenzüberschreitenden Datenaustausch verwendete Informationssysteme und Datenbanken***
- ***Rechtsvorschriften – gesetzgeberischer Kontext sowie Regeln und Leitlinien für die wichtigsten Kommunikationsverfahren und - systeme.***

Teil III – "Nationale Merkblätter" – im Addendum 1 zu diesem Vermerk enthält die nationalen Merkblätter mit ausführlichen Angaben zu den Anlaufstellen für alle in diesem Dokument angesprochenen Aspekte des grenzüberschreitenden Informationsaustauschs. Es ist Sache der Mitgliedstaaten, dem Generalsekretariat des Rates umgehend etwaige Änderungen zu melden. Mit der regelmäßigen Aktualisierung der im Addendum zum Leitfaden enthaltenen nationalen Merkblätter kommen die Mitgliedstaaten den vielfältigen Mitteilungspflichten gemäß den einzelnen Rechtsinstrumenten nach. Dies dürfte künftig die Verwaltung und das Auffinden der betreffenden Informationen erleichtern.

Teil IV - "Praktischer Ratgeber" für den Informationsaustausch im Bereich der Strafverfolgung

Der in Addendum 2 zu diesem Vermerk enthaltene praktische Ratgeber bietet eine benutzerfreundlich gestaltete Gegenüberstellung der Anforderungen an den Informationsaustausch im Hinblick auf die jeweiligen Kanäle (Interpol /Europol /SIRENE / Verbindungsbeamte / Zentrum für die Zusammenarbeit von Polizei und Zoll). Zudem enthält der Ratgeber praktische Informationen und Hinweise zu den Instrumenten der Zusammenarbeit im Bereich Strafverfolgung, die nicht nur für die Bediensteten der einzigen Anlaufstellen (SPOC), sondern auch anderer nationaler Strafverfolgungsbehörden von Nutzen sein könnten.

Teil I - Operativer Kontext

CHECKLISTE A: INFORMATIONSAUSTAUSCH FÜR DIE ZWECKE DER VERHÜTUNG UND UNTERSUCHUNG VON STRAFTATEN

Informationssystem	**Nationale Zugangsstelle**	**Rechtsgrundlage**	**Handbuch**
Schengener Informationssystem/SIS II	SIRENE-Büro (**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntries – Antrag auf Zusatzinformationen bei der nationalen Eingangsstelle)	Schengen-Besitzstand gemäß Artikel 1 Absatz 2 des Beschlusses 1999/435/EG des Rates vom 20. Mai 1999 ABl. L 239 vom 22.9.2000, S. 1 Beschluss 2007/533/JI des Rates ABl. L 205 vom 7.8.2007, S. 63 Verordnung (EG) Nr. 1986/2006 ABl. L 381 vom 28.12.2006, S. 1 Verordnung (EG) Nr. 1987/2006 ABl. L 381 vom 28.12.2006, S. 4	Überarbeitete Fassung des aktualisierten Katalogs von Empfehlungen für die ordnungsgemäße Anwendung des Schengen-Besitzstands und der bewährten Praktiken 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484 Durchführungsbeschluss (EU) 2017/1528 der Kommission 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 231 vom 7.9.2017, S. 6).

Europol / Europol-Informationssystem (EIS) – EIS-Indexsystem Arbeitsdateien zu Analysezwecken – AWF (Analysis Work Files)	Nationale Europol-Stellen (ENU)	Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates, ABl. L 135 vom 24.5.2016, S. 53-114 (anwendbar seit dem 1. Mai 2017).	
Interpol/I-24/7	Nationales Zentralbüro von Interpol (NZB) (Nationales Zentralbüro)	Interpol-Datenverarbeitungsvorschriften [III/IRPD/GA/2011(2014)] Vorschriften über die Kontrolle der Informationen und des Zugangs zu den Dateien von Interpol [II.E/RCIA/GA/2004(2009)]	
DNA/Prüm – automatisierter Abruf benannter nationaler Datenbanken	Nationale Kontaktstelle erster Schritt: automatisierter Abruf	Beschluss 2008/615/JI des Rates, Artikel 3 und 4 ABl. L 210 vom 6.8.2008, S. 1	
	zweiter Schritt: Übermittlung weiterer personenbezogener Daten und sonstiger Informationen	Nationale Rechtsvorschriften Rahmenbeschluss 2006/960/JI des Rates ("schwedischer Rahmenbeschluss") ABl. L 386 vom 29.12.2006, S. 89, Korrigendum in ABl. L 75 vom 15.3.2007, S. 26	

Fingerabdrücke/Prüm – automatischer Abruf des nationalen automatisierten Fingerabdruck-Identifizierungssystems (AFIS)	Nationale Kontaktstelle erster Schritt: automatisierter Abruf	Beschluss 2008/615/JI des Rates, Artikel 9 ABl. L 210 vom 6.8.2008, S. 1	
	zweiter Schritt: Übermittlung weiterer personenbezogener Daten und sonstiger Informationen	Nationale Rechtsvorschriften Rahmenbeschluss 2006/960/JI des Rates ("schwedischer Rahmenbeschluss")	
Fahrzeugregisterdaten (VRD/ Prüm – automatisierter Abruf von Fahrzeugregisterdatenbanken	Nationale Kontaktstelle für eingehende Ersuchen	Beschluss 2008/615/JI des Rates, Artikel 12 ABl. L 210 vom 6.8.2008, S. 1	
	für ausgehende Ersuchen	wie oben	
Fluggastdatensätze (PNR-Daten)	PNR-Zentralstelle	Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität. ABl. L 119 vom 4.5.2016, S. 132	

Visa-Informationssystem (VIS)	Zentrale nationale Zugangsstellen	Entscheidung 2004/512/EG des Rates ABl. L 213 vom 15.6.2008, S. 5 Beschluss 2008/633/JI des Rates ABl. L 218 vom 13.8.2008, S. 126 Verordnung (EG) Nr. 767/2008 *ABl. L 218 vom 13.8.2008,* Liste der zuständigen Behörden, deren ordnungsgemäß ermächtigte Bedienstete Zugang zum Visa-Informationssystem (VIS) für die Eingabe, Änderung, Löschung oder Abfrage von Daten haben (2016/C 187/04), ABl. C 187 vom 26.5.2016, S. 4.	

Eurodac	Zuständige nationale Behörden	Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (Neufassung) ABl. L 180 vom 29.6.2013, S. 1 *Verordnung (EU) Nr. 604/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist* ABl. L 180 vom 29.6.2013, S. 31	

ZIS – Zollinformationssystem	Nationale Zugangsstellen	Beschluss 2009/917/JI des Rates vom 30. November 2009 über den Einsatz der Informationstechnologie im Zollbereich ABl. L 323 vom 10.12.2009, S. 20	
Europäisches Strafregisterinformationssystem (ECRIS)	Nationales Zentralbüro	Richtlinie (EU) 2019/884 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Änderung des Rahmenbeschlusses 2009/315/JI des Rates im Hinblick auf den Austausch von Informationen über Drittstaatsangehörige und auf das Europäische Strafregisterinformationssystem (ECRIS) sowie zur Ersetzung des Beschlusses 2009/316/JI des Rates ABl. L 151 vom 7.6.2019, S. 143	ECRIS – Nicht bindendes Handbuch für Rechtsanwender in elektronischem Format beim Kommunikations- und Informationszentrum für Behörden, Unternehmen und Bürger (CIRCABC) abrufbar unter: https://circabc.europa.eu
Camdener zwischenstaatliches Netz der Vermögensabschöpfungsstellen (CARIN)	Vermögensabschöpfungsstelle (ARO)	Beschluss 2007/845/JI des Rates vom 6. Dezember 2007 über die Zusammenarbeit zwischen den Vermögensabschöpfungsstellen der Mitgliedstaaten auf dem Gebiet des Aufspürens und der Ermittlung von Erträgen aus Straftaten oder anderen Vermögensgegenständen im Zusammenhang mit Straftaten ABl. L 332 vom 18.12.2007, S. 103	Handbuch bewährter Vorgehensweisen zur Bekämpfung der Finanzkriminalität: Eine Sammlung von Beispielen ausgereifter Systeme zur Bekämpfung der Finanzkriminalität in den Mitgliedstaaten 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37

FIU.NET	Zentrale Meldestellen für Geldwäsche-Verdachtsanzeigen (FIU)	Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission ABl. L 141 vom 141 vom 5.6.2015, S. 73 Zudem gelten für FIU neue Regeln nach der Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Festlegung von Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten und zur Aufhebung des Beschlusses 2000/642/JI des Rates. ABl. L 186 vom 11.7.2019, S. 122	Handbuch bewährter Vorgehensweisen zur Bekämpfung der Finanzkriminalität: Eine Sammlung von Beispielen ausgereifter Systeme zur Bekämpfung der Finanzkriminalität in den Mitgliedstaaten 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37

CHECKLISTE B: INFORMATIONSAUSTAUSCH FÜR DIE ZWECKE DER BEKÄMPFUNG TERRORISTISCHER STRAFTATEN

Informationssystem	**Nationale Zugangsstelle**	**Rechtsgrundlage**	**Handbuch**
Schengener Informationssystem/SIS II	SIRENE-Büro (**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntries – Antrag auf Zusatzinformationen bei der nationalen Eingangsstelle)	Schengen-Besitzstand gemäß Artikel 1 Absatz 2 des Beschlusses 1999/435/EG des Rates vom 20. Mai 1999 ABl. L 239 vom 22.9.2000, S. 1 Beschluss 2007/533/JI des Rates ABl. L 205 vom 7.8.2007, S. 63 Verordnung (EG) Nr. 1986/2006 ABl. L 381 vom 28.12.2006, S. 1 Verordnung (EG) Nr. 1987/2006 ABl. L 381 vom 28.12.2006, S. 4	Überarbeitete Fassung des aktualisierten Katalogs von Empfehlungen für die ordnungsgemäße Anwendung des Schengen-Besitzstands und der bewährten Praktiken: 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484 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) (bekanntgegeben unter Aktenzeichen C(2015) 326)

Europol / Europol-Informationssystem (EIS) – EIS-Indexsystem Arbeitsdateien zu Analysezwecken – AWF (Analysis Work Files)	Nationale Europol-Stellen (ENU)	Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates, ABl. L 135 vom 24.5.2016, S. 53-114 (anwendbar seit dem 1. Mai 2017).	
Interpol/I-24/7	Nationales Zentralbüro von Interpol (NZB) (Nationales Zentralbüro)	Interpol-Datenverarbeitungsvorschriften [III/IRPD/GA/2011(2014)] Vorschriften über die Kontrolle der Informationen und des Zugangs zu den Dateien von Interpol [II.E/RCIA/GA/2004(2009)]	
DNA/Prüm – automatisierter Abruf benannter nationaler Datenbanken	Nationale Kontaktstelle erster Schritt: automatisierter Abruf	Beschluss 2008/615/JI des Rates, Artikel 3 und 4 ABl. L 210 vom 6.8.2008, S. 1	
	zweiter Schritt: Übermittlung weiterer personenbezogener Daten und sonstiger Informationen	Nationale Rechtsvorschriften Rahmenbeschluss 2006/960/JI des Rates ("schwedischer Rahmenbeschluss") ABl. L 386 vom 29.12.2006, S. 89, Korrigendum in ABl. L 75 vom 15.3.2007, S. 26	

Fingerabdrücke/Prüm – automatischer Abruf des nationalen automatisierten Fingerabdruck-Identifizierungssystems (AFIS)	Nationale Kontaktstelle erster Schritt: automatisierter Abruf	Beschluss 2008/615/JI des Rates, Artikel 9 ABl. L 210 vom 6.8.2008, S. 1	
	zweiter Schritt: Übermittlung weiterer personenbezogener Daten und sonstiger Informationen	Nationale Rechtsvorschriften Rahmenbeschluss 2006/960/JI des Rates ("schwedischer Rahmenbeschluss")	
Fahrzeugregisterdaten (VRD/ Prüm – automatisierter Abruf von Fahrzeugregisterdatenbanken	Nationale Kontaktstelle für eingehende Ersuchen	Beschluss 2008/615/JI des Rates, Artikel 12 ABl. L 210 vom 6.8.2008, S. 1	
	für ausgehende Ersuchen	wie oben	
DNA/Prüm – automatisierter Abruf benannter nationaler Datenbanken	Nationale Kontaktstelle erster Schritt: automatisierter Abruf	Beschluss 2008/615/JI des Rates, Artikel 3 und 4 ABl. L 210 vom 6.8.2008, S. 1	*Anwendungsleitfaden – DNA-Datenaustausch* 7148/15 DAPIX 40 CRIMORG 25 ENFOPOL 61
Prüm-Netz für die Übermittlung personenbezogener Daten und spezieller Informationen für die Verhütung terroristischer Straftaten	Nationale Prüm-Kontaktstelle für die Terrorismusbekämpfung	Beschluss 2008/615/JI des Rates, Artikel 16 ABl. L 210 vom 6.8.2008, S. 1	

Fluggastdatensätze (PNR-Daten)	PNR-Zentralstelle	Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität. ABl. L 119 vom 4.5.2016, S. 132	
Visa-Informationssystem (VIS)	Zentrale nationale Zugangsstellen	Entscheidung 2004/512/EG des Rates ABl. L 213 vom 15.6.2008, S. 5 Beschluss 2008/633/JI des Rates ABl. L 218 vom 13.8.2008, S. 126 Verordnung (EG) Nr. 767/2008 ABl. L 218 vom 13.8.2008 Liste der zuständigen Behörden, deren ordnungsgemäß ermächtigte Bedienstete Zugang zum Visa-Informationssystem (VIS) für die Eingabe, Änderung, Löschung oder Abfrage von Daten haben (2016/C 187/04), ABl. C 187 vom 26.5.2016, S. 4.	

Eurodac	Zuständige nationale Behörden	Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (Neufassung) ABl. L 180 vom 29.6.2013, S. 1 Verordnung (EU) Nr. 604/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist ABl. L 180 vom 29.6.2013, S. 31	

Europäisches Strafregisterinformationssystem (ECRIS)	Nationales Zentralbüro	Richtlinie (EU) 2019/884 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Änderung des Rahmenbeschlusses 2009/315/JI des Rates im Hinblick auf den Austausch von Informationen über Drittstaatsangehörige und auf das Europäische Strafregisterinformationssystem (ECRIS) sowie zur Ersetzung des Beschlusses 2009/316/JI des Rates ABl. L 151 vom 7.6.2019, S. 143	ECRIS – Nicht bindendes Handbuch für Rechtsanwender in elektronischem Format beim Kommunikations- und Informationszentrum für Behörden, Unternehmen und Bürger (CIRCABC) abrufbar unter: https://circabc.europa.eu

Europäisches Strafregisterinformationssystem zu Drittstaatsangehörigen und Staatenlosen (European Criminal Records System on Third-Country National and Stateless Persons – ECRIS-TCN)	Nationales Zentralbüro	Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) 2018/1726 ABl. L 135 vom 7.6.2019, S. 1 Richtlinie (EU) 2019/884 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Änderung des Rahmenbeschlusses 2009/315/JI des Rates im Hinblick auf den Austausch von Informationen über Drittstaatsangehörige und auf das Europäische Strafregisterinformationssystem (ECRIS) sowie zur Ersetzung des Beschlusses 2009/316/JI des Rates ABl. L 151 vom 7.6.2019, S. 143	
Camdener zwischenstaatliches Netz der Vermögensabschöpfungsstellen (CARIN)	Vermögensabschöpfungsstelle (ARO)	Beschluss 2007/845/JI des Rates vom 6. Dezember 2007 über die Zusammenarbeit zwischen den Vermögensabschöpfungsstellen der Mitgliedstaaten auf dem Gebiet des Aufspürens und der Ermittlung von Erträgen aus Straftaten oder anderen Vermögensgegenständen im Zusammenhang mit Straftaten ABl. L 332 vom 18.12.2007, S. 103	

FIU.NET	Zentrale Meldestellen für Geldwäsche-Verdachtsanzeigen (FIU)	Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission ABl. L 141 vom 5.6.2015, S. 73 Zudem gelten für FIU neue Regeln nach der Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Festlegung von Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten und zur Aufhebung des Beschlusses 2000/642/JI des Rates ABl. L 186 vom 11.7.2019, S. 122	

CHECKLISTE C: INFORMATIONSAUSTAUSCH FÜR DIE ZWECKE DER AUFRECHTERHALTUNG DER ÖFFENTLICHEN ORDNUNG UND SICHERHEIT

Informationssystem	**Nationale Zugangsstelle**	**Rechtsgrundlage**	
Netz der ständigen Anlaufstellen für den Bereich der öffentlichen Sicherheit	Nationale Anlaufstellen	Gemeinsame Maßnahme 97/339/JI vom 26. Mai 1997 – vom Rat aufgrund von Artikel K.3 des Vertrags über die Europäische Union angenommen – betreffend die Zusammenarbeit im Bereich der öffentlichen Ordnung und Sicherheit *ABl. L 147 vom 5.6.1997, S. 1*	
Prüm-Netz zur Bereitstellung nichtpersonenbezogener und personenbezogener Daten zur Verhinderung von Straftaten und zur Abwehr einer Gefahr für die öffentliche Sicherheit und Ordnung bei Großveranstaltungen mit grenzüberschreitender Dimension	Nationale Prüm-Kontaktstelle/ Großveranstaltungen	Beschluss 2008/615/JI des Rates, Artikel 15 ABl. L 210 vom 6.8.2008, S. 1 Nationale Rechtsvorschriften	

Netz der nationalen Fußballinformationsstellen	Nationale Fußballinformationsstellen/ NFIP	Beschluss 2002/348/JI des Rates vom 25. April 2002 über die Sicherheit bei Fußballspielen von internationaler Bedeutung ABl. L 121 vom 8.5.2002, S. 1 Beschluss 2007/412/JI des Rates vom 12. Juni 2007 zur Änderung des Beschlusses 2002/348/JI über die Sicherheit bei Fußballspielen von internationaler Bedeutung ABl. L 155 vom 15.6.2007, S. 76	Empfehlung des Rates vom 6. Dezember 2007 betreffend einen Leitfaden für die Polizei- und Sicherheitsbehörden zur Zusammenarbeit bei Großveranstaltungen mit internationaler Dimension (2007/C 314/02) ABl. C 314 vom 22.12.2007, S. 4 Entschließung des Rates vom 3. Juni 2010 betreffend ein aktualisiertes Handbuch mit Empfehlungen für die internationale polizeiliche Zusammenarbeit und Maßnahmen zur Vorbeugung und Bekämpfung von Gewalttätigkeiten und Störungen im Zusammenhang mit Fußballspielen von internationaler Dimension, die zumindest einen Mitgliedstaat betreffen ABl. C 444 vom 29.11.2016, S. 1

Europäisches Netz zum Schutz von Persönlichkeiten des öffentlichen Lebens	Nationale Zugangsstellen	Beschluss 2009/796/JI des Rates vom 4. Juni 2009 zur Änderung des Beschlusses 2002/956/JI zur Schaffung eines Europäischen Netzes zum Schutz von Persönlichkeiten des öffentlichen Lebens ABl. L 283 vom 30.10.2009, S. 62	Handbuch des Europäischen Netzes zum Schutz von Persönlichkeiten des öffentlichen Lebens Dok. 10478/13 ENFOPOL 173
Zentren für die Zusammenarbeit von Polizei und Zoll	Zentren für die Polizei- und Zollzusammenarbeit	Bilaterale Vereinbarungen	

TEIL II – ALLGEMEINE INFORMATIONEN

1. KONTAKTKANÄLE[3]

1.1. Einzige Anlaufstellen (Single Point of Contact/SPOC)

Zahlreiche nationale Anlaufstellen

Die Mitgliedstaaten bewältigen – sowohl als ersuchte als auch als ersuchende Staaten – den zunehmenden grenzüberschreitenden Informationsfluss durch Verbesserung der Effizienz der operativen Strukturen und Netze, sowohl auf nationaler als auch auf europäischer Ebene. In vielen der Rechtsinstrumente der EU für die grenzüberschreitende Zusammenarbeit bei der Strafverfolgung wird zur Schaffung spezieller zuständiger Behörden/Stellen/Büros oder nationaler Anlaufstellen (NCP) aufgerufen. Polizei, Zoll oder andere nach dem nationalen Recht ermächtigte zuständige Behörden müssen Informationen über diese benannten nationalen Anlaufstellen (NCP), bei denen es sich um unterschiedliche Abteilungen der Polizeikräfte oder sogar unterschiedliche Ministerien handeln kann, austauschen. Um einen Überblick zu vermitteln, sind in Teil III dieses Dokuments Listen spezieller nationaler Anlaufstellen für den Informationsaustausch im Bereich der Strafverfolgung aufgeführt, die vom Generalsekretariat des Rates regelmäßig herausgegeben und aktualisiert werden.

Grundsatz der Verfügbarkeit – "schwedischer Rahmenbeschluss"

Der Austausch strafrechtlich relevanter[4] Informationen und Erkenntnisse von grenzüberschreitender Bedeutung sollte den Bedingungen entsprechen, die sich aus dem im sogenannten "schwedischen Rahmenbeschluss" verankerten "Grundsatz der Verfügbarkeit" ergeben. Dies bedeutet, dass

- ein Strafverfolgungsbeamter, der zur Erfüllung seiner Aufgaben Informationen benötigt, diese von einem anderen Mitgliedstaat erhalten kann;

- die Strafverfolgungsbehörden in dem Mitgliedstaat, der über diese Informationen verfügt, sie für den angegebenen Zweck bereitstellen, wobei sie den Erfordernissen der Ermittlungen in jenem Mitgliedstaat Rechnung tragen;

---

3 Nationale Stellen, die mit dem Austausch von strafverfolgungsrelevanten Informationen befasst sind.

4 Für die Zwecke dieses Leitfadens bezeichnet "Strafverfolgung" die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten im Sinne der Richtlinie (EU) 2017/541 oder von schweren Straftaten im Sinne von Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI über den Europäischen Haftbefehl (EuHb), wenn sie nach innerstaatlichem Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind.

- sobald polizeiliche Informationen in einem Mitgliedstaat verfügbar sind, diese grenzüberschreitend nach den gleichen Bedingungen ausgetauscht werden, die auch für den Informationsaustausch auf nationaler Ebene gelten, was bedeutet, dass die für grenzüberschreitende Fälle geltenden Regeln nicht strenger sind als diejenigen, die für den Datenaustausch auf nationaler Ebene gelten ("Grundsatz des gleichwertigen Zugangs").

Einzige Anlaufstelle (SPOC)

Die Kombination aus den strengen Anforderungen des "schwedischen Rahmenbeschlusses" und dem Bestehen unterschiedlicher nationaler Strategien zur Bewältigung der verschiedenen Informationsaustauschinitiativen macht eine einfachere und einheitlichere Vorgehensweise auf der Ebene der Mitgliedstaaten erforderlich, damit sichergestellt wird, dass alle zwischen Strafverfolgungsbehörden in der EU laufenden Informationsersuchen wirksam und effizient bearbeitet werden.

In den im Juni 2013 angenommenen Schlussfolgerungen des Rates zum Europäischen Modell für den Informationsaustausch (EIXM)[5] wurde das mit einer einzigen Anlaufstelle für den Informationsaustausch in jedem Mitgliedstaat verbundene Potenzial für die Straffung des Prozesses in einem zusehends komplexeren rechtlichen und operativen Umfeld gewürdigt.

Der Ansatz, den Informationsaustausch so weit wie möglich über eine einzige Anlaufstelle durchzuführen, ist von nahezu allen Mitgliedstaaten umgesetzt worden, auch wenn die Antwort auf die Frage, was genau eine einzige Anlaufstelle ausmacht, anscheinend von Mitgliedstaat zu Mitgliedstaat unterschiedlich ausfallen kann. In den SPOC-Leitlinien[6] ist angegeben, wie die einzigen Anlaufstellen strukturiert werden können, um die Ressourcen möglichst optimal zu nutzen, Überschneidungen zu vermeiden und die Zusammenarbeit mit anderen Mitgliedstaaten effizienter, zweckmäßiger und transparenter zu gestalten.

Aus diesen Leitlinien sollten die Mitgliedstaaten die für ihre Situation geeignete Lösung mit Blick auf das gemeinsame und vereinbarte Ziel einer Verstärkung der internationalen Zusammenarbeit auswählen und geeignete Wege erwägen, um die anderen Mitgliedstaaten im Hinblick auf den Austausch vorbildlicher Verfahren über die gewählte Lösung zu unterrichten.

---

5 Schlussfolgerungen des Rates im Anschluss an die Mitteilung der Kommission über das Europäische Modell für den Informationsaustausch (EIXM) (9811/13 JAI 400 DAPIX 82 CRIMORG 76 ENFOCUSTOM 88 ENFOPOL 146).

6 Entwurf von Leitlinien für eine einzige Anlaufstelle (Single Point of Contact – SPOC) für den internationalen Austausch von strafverfolgungsrelevanten Informationen – Strukturen der internationalen Zusammenarbeit im Bereich der Strafverfolgung in den einzelnen Mitgliedstaaten (10492/14 DAPIX 75 ENFOPOL 157 und 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1).

Im Idealfall gilt, dass die SPOC

- Zugang zum größtmöglichen Spektrum an einschlägigen nationalen, europäischen und internationalen strafverfolgungsrelevanten Datenbanken erhält, um den direkten Informationsaustausch zwischen den zuständigen nationalen Behörden zügig abwickeln zu können;

- die jeweiligen nationalen Stellen bzw. Büros für SIRENE, Europol und Interpol beherbergt;

- die Anlaufstelle für die Verbindungsbeamten, die gemäß dem "schwedischen Rahmenbeschluss" und den Prüm-Beschlüssen benannten Kontaktstellen sowie gegebenenfalls die Anlaufstellen für regionale und bilaterale Büros beherbergt;

- in einer gesicherten Arbeitsumgebung eingerichtet ist und – einschließlich Übersetzungs- oder Dolmetschkapazitäten – über eine ausreichende und angemessene Personalausstattung verfügt, damit sie täglich rund um die Uhr tätig sein kann. Das Personal sollte so weit wie möglich geschult und ausgestattet/beauftragt sein, um alle Arten von Aufgaben innerhalb der SPOC übernehmen zu können. Wenn dies nicht möglich ist, sollte dafür gesorgt werden, dass alle Aufgaben von täglich rund um die Uhr erreichbaren Beamten im Bereitschaftsdienst erledigt werden können;

- eine behördenübergreifende Organisation ist, deren Personal verschiedenen Dienststellen und/oder Ministerien entstammt bzw. diesen angehört, einschließlich der Kriminalpolizei, des Grenzschutzes, des Zolls und der Justizbehörden.

Typische Struktur einer nationalen Anlaufstelle (SPOC)

Die Zentralstelle für operative Polizeizusammenarbeit (S.C.C.O.Pol), Plattform für den Informationsaustausch

Die Zentralstelle für operative Polizeizusammenarbeit (S.C.C.O.Pol) ist eine ***ministerienübergreifende*** *Struktur, der 67 Polizeibeamte, Gendarmen und Zollbeamte angehören. Die Richter bzw. Staatsanwälte des Büros für die internationale Zusammenarbeit in Strafsachen (BEPI) des Justizministeriums unterhalten in denselben Räumlichkeiten einen Basisdienst, um französische Anträge auf Ausstellung eines Europäischen Haftbefehls und auf Registrierung von Inhaftnahmeersuchen und ausländischen Rotecken in der nationalen Datei gesuchter Personen zu validieren.*

Um den erforderlichen ***übergreifenden Charakter*** *der drei Kooperationskanäle zu gewährleisten, wurde im August 2004 eine zentrale Anlaufstelle (C.C.P.) bei der S.C.C.O.Pol benannt. Ihre Aufgabe besteht hauptsächlich darin, die französischen Strafverfolgungsbehörden bei der Wahl des Instruments der polizeilichen Zusammenarbeit, das sich nach Art und Komplexität der laufenden Ermittlungen am besten eignet, zu unterstützen. Sie prüft die Rechtmäßigkeit der Anträge, nimmt erste Gegenkontrollen vor und lenkt die betreffenden Ermittlungen in die in Anbetracht des Ersuchens der Ermittler am besten geeigneten Kooperationskanäle. Nur Ersuchen in Bezug auf eine Schengen-Ausschreibung fallen in die ausschließliche Zuständigkeit von SIRENE Frankreich.*

Infolge einer erfolgreichen Ressourcenbündelung bearbeitet die S.C.C.O.Pol ***rund um die Uhr*** *auf einer* ***einzigen gesicherten Plattform*** *mit einer begrenzten Personalausstattung nahezu* ***350 000 Nachrichten*** *im Jahr.*

Durch die für mehrere Kanäle geltende Zuständigkeit der S.C.C.O.Pol kann diese die Vertretung Frankreichs in EU-Gremien (Gruppe SIS/VIS, Gruppe SIS/SIRENE, Gruppe der Leiter der nationalen Europol-Stellen (ENU)) oder Interpol-Stellen (Sitzung der Interpol-Kontaktbeamten, Ausschreibungsgruppe) gewährleisten und der in Frankreich für die Überwachung der Leitungsgremien von Interpol und Europol zuständigen Einheit der DRI (Abteilung für internationale Beziehungen) eine sachdienliche operative Stellungnahme vortragen.

1.2. SIRENE-Büros

Die SIRENE-Büros sind entscheidend für den SIS-Betrieb und den Informationsaustausch. In allen Mitgliedstaaten sind als Teil des Schengen-Besitzstands[7] ständige SIRENE-Büros als benannte Behörden eingerichtet (SIRENE steht für **S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntries – Antrag auf Zusatzinformationen bei der nationalen Eingangsstelle), die die zentrale Verantwortung für die nationale Sektion des Schengener Informationssystems (SIS II) wahrnehmen. Sie sind die Kontaktstellen für die SIRENE-Büros der anderen Vertragsparteien und die Verbindungsstelle zu den nationalen Behörden und Agenturen. Das SIS II ist ein System für Abfragen nach dem Treffer/kein-Treffer-Verfahren. Diese Büros tauschen rund um die Uhr Daten in Bezug auf SIS-II-Ausschreibungen aus[8], wobei als "Ausschreibung" ein Datensatz bezeichnet wird, der es den Behörden ermöglicht, Personen oder Gegenstände im Hinblick auf die Ergreifung geeigneter Maßnahmen zu identifizieren.

"Zusatzinformationen" sind definiert als nicht im SIS II gespeicherte, aber mit SIS-II-Ausschreibungen verknüpfte Informationen, die in folgenden Fällen bilateral oder multilateral durch Formulare ausgetauscht werden:

i) wenn ermöglicht werden soll, dass die Mitgliedstaaten einander bei Eingabe einer Ausschreibung konsultieren und benachrichtigen können;

ii) nach einem Treffer, damit die erforderlichen Maßnahmen ergriffen werden können;

iii) in Fällen, in denen die erforderlichen Maßnahmen nicht ergriffen werden können;

iv) bei Fragen zur Qualität der SIS-II-Daten;

v) bei Fragen der Kompatibilität und Priorität von Ausschreibungen;

vi) bei Fragen des Auskunftsrechts.

---

7 Siehe Schengener Durchführungsübereinkommen, ABl. L 239 vom 22.9.2000.

8 Siehe 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.

Der Austausch von Zusatzinformationen erfolgt im Einklang mit den Bestimmungen des SIRENE-Handbuchs[9] über die Kommunikationsinfrastruktur[10]. Das SIS II[11] hat im Vergleich zu seinem Vorgänger verbesserte Funktionen wie die Möglichkeit der Eingabe von Fingerabdrücken und Lichtbildern und neuer Arten von Gegenständen (gestohlene Luftfahrzeuge, Boote, Container, Zahlungsmittel) sowie die Möglichkeit für den für die Ausschreibung Verantwortlichen, verschiedene Ausschreibungen miteinander zu verknüpften. Das SIS II enthält Kopien Europäischer Haftbefehle, die direkt mit Ausschreibungen zu den betreffenden Personen verknüpft sind.

Die SIRENE-Büros erleichtern die Zusammenarbeit in polizeilichen Angelegenheiten und können auch beim Informationsaustausch außerhalb des SIS-II-Anwendungsbereichs gemäß den Bestimmungen, die zuvor unter die durch den **"schwedischen Rahmenbeschluss"** ersetzten Artikel 39 und 46 des Schengener Durchführungsübereinkommens fielen, eine Rolle spielen. Gemäß Artikel 12 Absatz 1 des "schwedischen Rahmenbeschlusses" werden die "Bestimmungen des Artikels 39 Absätze 1, 2 und 3 und des Artikels 46 des Übereinkommens zur Durchführung des Übereinkommens von Schengen (...), soweit sie den in diesem Rahmenabschluss vorgesehenen Austausch von Informationen und Erkenntnissen für die Zwecke strafrechtlicher Ermittlungen oder polizeilicher Erkenntnisgewinnungsverfahren betreffen, durch die Bestimmungen dieses Rahmenbeschlusses ersetzt".

1.3. Nationale Europol-Stellen (ENU)

Jeder Mitgliedstaat verfügt über eine benannte nationale Europol-Stelle (ENU), bei der es sich um die Verbindungsstelle zwischen Europol und den zuständigen nationalen Behörden handelt. Die von der ENU zu Europol entsandten Verbindungsbeamten sollten rund um die Uhr die Verbindung zwischen dem Europol-Sitz in Den Haag und den ENU in den 28 Mitgliedstaaten gewährleisten. Europol beherbergt ferner Verbindungsbeamte aus 10 Nicht-EU-Ländern und - Organisationen. Das Netz wird durch von Europol bereitgestellte gesicherte Kommunikationskanäle unterstützt.

---

9 Durchführungsbeschluss der Kommission vom 26. Februar 2013 über das SIRENE-Handbuch und andere Durchführungsbestimmungen für das Schengener Informationssystem der zweiten Generation (SIS II) (bekanntgegeben unter Aktenzeichen C(2013) 1043), ABl. L 71 vom 14.3.2013, S. 1.

10 Infolge der Schließung des SISNET-Mailnetzes können die SIRENE-Büros nunmehr den sTESTA-Maildienst nutzen. Andere Informationsaustauschvorgänge können über die Kommunikationskanäle sTESTA-Netz, SIENA oder I- 24/7 durchgeführt werden.

11 Bericht der Kommission an das Europäische Parlament und den Rat über die Evaluierung des Schengener Informationssystems der zweiten Generation (SIS II) nach den Artikeln 24 Absatz 5, 43 Absatz 3 und 50 Absatz 5 der Verordnung (EG) Nr. 1987/2006 in Verbindung mit den Artikeln 59 Absatz 3 und 66 Absatz 5 des Beschlusses 2007/533/JI, Dok. 15810/16 SIRIS 175 COMIX 860.

Europol[12] unterstützt die Strafverfolgungsbehörden der Mitgliedstaaten bei der Prävention und Bekämpfung von organisierter Kriminalität, schwerer internationaler Kriminalität und Terrorismus, wenn zwei oder mehr Mitgliedstaaten betroffen sind. Für Erhebung, Speicherung, Verarbeitung und Analyse personenbezogener Daten und den Austausch von Informationen und Erkenntnissen hängt Europol von den von den Mitgliedstaaten bereitgestellten Daten ab. In der Europol-Verordnung sind die verschiedene Unterrichtungsaufgaben sowie die Vorschriften über die Verwendung und den Austausch von Daten mit Dritten auf der Grundlage einer soliden Datenschutz- und Datensicherheitsregelung niedergelegt.

1.4. INTERPOL – Nationale Zentralbüros (NZB)

Die **Nationalen Zentralbüros (NZB)** bei den nationalen Polizeizentralen spielen eine wesentliche Rolle bei der Verarbeitung der von ihren Ländern bereitgestellten Daten im Interpol-Informationssystem. Sie sind zum direkten Zugriff auf das System berechtigt; dies schließt Folgendes ein:

- Aufzeichnung, Aktualisierung und Löschung von Daten unmittelbar in den polizeilichen Datenbanken der Organisation sowie die Herstellung von Verknüpfungen zwischen Daten;
- direkte Abfrage dieser Datenbanken;
- Nutzung der Interpol-Ausschreibungen und -Rundschreiben für die Übermittlung von Kooperationsersuchen und internationalen Ausschreibungen.

Die NZB können Daten rasch abfragen und abgleichen, wobei sie rund um die Uhr über den Zugang zu den Datenbanken verfügen, die Informationen über mutmaßliche Terroristen, gesuchte Personen, Fingerabdrücke, DNA-Profile, verlorene oder gestohlene Reisedokumente, gestohlene Kraftfahrzeuge, gestohlene Kunstwerke usw. enthalten.

---

[12] Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates, ABl. L 135 vom 24.5.2016, S. 53-114 (anwendbar seit dem 1. Mai 2017)

So weit wie möglichen sollten die Nationalen Zentralbüros den an der internationalen Polizeizusammenarbeit beteiligten Strafverfolgungsbehörden ihrer Länder den Zugang zum Informationssystem von Interpol ermöglichen. Die NZB kontrollieren die Stufen des Zugangs der anderen befugten Nutzer ihrer Länder zu den Diensten von Interpol und können verlangen, über Abfragen ihrer nationalen Datendanken durch andere Länder unterrichtet zu werden.

1.5. Nationale Prüm-Kontaktstellen

Mit den Prüm-Beschlüssen[13] wurde eine neue grenzüberschreitende Dimension der Bekämpfung der Kriminalität eröffnet, indem ein gegenseitiger grenzüberschreitender Zugang zu den benannten nationalen DNA-Datenbanken, zu den automatisierten Fingerabdruck-Identifizierungssystemen (AFIS) und den Fahrzeugregister-Datenbanken (VRD) vorgesehen wurde. Für die Übermittlung von Daten wird in jedem teilnehmenden Mitgliedstaat eine spezifische nationale Kontaktstelle für jede Art von Datenaustausch benannt[14]. Die Datenschutzbestimmungen und maßgeschneiderte Bestimmungen über Datensicherheit tragen dem spezifischen Charakter des Online-Zugangs zu den betreffenden Datenbanken Rechnung. Die Übermittlung personenbezogener Daten erfordert ein angemessenes Datenschutz- und Datensicherheitsniveau, das die Mitgliedstaaten gegenseitig prüfen und vor dem Beginn des Datenaustauschs billigen.

1.5.1. Nationale Prüm-Kontaktstelle – DNA und Fingerabdrücke

Im Falle von DNA- und Fingerabdruckdaten erfolgt der automatisierte Abgleich biometrischer Bezugsdaten auf der Grundlage eines Treffer-/Kein-Treffer-Verfahrens. Die Bezugsdaten ermöglichen keine unmittelbare Identifizierung des Betroffenen. Bei einem Treffer kann die nationale Kontaktstelle des anfragenden Mitgliedstaates daher um zusätzliche spezifische personenbezogene Daten ersuchen. Die Bereitstellung solcher zusätzlicher Daten muss im Wege von Amtshilfeverfahren – auch solcher, die nach dem "schwedischen Rahmenbeschluss" angenommen worden sind – beantragt werden und richtet sich nach dem nationalen Recht des ersuchten Mitgliedstaats einschließlich der Vorschriften über rechtlichen Beistand.

---

13 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.
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.

14 5010/15 JAI 1 DAPIX 1 ENFOPOL 1 CRIMORG 1.

1.5.1.1. Leitfaden mit bewährten Verfahren für Abfragen nach Fingerabdrücken

Bei der Nutzung der Prüm-Funktion der automatisierten Fingerabdruck-Abfrage sollte der ersuchende Mitgliedstaat den im Dokument *"Good Practices for consulting Member States' databases"* (Bewährte Verfahren für die Abfrage der Datenbanken der Mitgliedstaaten, Dok. 14885/1/08 REV 1) enthaltenen Empfehlungen folgen. Darin werden die begrenzten Abfragekapazitäten von **Fingerabdruckdatenbanken** eingeräumt und es wird empfohlen, folgende Vorgehensweisen auf operativer Ebene zu fördern:

- Die Frage, ob die Fingerabdruckdatenbanken der Mitgliedstaaten konsultiert werden sollten oder nicht und in welcher Reihenfolge solche Abfragen durchgeführt und wiederholt werden sollten, betrifft in jedem Einzelfall zu treffende Ermittlungsentscheidungen und sollte nicht systematisch im Voraus geregelt werden.

- Die Fingerabdruckdatenbanken anderer Mitgliedstaaten sollten grundsätzlich erst abgefragt werden, nachdem die eigenen Fingerabdruckdatenbanken des ersuchenden Mitgliedstaats abgefragt wurden.

- Bei der Entscheidung, ob die Datenbanken eines oder mehrerer Mitgliedstaaten abgefragt werden sollen, sollte insbesondere Folgendes berücksichtigt werden:

  – die Schwere des Falls

  – und/oder bestehende Ermittlungsansätze, insbesondere Informationen, die auf einen Mitgliedstaat oder eine Gruppe von Mitgliedstaaten hindeuten,

  – und/oder die spezifischen Erfordernisse der Ermittlung.

- Allgemeine Abfragen sollten nur erfolgen, wenn die Nummern 1 bis 3 der bewährten Verfahren ausgeschöpft worden sind.

Beispiele für den automatisierten Datenaustausch entsprechend den Prüm-Beschlüssen des Rates

2011 wurde bei den Ermittlungen in einem Mordfall genetisches Material in die tschechische nationale DNA-Datenbank eingegeben. Die Ermittlungen wurden gegen einen Tatverdächtigen geführt, der sich ins Ausland abgesetzt hatte. Das genetische Material stammte von einem Zigarettenstummel in einem Aschenbecher in der Wohnung, in der das Verbrechen verübt worden war. Bei einer Abfrage der österreichischen DNA-Datenbank im Jahr 2014 wurde festgestellt, dass dasselbe Profil in Österreich verarbeitet worden war. Im Rahmen der polizeilichen Zusammenarbeit wurden von den einzigen Anlaufstellen beider Länder weitere personenbezogene Daten ausgetauscht. Danach wurde die Strafjustizbehörde in Österreich kontaktiert und ersucht, den Verdächtigen im Wege der Rechtshilfe in Strafsachen zur Strafverfolgung in die Tschechische Republik zu überstellen.

2005 wurde bei den Ermittlungen in einem Fall von Raub genetisches Material in die tschechische nationale DNA-Datenbank eingegeben. 2014 wurde ein Verdächtiger nach Abfrage der österreichischen DNA-Datenbank identifiziert. Die österreichische Seite wurde über die einzigen Anlaufstellen um Übermittlung eines aktuellen Lichtbilds und anderer personenbezogener Daten ersucht.

1.5.2. Nationale Prüm-Kontaktstelle – Fahrzeugregisterdaten (VRD)

Was VRD anbelangt, so können Abfragen mit vollständiger Fahrgestellnummer in allen Mitgliedstaaten oder mit vollständiger Zulassungsnummer in einem bestimmten Mitgliedstaat durchgeführt werden. Der Informationsaustausch erfolgt über die nationalen einzigen Anlaufstellen, die sowohl für eingehende als auch für ausgehende Ersuchen benannt wurden. Die Mitgliedstaaten gewähren einander den Online-Zugang zu den nationalen VRD in Bezug auf

a) Eigentümer- oder Halterdaten sowie

b) Fahrzeugdaten.

Die Mitgliedstaaten verwenden für diesbezügliche Abfragen eine speziell für Prüm-bezogene Zwecke konzipierte Version der Softwareanwendung "Europäisches Fahrzeug- und Führerschein-Informationssystem (EUCARIS)". VRD-Abfragen unterscheiden sich insoweit von DNA- und Fingerabdruckabfragen, als sie bei Treffern sowohl personenbezogene als auch Bezugsdaten ausgeben. Wie bei anderen automatisierten Abfragen gilt, dass die Bereitstellung personenbezogener Daten dem von den Empfängermitgliedstaaten praktizierten angemessenen Datenschutzniveau entsprechen muss.

1.5.3. Nationale Prüm-Kontaktstelle – Terrorismusprävention

Die benannten nationalen Prüm-Kontaktstellen können auf Antrag oder von sich aus Informationen über Personen, die der Begehung terroristischer Straftaten verdächtig sind, austauschen. Die Daten umfassen Familiennamen, Vornamen, Geburtsdatum und - ort des Verdächtigen und eine Beschreibung der Gegebenheiten, die zu der Überzeugung geführt haben, dass der Betroffene in Verbindung mit terroristischen Aktivitäten stehende Straftaten begehen wird.

Der übermittelnde Mitgliedstaat kann nach Maßgabe des innerstaatlichen Rechts Bedingungen für die Verwendung dieser Daten und Informationen durch den empfangenden Mitgliedstaat, der an diese Bedingungen gebunden ist, festlegen.

1.5.4. Nationale Prüm-Kontaktstelle – Großveranstaltungen

Mitgliedstaaten, in denen Großveranstaltungen mit internationaler Dimension stattfinden, müssen die Sicherheit der Veranstaltung sowohl unter dem Aspekt der öffentlichen Ordnung als auch unter dem Aspekt der Terrorismusbekämpfung gewährleisten. Je nach der Art der Veranstaltung (politischer, sportlicher, sozialer, kultureller oder anderer Art) kann einer dieser Aspekte relevanter sein als der andere. Beide Aspekte müssen jedoch berücksichtigt werden, auch wenn möglicherweise verschiedene Behörden befasst sind. Dem Phänomen der reisenden Gewalttäter (travelling violent offenders/TVO) wird, insbesondere in Bezug auf internationale Fußballspiele, besondere Aufmerksamkeit gewidmet.

Für die Zwecke der Prävention von Straftaten und der Wahrung der öffentlichen Ordnung und Sicherheit im Zusammenhang mit Großveranstaltungen und ähnlichen (politischen, sportlichen, gesellschaftlichen, kulturellen oder anderen) Massenveranstaltungen sowie Katastrophen und schweren Unglücksfällen mit grenzüberschreitenden Auswirkungen übermitteln die benannten nationalen Kontaktstellen auf Antrag oder auf eigene Initiative einander Folgendes:

- nicht-personenbezogene Daten oder
- personenbezogene Daten, wenn rechtskräftige Verurteilungen oder andere Umstände Anlass zu der Vermutung geben, dass die Betroffenen auf den Veranstaltungen Straftaten begehen oder eine Bedrohung der öffentlichen Ordnung und Sicherheit darstellen werden.

Die personenbezogenen Daten dürfen nur zu den vorgenannten Zwecken und für die angegebenen Veranstaltungen, für die sie mitgeteilt wurden, verarbeitet werden. Die Daten sind unverzüglich zu löschen, sobald die damit verfolgten Zwecke erreicht wurden, spätestens aber nach einem Jahr. Die Informationen werden nach Maßgabe des innerstaatlichen Rechts des übermittelnden Mitgliedstaats übermittelt.

1.5.4.1. Leitfaden für die Zusammenarbeit bei Großveranstaltungen mit internationaler Dimension[15]

Dieser Leitfaden enthält Leitlinien und Anregungen für Strafverfolgungsbehörden, die mit der Gewährleistung der öffentlichen Sicherheit bei größeren Veranstaltungen wie den Olympischen Spielen oder anderen größeren Veranstaltungen sportlicher oder sozialer Art oder bei politischen Tagungen auf hoher Ebene betraut sind.

Das Handbuch, das entsprechend der Weiterentwicklung der bewährten Verfahren kontinuierlich geändert und angepasst wird, enthält Leitvorgaben für das Informations- und Veranstaltungsmanagement sowie zur veranstaltungsbezogenen und strategischen Evaluierung. Die in der Anlage enthaltenen Standardformblätter betreffen Folgendes:

- Ersuchen um Entsendung von Verbindungsbeamten;
- Risikoanalyse betreffend potenzielle Demonstranten und andere Gruppierungen;
- Austausch von Informationen über Personen oder Gruppen, die eine terroristische Bedrohung darstellen;
- eine Aufstellung von Bezugsdokumenten;
- eine Tabelle mit den Angaben zu den Ständigen Kontaktstellen für den Bereich der öffentlichen Sicherheit.

1.6. Nationale Fußballinformationsstellen (der Polizei) (NFIP)[16]

Über die nationale Prüm-Kontaktstelle für Großveranstaltungen hinaus und mit besonderer Berücksichtigung internationaler Fußballspiele ist in jedem Mitgliedstaat eine nationale Fußballinformationsstelle (NFIP) damit beauftragt, einschlägige Informationen auszutauschen und die grenzüberschreitende polizeiliche Zusammenarbeit weiterzuentwickeln. Die taktischen, strategischen und operativen Informationen können von der NFIP selbst verwendet werden oder werden den zuständigen Behörden oder Polizeidienststellen zugeleitet.

Die Kontakte zwischen den Polizeidienststellen der einzelnen von einer Großveranstaltung betroffenen Länder werden von der NFIP koordiniert und gegebenenfalls organisiert. Die auf dem CIV basierende Website für NFIP (www.nfip.eu) verbreitet Informationen und Empfehlungen in Bezug auf die verfügbaren rechtlichen und sonstigen Optionen für die Sicherheit bei Fußballspielen.

---

15 Empfehlung des Rates vom 6. Dezember 2007 betreffend einen Leitfaden für die Polizei- und Sicherheitsbehörden zur Zusammenarbeit bei Großveranstaltungen mit internationaler Dimension (2007/C 314/02), ABl. C 314 vom 22.12.2007, S. 4.

16 Beschluss 2002/348/JI des Rates vom 25. April 2002 über die Sicherheit bei Fußballspielen von internationaler Bedeutung, ABl. L 121 vom 8.5.2002, S. 1.

Die NFIP koordiniert die Verarbeitung der Informationen über Risikofans im Hinblick auf die Vorbereitung und die Ergreifung geeigneter Maßnahmen zur Aufrechterhaltung der öffentlichen Ordnung bei einer Fußballveranstaltung. Zu diesen Informationen gehören insbesondere die Detailangaben zu Personen, die eine reale oder potenzielle Bedrohung der öffentlichen Ordnung und Sicherheit darstellen. Der Informationsaustausch sollte mithilfe der entsprechenden Formulare[17] im Anhang des Fußballhandbuchs erfolgen.

1.6.1. Fußballhandbuch[18]

Das Fußballhandbuch ist der Entschließung 2006/C 322/01 des Rates im Anhang beigefügt und vermittelt der Polizei Beispiele dafür, wie sie auf internationaler Ebene kooperieren sollte, um Gewalttätigkeiten und Störungen im Zusammenhang mit Fußballspielen vorzubeugen und sie zu bekämpfen. Der Inhalt besteht insbesondere aus Empfehlungen betreffend

- das Informationsmanagement durch die Polizeidienststellen;
- die Organisation der Zusammenarbeit zwischen den Polizeidienststellen;
- die Checkliste "Medienpolitik und Kommunikationsstrategie" (für die Polizei/Behörden).

1.7. Zentren für die Zusammenarbeit von Polizei und Zoll (PCCC)

PCCC werden auf der Grundlage bi- oder multilateraler Vereinbarungen gemäß Artikel 39 Absatz 4 des Schengener Durchführungsübereinkommens (SDÜ) eingerichtet. In diesen Vereinbarungen legen die Vertragsparteien die Grundlagen für ihre grenzüberschreitende Zusammenarbeit, unter anderem auch die Aufgaben der PCCC sowie den Rechtsrahmen und die Verfahren für die Einrichtung und die Arbeitsweise der PCCC, fest. Die PCCC bringen Personal aus benachbarten Ländern zusammen und sind eng verbunden mit den nationalen Stellen, die mit der internationalen Zusammenarbeit befasst sind (nationale Anlaufstellen, Interpol-NZB, nationale Europol-Stellen, SIRENE-Büros).

---

17 Beschluss 2007/412/JI des Rates vom 12. Juni 2007 zur Änderung des Beschlusses 2002/348/JI über die Sicherheit bei Fußballspielen von internationaler Bedeutung, ABl. L 155 vom 15.6.2007, S. 76.

18 Entschließung des Rates betreffend ein aktualisiertes Handbuch mit Empfehlungen für die internationale polizeiliche Zusammenarbeit und Maßnahmen zur Vorbeugung und Bekämpfung von Gewalttätigkeiten und Störungen im Zusammenhang mit Fußballspielen von internationaler Dimension, die zumindest einen Mitgliedstaat betreffen ("EU-Fußballhandbuch") (2016/C 444/01), ABl. C 444 vom 29.11.2016, S. 1.

Die PCCC unterstützen die nationalen operativen Polizeikräfte, den Zoll und andere Agenturen mit Beratungsleistungen und nicht operativer Unterstützung in der Grenzregion, in der sie sich befinden. Das Personal der PCCC hat die Aufgabe, gemäß dem Beschluss 2006/960/JI des Rates ("schwedischer Rahmenbeschluss") angeforderte Informationen bereitzustellen.

Ende 2016 waren 8 der 59 bestehenden PCCC mit SIENA, der Europol-Netzanwendung für sicheren Datenaustausch, verbunden. Die über die PCCC ausgetauschten Informationen betreffen hauptsächlich die kleine und mittlere Kriminalität, die illegale Migration und Störungen der öffentlichen Ordnung. Hierbei kann es sich auch um die Feststellung der Identität von Fahrern oder die Überprüfung der rechtmäßigen Verwendung und Echtheit von Identitäts- und Reisedokumenten handeln.

Die Vertragsparteien können gemeinsam beschließen, ein PCCC in ein operatives regionales Koordinierungszentrum umzuwandeln, das allen betroffenen Stellen zu Diensten steht, insbesondere im Falle unvorhergesehener regionaler Ereignisse (Naturkatastrophen) oder größerer geplanter Ereignisse (Olympische Spiele, Fußballweltmeisterschaft usw.).

Sollten einem PCCC dennoch Informationen zugehen, die in den Zuständigkeitsbereich der nationalen Zentralstellen fallen, so muss es die Informationen unverzüglich den einzigen Anlaufstellen/Zentralstellen zuleiten. Sollte ein PCCC Informationen von offensichtlichem Interesse für Europol erhalten, so kann es diese Informationen der in der einzigen Kontaktstelle angesiedelten nationalen Europol-Stelle zuleiten, die sie dann an Europol selbst weiterleitet.

Beispiel für den Informationsaustausch über ein PCCC

EPICC ("Euregio Police Information and Cooperation Centre") ist die Kurzbezeichnung des PCCC Heerlen.

Das Zentrum wurde 2005 ad hoc (ohne speziellen Rechtsakt) auf Initiative von "NeBeDeAgPol", einer Vereinigung von Polizeichefs in der Euregio Maas-Rhein im Grenzgebiet zwischen den Niederlanden, Belgien und Deutschland – einem der am dichtesten bevölkerten Grenzgebiete der Europäischen Union – gegründet.

In diesem PCCC arbeiten etwa dreißig belgische, deutsche und niederländische Polizeibeamte in einer Plattform zusammen.

Diese Beamten haben von der Plattform aus Zugang zum Großteil der Inhalte der Datenbanken ihrer jeweiligen Länder. Dies ermöglicht ihnen, innerhalb kürzester Zeit mit präzisen, vollständigen und zuverlässigen Antworten auf polizeiliche Informationsersuchen, die Belgien, Deutschland oder die Niederlande betreffen, zu reagieren. Der Informationsaustausch zwischen den drei Delegationen innerhalb des EPICCC erfolgt über die Europol-Anwendung "SIENA".

EPICCC sammelt und analysiert polizeiliche Informationen in der Grenzregion, um Probleme für die Grenzsicherheit (neue Phänomene oder Modi operandi, in der Grenzregion tätige Gruppen von Kriminellen, Veranstaltungen oder Personen, denen besondere Aufmerksamkeit zu widmen ist, usw.) zu ermitteln, zu beschreiben und weiterzuverfolgen.

Dank seiner Fachkompetenz und gemischten Zusammensetzung kann das PCCC Heerlen bei der Vorbereitung und Durchführung grenzüberschreitender Einsätze, Ermittlungen oder Überwachungsmaßnahmen effiziente Unterstützung leisten.

1.8. Verbindungsbeamte

Gemäß Artikel 47 des Schengener Durchführungsübereinkommens (SDÜ) können die Mitgliedstaaten "*bilaterale Absprachen über die befristete oder unbefristete Entsendung von Verbindungsbeamten [eines Mitgliedstaats] zu Polizeidienststellen [eines anderen Mitgliedstaats] treffen*". Die Rolle der Verbindungsbeamten ist es, direkte Kontakte zu knüpfen und aufrechtzuerhalten, um die Zusammenarbeit für die Zwecke der Kriminalitätsbekämpfung – insbesondere durch Unterstützungsleistungen – zu fördern und zu beschleunigen. Die Verbindungsbeamten sind nicht befugt, selbstständig polizeiliche Maßnahmen zu treffen. Sie gewährleisten eine rasche und effiziente Zusammenarbeit auf der Grundlage persönlicher Kontakte und gegenseitigen Vertrauens, indem sie

- die Sammlung und den Austausch von Informationen erleichtern und beschleunigen;
- Ersuchen um polizeiliche Hilfe und Rechtshilfe in Strafsachen erledigen;
- grenzüberschreitende Einsätze organisieren und sicherstellen.

Verbindungsbeamte können in andere Mitgliedstaaten oder Drittstaaten oder zu EU-Agenturen oder internationalen Organisationen entsandt werden. Das Kompendium für Verbindungsbeamte auf dem Gebiet der Strafverfolgung[19], das alljährlich vom Generalsekretariat des Rates aktualisiert wird, erläutert die Arbeit und die Aufgaben der Verbindungsbeamten und enthält Listen von Verbindungsbeamten einschließlich der Kontaktangaben.

Auf der Grundlage vergangener und aktueller Erfahrungen in verschiedenen Gastländern und im Hinblick auf eine stärkere Bündelung der Tätigkeiten der Mitgliedstaaten gegenüber Drittländern hinsichtlich der Arbeit der Verbindungsbeamten und der technischen Zusammenarbeit wurden einige bewährte Verfahren herausgearbeitet, die im Kompendium festgehalten sind. Es wird vorgeschlagen, dass die Verbindungsbeamten der Mitgliedstaaten und ihre jeweiligen Behörden diese anwenden, wann immer dies zweckmäßig erscheint.

---

[19] "Update of the Compendium on law enforcement liaison officers (2018)" (Dok. 10095/1/18 REV 1 ENFOPOL 397 JAIEX 84 COMIX 422).

Typische Beispiele für den Informationsaustausch zwischen Verbindungsbeamten

- *Die Verbindungsbeamten können damit betraut werden, den Kontakt sicherzustellen, um eine unmittelbare Zusammenarbeit in speziellen Fällen wie etwa bei Drogendelikten herzustellen.*
- *Die Verbindungsbeamten können spezifische Informationen über nationale Vorschriften und Rechtsvorschriften über die internationale polizeiliche Zusammenarbeit oder die Rechtshilfe in Strafsachen bereitstellen.*
- *In einigen Fällen führen die Verbindungsbeamten auf dem neuesten Stand gehaltene Verzeichnisse der in ihrem Mitgliedstaat zuständigen Behörden.*
- *Die Verbindungsbeamten sind ferner in einigen Mitgliedstaaten damit betraut worden, Ersuchen um Zusammenarbeit nach Artikel 17 des Prüm-Beschlusses (gemeinsame Einsatzformen) zu bearbeiten. So wurde beispielsweise der dänische Verbindungsbeamte bei Europol von der Tschechischen Republik ersucht, ein Ersuchen an Dänemark weiterzuleiten, in dem um die Zuweisung von vier dänischen Polizeibeamten zur Unterstützung in einem beide Mitgliedstaaten betreffenden Fall ersucht wurde.*

1.9. Vermögensabschöpfungsstellen (ARO) der Mitgliedstaaten

Die Finanzkriminalität deckt eine breite Palette von Aktivitäten ab, so etwa Geldfälschung, Korruption und Betrug (beispielsweise Kreditkartenbetrug, Hypothekenbetrug, medizinischer Betrug und Wertpapierbetrug, Bestechung oder Veruntreuung, Geldwäsche, Identitätsdiebstahl und Steuerumgehung). Eine bessere Zusammenarbeit wird erreicht durch eine engere grenzüberschreitende Zusammenarbeit zwischen den Vermögensabschöpfungsstellen (ARO), den Zentralstellen für Geldwäsche-Verdachtsanzeigen (FIU) sowie den Polizei- und Zollbehörden[20].

Im Anschluss an die Annahme des Beschlusses 2007/845/JI des Rates vom 6. Dezember 2007 über die Zusammenarbeit zwischen den Vermögensabschöpfungsstellen der Mitgliedstaaten auf dem Gebiet des Aufspürens und der Ermittlung von Erträgen aus Straftaten oder anderen Vermögensgegenständen im Zusammenhang mit Straftaten[21] haben unterdessen alle Mitgliedstaaten Vermögensabschöpfungsstellen (ARO) eingerichtet und benannt. Diese Facheinheiten haben sich zu einem eng verflochtenen Netz von Fachleuten entwickelt, das direkt über das SIENA-System Informationen über Angelegenheiten in Bezug auf Abschöpfung von Vermögenswerten austauschen kann. Unter der Schirmherrschaft der Europäischen Kommission und Europols erleichtert das ARO-Netz die Zusammenarbeit zwischen den Vermögensabschöpfungsstellen der Mitgliedstaaten und die strategische Erörterung und den Austausch bewährter Verfahren. Das Europol-Büro für Erträge aus Straftaten (ECAB) fungiert als Zentralstelle für die Abschöpfung von Vermögenswerten innerhalb der EU.

Mit der Richtlinie 2014/42/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Sicherstellung und Einziehung von Tatwerkzeugen und Erträgen aus Straftaten in der Europäischen Union[22] soll die Wirksamkeit der Zusammenarbeit zwischen den Vermögensabschöpfungsstellen innerhalb der Europäischen Union weiter verbessert werden. Die Mitgliedstaaten sind aufgefordert, die Richtlinie bis zum 4. Oktober 2016 umzusetzen.

---

20 Handbuch bewährter Vorgehensweisen zur Bekämpfung der Finanzkriminalität: Eine Sammlung von Beispielen ausgereifter Systeme zur Bekämpfung der Finanzkriminalität in den Mitgliedstaaten (Dok. 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144).

21 Beschluss 2007/845/JI des Rates vom 6. Dezember 2007 über die Zusammenarbeit zwischen den Vermögensabschöpfungsstellen der Mitgliedstaaten auf dem Gebiet des Aufspürens und der Ermittlung von Erträgen aus Straftaten oder anderen Vermögensgegenständen im Zusammenhang mit Straftaten, ABl. L 332 vom 18.12.2007, S. 103.

22 Richtlinie 2014/42/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Sicherstellung und Einziehung von Tatwerkzeugen und Erträgen aus Straftaten in der Europäischen Union, ABl. L 127 vom 29.4.2014, S. 39.

Das **Camdener zwischenstaatliche Netz der Vermögensabschöpfungsstellen (CARIN)**, das 2004 eingerichtet wurde, um Aufspüren, Einfrieren, Beschlagnahme und Einziehung von Vermögenswerten im Zusammenhang mit Straftaten über die Grenzen hinweg zu unterstützen, verbessert den gegenseitigen Austausch von Informationen über verschiedene über die EU hinausreichende nationale Ansätze.

Seit 2015 umfasst das CARIN Angehörige der Rechtsberufe aus 53 Hoheitsgebieten und 9 internationalen Organisationen, die als Kontaktstellen für die Zwecke eines raschen – auf Antrag oder auf eigene Initiative erfolgenden – grenzüberschreitenden Informationsaustauschs dienen. Die nationalen Geldabschöpfungsstellen arbeiten untereinander oder mit anderen Behörden, die das Aufspüren und die Ermittlung von Erträgen aus Straftaten erleichtern, zusammen. Zwar haben alle Mitgliedstaaten eine Geldabschöpfungsstelle eingerichtet, aber es bestehen noch größere Unterschiede zwischen den Mitgliedstaaten in Bezug auf Organisationsstruktur, Ressourcen und Tätigkeiten.

Die ausgetauschten Informationen können entsprechend den Datenschutzvorschriften des empfangenden Mitgliedstaaten verwendet werden und unterliegen den gleichen Datenschutzvorschriften, die auch gelten würden, wenn die Informationen im empfangenden Mitgliedstaat erhoben worden wären. Der spontane Informationsaustausch nach dem betreffenden Beschluss unter Einhaltung der im schwedischen Rahmenbeschluss vorgesehenen Verfahren und Fristen muss gefördert werden.

1.10. Geldwäsche – Zusammenarbeit zwischen den Zentralstellen für Geldwäsche-Verdachtsanzeigen (FIU)[23][24]

Einschlägige Informationen über alle Tatsachen, die ein Indiz für Geldwäsche oder Terrorismusfinanzierung sein könnten, sollten den nationalen zentralen Meldestellen (FIU) gemeldet werden. Die zentralen Meldestellen werten in jedem Einzelfall die erhaltenen Informationen aus, um Bezüge zwischen verdächtigen Transaktionen und zugrunde liegenden strafbaren Handlungen festzustellen und auf diese Weise Geldwäsche und Terrorismusfinanzierung zu verhüten und zu bekämpfen. Die zentralen Meldestellen fungieren als eine zentrale nationale Stelle für den Erhalt und die Auswertung von Informationen und die Weiterleitung der Auswertungsergebnisse an die zuständigen Behörden. Die zentralen Meldestellen sind in operativer Hinsicht unabhängig und autonom und nehmen ihre Aufgaben eigenständig war, einschließlich der autonomen Entscheidung, spezifische Informationen zu analysieren, anzufragen und weiterzuleiten.

---

23 Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Festlegung von Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten und zur Aufhebung des Beschlusses 2000/642/JI des Rates, ABl. L 186 vom 11.7.2019, S. 122.

24 Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission, ABl. L 141 vom 5.6.2015, S. 73.

Die zentralen Meldestellen dienen auch als nationale Kontaktstellen für den grenzüberschreitenden Austausch von Informationen. Wie bei den Vermögensabschöpfungsstellen gibt es zwischen den Mitgliedstaaten beträchtliche Unterschiede in Bezug auf ihre Organisationsstruktur, Funktionen und Ressourcen. Sie unterstehen entweder Justizbehörden oder sind innerhalb von Polizeieinrichtungen angesiedelt oder "hybrid" konzipiert und in diesem Fall mit einer Kombination von polizeilichen und staatsanwaltschaftlichen Befugnissen ausgestattet. Diese Vielfalt kann sich manchmal als hinderlich für die internationale Zusammenarbeit erweisen.

Angesichts des länderübergreifenden Charakters der Geldwäsche und der Terrorismusfinanzierung sind jedoch die Koordinierung und Zusammenarbeit zwischen den zentralen Meldestellen außerordentlich wichtig. In der Richtlinie (EU) 2015/849 sind detaillierte Bestimmungen festgelegt, um diese Koordinierung und Zusammenarbeit zu verbessern und sicherzustellen, dass Meldungen verdächtiger Transaktionen die zentrale Meldestelle des Mitgliedstaats, für den sie besonders relevant sind, tatsächlich erreichen. Um rasch, konstruktiv und wirksam eine möglichst weitreichende grenzüberschreitende Zusammenarbeit zu erreichen, sollten die Mitgliedstaaten insbesondere gewährleisten, dass ihre zentralen Meldestellen frei, spontan oder auf Antrag Informationen mit den zentralen Meldestellen von Drittländern austauschen.

Für die Verbesserung des Informationsaustauschs zwischen den zentralen Meldestellen in der Union bedarf es der Nutzung gesicherter Einrichtungen, insbesondere des dezentralisierten FIU.NET-Computernetzes. Alle 28 zentralen Meldestellen sind an das Netz FIU.NET angeschlossen. FIU.NET hat sich in den letzten Jahren von einem sicheren Basiswerkzeug für einen strukturierten bilateralen Informationsaustausch zu einem sicheren Multifunktionswerkzeug für den multilateralen Informationsaustausch entwickelt, dass auch über Fallverwaltungsfunktionen sowie eine halbautomatische Standardisierung der Prozesse verfügt. Im FIU.NET sind jede neue Funktion und die automatische Verarbeitung optional, ohne Auflagen. Die einzelne zentrale Meldestelle kann entscheiden, welche der vom FIU.NET gebotenen Möglichkeiten und Funktionen sie nutzen will; sie nutzt die Funktionen, mit denen sie gut zurecht kommt, und schließt die Funktionen aus, die sie nicht nutzen muss oder will.

1.11. Neapel-II-Übereinkommen[25]

Die Mitgliedstaaten unterstützen einander im Rahmen des Neapel- II-Abkommens, um Verstöße gegen nationale Zollvorschriften zu verhüten und aufzuspüren und Verstöße gegen gemeinschaftliche und nationale Zollvorschriften zu verfolgen und zu bestrafen. In Bezug auf strafrechtliche Ermittlungen enthält das Übereinkommen Bestimmungen, wonach die Zollverwaltungen gemeinsam handeln und auf eigene Initiative oder auf Antrag Daten über illegale Handelsvorgänge austauschen können.

Ersuchen werden in einer Amtssprache des Mitgliedstaats der ersuchten Behörde oder in einer von dieser zugelassenen Sprache gestellt. In einem Formular ist der Standard für die Informationsübermittlung vorgegeben. Die betreffenden Behörden übermitteln alle Informationen, die für die Verhütung, Aufklärung und Verfolgung von Verstößen hilfreich sein können. Sie tauschen personenbezogene Daten aus, d. h. alle Informationen zu einer bestimmten oder bestimmbaren natürlichen Person.

Bei der erbetenen Amtshilfe verfährt die ersuchte Behörde oder die von ihr befasste zuständige Behörde so, als ob sie in Erfüllung eigener Aufgaben oder auf Ersuchen einer anderen Behörde ihres eigenen Mitgliedstaats handeln würde.

Der Leitfaden zum Übereinkommen über gegenseitige Amtshilfe und Zusammenarbeit der Zollverwaltungen (Neapel II) ist in drei Teile gegliedert:

- die allgemeinen Bestimmungen in Dok. 13615/05 ENFOCUSTOM 61 + COR 1 (CZ);
- die nationalen Merkblätter in der aktualisierten Fassung von 2016, Dok. 15429/16 JAI 1028 ENFOCUSTOM 238;
- die Anlagen, einschließlich der Musterformulare für die Übermittlung von Informationen in Dok. 13615/05 ENFOCUSTOM 61 ADD 1.

[25] Rechtsakt des Rates vom 18. Dezember 1997 über die Ausarbeitung des Übereinkommens aufgrund von Artikel K.3 des Vertrags über die Europäische Union über gegenseitige Amtshilfe und Zusammenarbeit der Zollverwaltungen, ABl. C 24 vom 23.1.1998, S. 1.

1.12. PNR-Zentralstelle

Gemäß der Richtlinie 2016/681[26] richtet jeder Mitgliedstaat eine PNR-Zentralstelle ein bzw. benennt eine solche Stelle. Diese Stellen sind für die Verarbeitung der von den Fluggesellschaften übermittelten Fluggastdatensätze (PNR-Daten) zuständig[27] und stellen außerdem den wesentlichen Kanal für den Informationsaustausch zwischen den Mitgliedstaaten und mit Europol dar. Zwei oder mehr Mitgliedstaaten können gemeinsam eine einzige Behörde errichten oder benennen, die als ihre gemeinsame PNR-Zentralstelle handelt.

Die Verarbeitung der PNR-Daten dient vor allem der Überprüfung von Fluggästen, um Personen zu ermitteln, die von den für die Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität zuständigen nationalen Behörden eingehender überprüft werden müssen. Die Richtlinie gilt für Drittstaatsflüge und kann auch auf EU-Flüge angewandt werden, wenn ein Mitgliedstaat dies beschließt.

Die Überprüfung von PNR-Daten erleichtert die Ermittlung von Personen, die vor einer solchen Überprüfung nicht der Beteiligung an terroristischen Straftaten oder schwerer Kriminalität verdächtig waren. Gemäß der EU-Datenschutzpolitik sollte die Verarbeitung solcher Daten sowohl relevant als auch erforderlich sein und in einem angemessenen Verhältnis zu den mit dieser Richtlinie verfolgten spezifischen Sicherheitsinteressen stehen.

---

26 Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. L 119 vom 4.5.2016, S. 132.

27 Die Richtlinie hindert die Mitgliedstaaten nicht daran, nach ihrem jeweiligen nationalen Recht eine Regelung zur Erhebung und Verarbeitung von PNR-Daten durch Wirtschaftsteilnehmer, die keine Beförderungsunternehmen sind, wie etwa Reisebüros oder Reiseveranstalter, die Dienstleistungen im Zusammenhang mit Reisen – einschließlich Flugbuchungen – erbringen, für die sie PNR-Daten erheben und verarbeiten, oder durch andere als in der Richtlinie angegebene Beförderungsunternehmen vorzusehen, sofern dieses nationale Recht mit dem Unionsrecht in Einklang steht.

Die PNR-Zentralstellen sind für folgende Aufgaben zuständig:

- auf nationaler Ebene für die Erhebung der PNR-Daten bei den Fluggesellschaften, die Speicherung und Verarbeitung dieser Daten sowie die Übermittlung der Daten oder des Ergebnisses ihrer Verarbeitung an die zuständigen nationalen Behörden;

- auf Ebene der Union für den Austausch der PNR-Daten und des Ergebnisses ihrer Verarbeitung

    a) untereinander. In Notfällen und unter bestimmten Bedingungen können die oben genannten zuständigen nationalen Behörden jedoch bei der PNR-Zentralstelle jedes anderen Mitgliedstaats PNR-Daten, die in deren Datenbank aufbewahrt werden, direkt anfordern; und

    b) mit Europol, das berechtigt ist, im Rahmen seiner Zuständigkeiten und zur Ausübung seiner Aufgaben solche Daten von den PNR-Zentralstellen anzufordern.

Die PNR-Zentralstellen üben ihre Aufgaben ausschließlich an einem gesicherten Ort im Hoheitsgebiet eines Mitgliedstaats aus. An die PNR-Zentralstellen übermittelte PNR-Daten müssen für einen Zeitraum von fünf Jahren ab ihrer Übermittlung an die PNR-Zentralstelle des Mitgliedstaats, in dem der Flug ankommt oder von dem er abgeht, in einer Datenbank gespeichert werden. Alle PNR-Daten müssen jedoch sechs Monate nach ihrer Übermittlung durch Unkenntlichmachung der in der Richtlinie festgelegten Datenelemente, mit denen die Identität des Fluggasts unmittelbar festgestellt werden könnte, depersonalisiert werden. Die Ergebnisse der Verarbeitung werden von der PNR-Zentralstelle nur so lange aufbewahrt, wie dies erforderlich ist, um die zuständigen nationalen Behörden und die PNR-Zentralstellen anderer Mitgliedstaaten über einen Treffer zu informieren.

Die PNR-Zentralstelle verarbeitet nur die in Anhang I der Richtlinie aufgeführten Daten zu folgenden Zwecken:

- Überprüfung von Fluggästen vor ihrer planmäßigen Ankunft in einem Mitgliedstaat oder vor ihrem Abflug von einem Mitgliedstaat, um diejenigen Personen zu ermitteln, die von den nationalen Behörden und gegebenenfalls von Europol genauer überprüft werden müssen;

- im Einzelfall Beantwortung von Anfragen der zuständigen Behörden hinsichtlich der Zurverfügungstellung und Verarbeitung von PNR-Daten in besonderen Fällen und der Zurverfügungstellung der Ergebnisse dieser Verarbeitung an die zuständigen Behörden und gegebenenfalls an Europol;

- Analyse von PNR-Daten zwecks Aktualisierung der Kriterien oder Aufstellung neuer Kriterien, die zur Ermittlung von Fluggästen angewandt werden, die möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind.

Bei der Durchführung solcher Überprüfungen kann die PNR-Zentralstelle die PNR-Daten entweder mit Datenbanken, die zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität maßgeblich sind, unter Einhaltung der für solche Datenbanken einschlägigen nationalen, internationalen und Unionsvorschriften abgleichen oder die PNR-Daten anhand von im Voraus festgelegten Kriterien verarbeiten. Diese vorher festgelegten Kriterien müssen zielgerichtet, verhältnismäßig und spezifisch sein. Es obliegt den PNR-Zentralstellen, diese Kriterien aufzustellen und in Zusammenarbeit mit den maßgeblichen zuständigen Behörden regelmäßig zu überprüfen. Diese Kriterien dürfen nicht auf sensiblen personenbezogenen Daten wie etwa der Rasse oder ethnischen Herkunft, politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen, der Gewerkschaftszugehörigkeit, dem Gesundheitszustand, dem Sexualleben oder der sexuellen Orientierung beruhen.

Die PNR-Zentralstelle übermittelt alle relevanten und erforderlichen PNR-Daten oder die Ergebnisse der Verarbeitung dieser Daten von Personen, die ermittelt wurden, den entsprechenden PNR-Zentralstellen der anderen Mitgliedstaaten. Diese PNR-Zentralstellen leiten die erhaltenen Daten an ihre eigenen zuständigen Behörden weiter.

Der von der PNR-Zentralstelle ernannte Datenschutzbeauftragte ist für die Überwachung der Verarbeitung der PNR-Daten zuständig. Eine betroffene Person hat das Recht, den Datenschutzbeauftragten als zentrale Kontaktstelle im Zusammenhang mit allen Fragen bezüglich der Verarbeitung der PNR-Daten der betroffenen Person zu kontaktieren.

Alle von den Fluggesellschaften vorgenommenen Übermittlungen von PNR-Daten an die PNR-Zentralstellen erfolgen mittels elektronischer Hilfsmittel, die die technische Sicherheit gewährleisten. Zu diesem Zweck sind sowohl die gemeinsamen Protokolle, die die Fluggesellschaften bei der Datenübermittlung einhalten müssen, als auch die unterstützten Datenformate, die gewährleisten, dass alle maßgeblichen Parteien die Daten lesen können, auf der Ebene der Union festgelegt[28].

---

28 Durchführungsbeschluss (EU) 2017/759 der Kommission vom 28. April 2017 über die gemeinsamen Protokolle und Datenformate, die von den Fluggesellschaften für die Übermittlung von Fluggastdatensätzen (PNR-Daten) an PNR-Zentralstellen zu verwenden sind, ABl. L 113 vom 29.4.2017, S. 48.

1.13. Nationale Zugangsstellen – EES

Das Einreise-/Ausreisesystem [29] (EES) dient hauptsächlich der Verbesserung des Außengrenzenmanagements der Union und wird zu diesem Zweck von Grenz-, Einwanderungs- und Visumbehörden genutzt[30]. Mit diesem System werden Zeitpunkt und Ort der Ein- und Ausreise bestimmter Drittstaatsangehöriger, die für einen Kurzaufenthalt im Hoheitsgebiet der Mitgliedstaaten zugelassen sind, elektronisch erfasst und wird die Dauer des zulässigen Aufenthalts berechnet. Das EES wird an den Außengrenzen betrieben. Die Mitgliedstaaten, die den Schengen-Besitzstand vollständig anwenden, führen das EES an ihren Binnengrenzen mit den Mitgliedstaaten ein, die den Schengen-Besitzstand noch nicht vollständig anwenden, sich aber am EES-Betrieb beteiligen oder nicht beteiligen. Mitgliedstaaten, die den Schengen-Besitzstand noch nicht vollständig anwenden, führen keine biometrischen Funktionen ein.

Zusätzlich zu den Grenz-, Einwanderungs- und Visumbehörden sind auch die von den einzelnen Mitgliedstaaten "benannten Behörden" unter den in der Verordnung festgelegten Voraussetzungen zur Abfrage des EES berechtigt. Sie führen EES-Abfragen zu Strafverfolgungszwecken durch sowie zur Ermöglichung der Erstellung von Informationen für Ermittlungen im Zusammenhang mit terroristischen oder sonstigen schweren Straftaten, einschließlich der Identifizierung von Tätern, Verdächtigen und Opfern derartiger Straftaten, die die Außengrenzen überschritten haben.

Die Mitgliedstaaten benennen die Behörden, die berechtigt sind, das EES zu Strafverfolgungszwecken abzufragen. Zudem benennt jeder Mitgliedstaat eine zentrale Zugangsstelle für das EES. Die zentrale Zugangsstelle ist von den benannten Behörden getrennt, nimmt ihre Aufgaben völlig unabhängig von den benannten Behörden wahr und sollte in Bezug auf den Ausgang der Verifizierung, d.h. den Abgleich von Datensätzen zur Überprüfung einer Identitätsangabe, von den benannten Behörden keine Anweisungen entgegennehmen, damit gewährleistet ist, dass die Verifizierung unabhängig durchgeführt wird. Nur die ordnungsgemäß ermächtigten Mitarbeiter der zentralen Zugangsstelle sind zum Zugriff auf das EES ermächtigt.

---

29 Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten der Europäischen Union und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011 (ABl. L 327 vom 9.12.2017, S. 20).

30 Die Kommission bestimmt den Zeitpunkt, zu dem das EES seinen Betrieb aufnimmt, nachdem die Voraussetzungen nach Artikel 66 der Verordnung (EU) Nr. 2017/2226 erfüllt sind

Operative Stellen innerhalb der benannten Behörden sind berechtigt, EES-Daten über die zentralen Zugangsstellen zu beantragen. Zu diesem Zweck muss die operative Stelle bei einer zentralen Zugangsstelle einen begründeten elektronischen oder schriftlichen Antrag auf Zugang zu EES-Daten stellen. Die zentrale Zugangsstelle prüft, ob die in der Verordnung festgelegten Zugangsbedingungen erfüllt sind, und bearbeitet den Antrag im Falle eines positiven Ergebnisses. Die EES-Daten werden dann der operativen Stelle so übermittelt, dass die Sicherheit der Daten nicht beeinträchtigt wird.

Folgende Voraussetzungen für den Zugang zu EES-Daten für Strafverfolgungszwecke sind zu prüfen:

- Der Zugang zum Zwecke von Abfragen ist für Strafverfolgungszwecke erforderlich;
- der Zugang zum Zwecke von Abfragen ist im Einzelfall erforderlich und verhältnismäßig;
- es liegen Beweise oder hinreichende Gründe für die Annahme vor, dass die Abfrage der EES-Daten zur Verhütung, Aufdeckung oder Untersuchung der betreffenden Straftaten beiträgt, insbesondere, wenn ein erheblicher Verdacht besteht, dass der Verdächtige, der Täter oder das Opfer einer terroristischen oder sonstigen schweren Straftat einer Personengruppe angehört, die unter die Verordnung fällt.

Zudem ist der Zugang zum EES als Instrument zur Identifizierung von Verdächtigen, Tätern oder Opfern derartiger Straftaten zulässig, wenn folgende Bedingungen erfüllt sind:

- Die nationalen Datenbanken wurden zuvor abgefragt, und
- im Falle einer Suche anhand von Fingerabdrücken wurde zuvor eine Abfrage gemäß dem Beschluss 2008/615/JI des Rates ("Prüm-Beschluss") durchgeführt, wenn Abgleiche von Fingerabdrücken technisch möglich sind, und diese Abfrage wurde entweder vollständig durchgeführt oder diese Abfrage war nicht innerhalb von zwei Tagen, nachdem sie gestartet wurde, vollständig abgeschlossen.

Ein Antrag auf eine Abfrage im VIS zu derselben betroffenen Person kann parallel zu einem Antrag auf eine Abfrage im EES gemäß den im Beschluss 2008/633/JI des Rates [31] festgelegten Bedingungen gestellt werden.

Schließlich ist der Zugang zum EES als Instrument zur Abfrage von Daten zu den bisherigen Reisen oder Aufenthalten im Hoheitsgebiet der Mitgliedstaaten von bekannten Verdächtigen, Straftätern oder mutmaßlichen Opfern terroristischer oder sonstiger schwerer Straftaten zulässig, wenn die oben genannten Grundsätze erfüllt sind.

1.14. Nationale ETIAS-Stellen[32]

Das Europäische Reiseinformations- und -genehmigungssystem (ETIAS) unterstützt[33] den Informationsaustausch für die Zwecke des Grenzmanagements, der Strafverfolgung und der Terrorismusbekämpfung. ETIAS dient dazu, vor der Einreise eines von der Visumpflicht befreiten Drittstaatsangehörigen in den Schengen-Raum und vor seiner Ankunft an Außengrenzübergangsstellen festzustellen, ob dieser zur Einreise berechtigt ist. ETIAS stellt eine Reisegenehmigung bereit, die sich naturgemäß von einem Visum unterscheidet, jedoch eine Voraussetzung für die Einreise und den Aufenthalt darstellt und anzeigt, dass mit dem Antragsteller kein Risiko für die Sicherheit, kein Risiko der illegalen Einwanderung und kein hohes Epidemierisiko verbunden ist.

ETIAS besteht aus

- dem ETIAS-Informationssystem, einschließlich der ETIAS-Überwachungsliste;
- der ETIAS-Zentralstelle, die zur Europäischen Agentur für die Grenz- und Küstenwache gehört,
- den nationalen ETIAS-Stellen.

---

31 Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten, ABl. L 218 vom 13.8.2008, S. 129.

32 Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226 (ABl. L 236 vom 19.9.2018, S. 1).
Verordnung (EU) 2018/1241 des Europäischen Parlaments und des Rates vom 12. September 2018 zur Änderung der Verordnung (EU) 2016/794 für die Zwecke der Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) (ABl. L 236 vom 19.9.2018, S. 72).

33 Die Kommission wird den Zeitpunkt bestimmen, zu dem das ETIAS seinen Betrieb aufnehmen wird, sobald die Voraussetzungen gemäß Artikel 88 der Verordnung (EU) 2018/1240 erfüllt sind.

Hat die automatisierte Antragsbearbeitung eine Übereinstimmung ("Treffer") zwischen den in dem Antragsdatensatz gespeicherten Daten und den Daten in den ETIAS-Informationssystemen, spezifischen Risikoindikatoren oder Ausschreibungen in den abgefragten EU-Informationssystemen ergeben, so ist die ETIAS-Zentralstelle dafür zuständig, diesen Treffer zu überprüfen und, wenn eine Übereinstimmung bestätigt wird oder wenn Zweifel bestehen bleiben, die manuelle Antragsbearbeitung gemäß Artikel 26 in dem genannten Mitgliedstaat einzuleiten.

Anschließend ist es die nationale ETIAS-Stelle des betreffenden Mitgliedstaats, die den betreffenden Antrag manuell bearbeitet. Sie erhält Zugriff auf den Antragsdatensatz und damit verbundene Antragsdatensätze sowie auf alle Treffer, die die automatisierte Bearbeitung ergeben hat. Nach der manuellen Bearbeitung erteilt oder verweigert die zuständige nationale Stelle letztlich gemäß den Bestimmungen der Verordnung eine Reisegenehmigung. Zu diesem Zweck kann die nationale Stelle zusätzliche Angaben oder Unterlagen anfordern.

Eine Reisegenehmigung wird verweigert, wenn der Antragsteller

- ein Reisedokument verwendet hat, das im SIS als verloren, gestohlen, unterschlagen oder für ungültig erklärt gemeldet worden ist;
- ein Risiko für die Sicherheit darstellt;
- ein Risiko der illegalen Einwanderung darstellt;
- ein hohes Epidemierisiko darstellt;
- im SIS zur Einreise- und Aufenthaltsverweigerung ausgeschrieben ist;
- ein Ersuchen um Übermittlung zusätzlicher Angaben oder Unterlagen nicht beantwortet oder nicht zu einer Befragung erscheint.

Die nationalen ETIAS-Stellen sind für die Prüfung der Anträge zuständig und entscheiden über die Erteilung, Verweigerung, Annullierung oder Aufhebung von Reisegenehmigungen. Bei der Beurteilung der Anträge sollten die nationalen ETIAS-Stellen miteinander und mit Europol kooperieren.

Eine nationale Stelle kann entscheiden, eine Reisegenehmigung zu verweigern, eine Reisegenehmigung zu annullieren, wenn sich herausstellt, dass die Voraussetzungen für ihre Erteilung zum Zeitpunkt der Erteilung nicht erfüllt waren, oder eine Reisgenehmigung aufzuheben, wenn sich herausstellt, dass die Voraussetzungen für ihre Erteilung nicht mehr erfüllt sind. Den betreffenden Antragstellern steht ein Rechtsmittel zu. Etwaige Rechtsmittel sind in dem Mitgliedstaat, der über die Verweigerung, Annullierung oder Aufhebung entschieden hat und im Einklang mit dem nationalen Recht dieses Mitgliedstaats einzulegen. Die zuständige nationale Stelle hat zur Aufgabe, die Antragsteller über das bei Einlegung eines Rechtsmittels zu befolgende Verfahren zu unterrichten.

Die für die Durchführung der Grenzübertrittskontrollen an den Außengrenzübergangsstellen zuständigen Grenzbehörden führen Abfragen des ETIAS-Zentralsystems anhand der in der maschinenlesbaren Zone des Reisedokuments gespeicherten Daten durch. Die Einwanderungsbehörden haben zur Prüfung oder Verifizierung, ob die Voraussetzungen für die Einreise in das oder den Aufenthalt im Hoheitsgebiet der Mitgliedstaaten erfüllt sind, Zugang zum ETIAS-Zentralsystem.

Die von den Mitgliedstaaten benannten Strafverfolgungsbehörden sind nur in bestimmten Fällen und nur dann, wenn dies zur Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten erforderlich ist, berechtigt, die Abfrage von im ETIAS-Zentralsystem gespeicherten personenbezogenen Daten zu beantragen. Die Richtlinie (EU) 2016/680 ("Polizeirichtlinie") gilt für die Verarbeitung solcher personenbezogener Daten durch die benannten Behörden der Mitgliedstaaten gemäß der ETIAS-Verordnung.

1.15. Interoperabilität

Hauptziel des "Pakets zur Interoperabilität" ist die Verbesserung der Datenverwaltungsarchitektur der Union im Bereich der Grenzkontrolle und der Sicherheit [34]zur Erleichterung der korrekten Identifizierung von Personen, die keine EU-Bürger sondern Drittstaatsangehörige sind. Die Interoperabilität zwischen dem EES (siehe Nr. 3.19), VIS (siehe Nr. 3.8), ETIAS (siehe Nr. 3.20), Eurodac (siehe Nr. 3.9), SIS (siehe Nr. 3.2) und ECRIS-TCN (siehe Nr. 3.14.1) soll ermöglichen, dass diese Informationssysteme der EU einander ergänzen. Zu diesem Zweck müssen ein Europäisches Suchportal (European search portal - ESP), ein gemeinsamer Dienst für den Abgleich biometrischer Daten (biometric matching service – BMS), ein gemeinsamer Speicher für Identitätsdaten (common identity repository – CIR) und ein Detektor für Mehrfachidentitäten (multiple-identity detector – MID) geschaffen werden[35].

a) Um die systematische Nutzung der oben genannten EU-Informationssysteme zu gewährleisten, sollten die benannten Behörden mit Zugangsberechtigung zu mindestens einem dieser Systeme, dem CIR und dem MID, zu Europol-Daten oder zu den Interpol-Datenbanken SLTD und TDAWN (siehe Nr. 2.4), das ESP verwenden, welches die gleichzeitige Abfrage dieser Informationssysteme ermöglicht.

b) Im gemeinsamen Speicher für Identitätsdaten (CIR) wird eine individuelle Datei für jede in diesen Informationssystemen erfasste Person angelegt; der CIR ist als gemeinsame Speichereinheit für Identitäts-, Reisedokumenten- und biometrische Daten von in den Systemen erfassten Personen zu verstehen. Der CIR sollte Teil der technischen Architektur der Systeme sein und als gemeinsame Komponente von ihnen für die Speicherung und Abfrage der von ihnen verarbeiteten Identitäts-, Reisedokumenten- und biometrischen Daten dienen.

---

[34] Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27). Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862, und (EU) 2019/816, ABl. L 135 vom 22.5.2019, S. 85

[35] Die Kommission wird den Zeitpunkt bestimmen, ab dem die Vorschriften der Verordnungen über das ESP, den gemeinsamen Dienst BMS, den CIR und den MID Anwendung finden.

Der Zugang zum CIR wird zu Zwecken folgender Art gewährt:

- zur korrekten Identifizierung der in den EU-Informationssystemen erfassten Personen, oder, soweit erforderlich,

- zur Unterstützung der Strafverfolgungsbehörden bei der Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten.

Ist eine Polizeibehörde aus verschiedenen Gründen nicht in der Lage, eine Person zu identifizieren, so kann sie eine Abfrage im CIR vornehmen. Zu diesem Zweck ermächtigen die Mitgliedstaaten ihre zuständige Behörde auf der Grundlage der nationalen Rechtsvorschriften, dies zu tun, und legen die Verfahren, Bedingungen und Kriterien für derartige Identitätskontrollen fest. Die Abfrage wird entweder anhand unmittelbar zuvor abgenommener Fingerabdrücke der betreffenden Person durchgeführt oder, sollte dies nicht möglich sein, anhand von Identitätsdaten der Person in Verbindung mit Reisedokumentendaten.

Ergibt die Abfrage, dass Daten über die Person im CIR gespeichert sind, so erhält die Polizeibehörde Auskunft über Namen, Vornamen, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Geschlecht, frühere Namen und gegebenenfalls – sofern verfügbar – über Pseudonyme oder Aliasnamen sowie Angaben zu den Reisedokumenten. Zudem darf die Polizei, sofern sie nach nationalem Recht dazu ermächtigt ist, im Falle einer Naturkatastrophe, eines Unfalls oder eines Terroranschlags und ausschließlich zum Zwecke der Identifizierung unbekannter Personen, die sich nicht ausweisen können, oder nicht identifizierter menschlicher Überreste Abfragen im CIR anhand von biometrischen Daten vornehmen.

CIR-Abfragen für Strafverfolgungszwecke: Insbesondere wenn ein Verdacht besteht, dass es sich bei einem Verdächtigen, Täter oder Opfer einer terroristischen oder schweren Straftat um eine Person handelt, deren Daten in den Informationssystemen erfasst sind, dürfen die benannten Behörden und Europol den CIR abfragen, um zu erfahren, ob Daten zu einer bestimmten Person gespeichert sind. Sind solche Daten vorhanden, so zeigt der CIR im Anschluss an die automatische Prüfung auf Vorliegen einer Übereinstimmung im System anhand der "Übereinstimmungskennzeichnungsfunktion“ (match-flag functionality) eine Referenz an, die auf das Informationssystem mit den übereinstimmenden Daten verweist. Diese Antwort in Form einer Übereinstimmungskennzeichnung sollte nur dazu verwendet werden, einen Antrag auf Zugang zu dem betreffenden EU-Informationssystem zu übermitteln. Eine derartige Antwort sollte außer dem Hinweis, dass Daten der betroffenen Person in einem der EU-Informationssysteme gespeichert sind, keine personenbezogenen Daten anzeigen.

Ermächtigte Endnutzer sollten keine die betroffene Person beschwerenden Entscheidungen treffen, die sich allein auf das Vorliegen einer Übereinstimmungskennzeichnung gründen. Der Zugriff des Endnutzers auf eine Übereinstimmungskennzeichnung sollte somit einen nur sehr begrenzten Eingriff in das Recht der betroffenen Person auf Schutz ihrer personenbezogenen Daten darstellen; gleichzeitig würde dies den benannten Behörden aber erlauben, effizientere Anträge auf Zugang zu personenbezogenen Daten zu stellen. Der vollständige Zugang zu Daten für Strafverfolgungszwecke unterliegt weiterhin den in der Eurodac-Verordnung festgelegten Bedingungen und Verfahren (siehe Nr. 2.7)

c) Mit dem Detektor für Mehrfachidentitäten (MID) werden Verknüpfungen zwischen den in den einzelnen EU-Informationssystemen erfassten Daten hergestellt und gespeichert. Bei der Strafverfolgung wird eine MID-Prüfung im CIR und im SIS eingeleitet, wenn eine Personenausschreibung im SIS erstellt oder aktualisiert wird oder wenn im ECRIS-TCN ein Datensatz angelegt oder geändert wird. Diese Prüfung wird nur durchgeführt, um Daten, die in einem EU-Informationssystem vorhanden sind, mit Daten in einem anderen EU-Informationssystem zu vergleichen. Die Verifizierung verschiedener Identitäten ist von dem betreffenden SIRENE-Büro oder den betreffenden Zentralbehörden manuell vorzunehmen.

Die Kommission wird

- den Zeitpunkt bestimmen, ab dem die Vorschriften der Verordnungen über das ESP, den gemeinsamen Dienst BMS, den CIR und den MID Anwendung finden;
- in enger Zusammenarbeit mit den Mitgliedstaaten, eu-LISA und anderen zuständigen Stellen der Union ein Handbuch für die Umsetzung und den Betrieb der Interoperabilitätskomponenten zur Verfügung stellen. Das Handbuch soll technische und operative Leitlinien, Empfehlungen und bewährte Verfahren enthalten.

1.16. Wahl des Kommunikationskanals – allgemein verwendete Kriterien

In einem Mitgliedstaat erfüllt eine einzige Anlaufstelle[36] eine entscheidende Funktion bei der Bestimmung des am besten geeigneten und maßgeblichsten Kanals, da bei ihr alle von der Einheit bearbeiteten (eingehenden und ausgehenden) Ersuchen zusammenlaufen. Im Interesse der Effizienz räumen die nationalen Behörden den Ermittlern eine beträchtliche Autonomie bei der Wahl des für die Ermittlungen am besten geeigneten Kanals ein. Folgendes sind generell die meistgenutzten Kommunikationskanäle:

[36] Leitlinien für eine einzige Anlaufstelle, 10492/14 DAPIX 75 ENFOPOL 157 und 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1.

- SIRENE über die SIS-Anlaufstellen jedes Schengen-Staates
- Europol über die nationalen Europol-Stellen/Europol-Verbindungsbeamten
- Interpol über die nationalen Zentralbüros in den Polizeizentralen
- Verbindungsbeamte
- die zwischen den Zollbehörden genutzten Amtshilfekanäle (Neapel-II-Übereinkommen)
- bilaterale Kanäle auf der Grundlage von Kooperationsvereinbarungen auf nationaler, regionaler und lokaler Ebene (PCCC).

Die allgemeine Regelung sieht vor, dass ein Ersuchen nur über einen Kanal übermittelt wird. In Ausnahmefällen kann ein Ersuchen auch gleichzeitig über verschiedene Kanäle übermittelt werden. In diesen Fällen sollte dies allen Parteien auf angemessene Weise eindeutig angegeben werden. Analog hierzu muss auch ein Wechsel des Kanals allen Beteiligten zusammen mit den Gründen für diesen Wechsel mitgeteilt werden.

Zur Vermeidung thematischer Überschneidungen oder von Situationen, in denen ein Ersuchen unnötigerweise über mehrere Kanäle übermittelt wird, kann der zuständige Sachbearbeiter (SIS, Europol, Interpol, bilateraler Verbindungsbeamter) im ersuchenden Staat anhand der nachstehenden Kriterien den am besten geeigneten Übermittlungsweg für ein Informationsersuchen bestimmen:

- geografische Kriterien, d. h. Staatsangehörigkeit/Wohnsitz/Herkunft der betreffenden Person bzw. der betreffenden Sache ist bekannt und das Ersuchen betrifft die Übermittlung von Einzelheiten (Adresse, Telefonnummer, Fingerabdrücke, DNA, Registrierung usw.);
- thematische Kriterien, d. h. organisierte Kriminalität, schwere Kriminalität, Terrorismus; Vertraulichkeit/Empfindlichkeit; Kanal, der für mit dem vorliegenden Fall in Verbindung stehende frühere Ersuchen verwendet wurde;
- technische Kriterien, d. h. die Notwendigkeit sicherer IT-Kanäle;
- Dringlichkeitskriterien, d. h. ein unmittelbares Risiko für die physische Integrität einer Person, unmittelbar bevorstehender Verlust von Beweismaterial, Ersuchen um dringende grenzüberschreitende Einsätze oder Überwachungsmaßnahmen.

2. INFORMATIONSSYSTEME

2.1. Schengener Informationssystem der zweiten Generation (SIS II)[37]

Gegenwärtig ist das Schengener Informationssystem der zweiten Generation ("SIS II") in 26 EU-Mitgliedstaaten sowie in vier mit der Schengen-Zusammenarbeit assoziierten Nicht-EU-Staaten (Norwegen, Island, Schweiz und Liechtenstein) in Betrieb. Es unterstützt die operative Zusammenarbeit zwischen Polizei- und Justizbehörden in Strafsachen. Da das SIS ein System sowohl der Polizeizusammenarbeit als auch der Grenzkontrolle ist, können benannte Polizei-, Grenzschutz- und Zollbeamte sowie Visum- und Justizbehörden im gesamten Schengen-Raum das SIS konsultieren[38].

SIS-II-Daten können (unter Einhaltung strenger Datenschutzvorschriften) rund um die Uhr über Zugangspunkte in den SIRENE-Büros, an den Grenzübergangsstellen, innerhalb des nationalen Hoheitsgebiets und in den konsularischen Vertretungen im Ausland abgefragt werden. Die Datenbank erfasst Daten sowohl zu Personen als auch zu Gegenständen und ermöglicht den Datenausaustausch für die Zwecke der Verhütung von Straftaten und zur Bekämpfung der irregulären Einwanderung. Durch Online-Abfrage von SIS stellt der untersuchende Beamte auf "Treffer/kein Treffer-Basis" rasch fest, ob eine überprüfte Person in der Datenbank aufgeführt ist oder nicht.

Die Daten werden als Ausschreibungen bezeichnet, wobei unter Ausschreibungen Datensätze zu verstehen sind, die den Behörden die Identifizierung von Personen oder Gegenständen ermöglichen, sodass sie geeignete Maßnahmen ergreifen können:

Ausschreibungen zu **Personen** (sowohl Unionsbürger als auch Drittstaatsangehörige). Diese erleichtern Maßnahmen wie die folgenden:

– Festnahmen zum Zwecke der Übergabehaft auf der Grundlage entweder des Europäischen Haftbefehls oder von Abkommen zwischen der EU und Drittländern oder aber für Auslieferungszwecke;

– Suche nach dem Verbleib vermisster Personen;

– Vorladungen vor ein Gericht im Zusammenhang mit einem Strafverfahren oder der Vollstreckung einer Freiheitsstrafe;

---

37 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.

38 Eine Liste der zuständigen nationalen Behörden, die das Recht auf Zugang zu den Ausschreibungen besitzen, wird alljährlich im *Amtsblatt der Europäischen Union* veröffentlicht.

– verdeckte und gezielte Kontrollen im Hinblick auf die Verfolgung von Straftaten, Abwehr von Bedrohungen der öffentlichen Sicherheit oder Abwehr von Bedrohungen der nationalen Sicherheit;

– Verweigerung der Einreise von eigenen Staatsangehörigen oder Ausländern in den Schengen-Raum infolge einer behördlichen oder gerichtlichen Entscheidung oder aufgrund einer Bedrohung der öffentlichen Sicherheit und Ordnung oder aufgrund der Nichteinhaltung nationaler Regelungen für die Einreise und den Aufenthalt von Ausländern.

SIS-II-Ausschreibungen zu **Gegenständen** werden für verdeckte oder gezielte Kontrollen, zum Zwecke der Beschlagnahme, zur Verwendung als Beweismittel in Strafverfahren oder zu Überwachungszwecken eingestellt. Diese Ausschreibungen können sich auf Folgendes beziehen:

– Fahrzeuge, Wasserfahrzeuge, Luftfahrzeuge oder Container;

– Feuerwaffen;

– gestohlene Dokumente;

– Banknoten;

– gestohlenes Eigentum wie Kunstgegenstände, Boote und Schiffe.

Besonders ermächtigte Bedienstete von Europol können im Rahmen ihres Mandats Auskunft über die in das SIS II eingegebenen Daten einholen und diese unmittelbar abfragen und können den betreffenden Mitgliedstaat um weitere Informationen ersuchen.

Die nationalen Eurojust-Mitglieder und ihre Assistenten haben das Recht, im Rahmen ihres Mandats auf die in das SIS II eingegebenen Daten zuzugreifen und diese abzufragen.

2.2. EIS – Europol-Informationssystem[39]

Mit der Europol-Verordnung wird ein neues Konzept für die Datenverarbeitung, das als Konzept zur integrierten Datenverwaltung (Integrated Data Management Concept – IDMC) bezeichnet wird, eingeführt. Das IDMC kann als die Möglichkeit definiert werden, Kriminalität betreffende Informationen zu vielfältigen Geschäftszwecken wie vom Dateneigentümer angegeben zu nutzen; dadurch wird die Verwaltung und die Verarbeitung in integrierter und technologieneutraler Weise ermöglicht. Nach dem Europol-Beschluss des Rates war die Datenverarbeitung nach Systemen strukturiert. Die Europol-Verordnung enthält nicht mehr Bezugnahmen auf Systeme, sondern schreibt stattdessen vor, dass Verarbeitungszwecke angegeben werden. Damit ein reibungsloser Übergang gewährleistet wird, können die Nutzer weiterhin mit den vorhandenen Systemen auf eine Weise arbeiten, die mit dem neuen Rechtsrahmen vereinbar ist.

Das Europol-Informationssystem (EIS), auf das im Europol-Beschluss Bezug genommen wird, ist ein von Europol betriebenes zentrales System, das es den Mitgliedstaaten und den Kooperationspartnern von Europol ermöglicht, Daten zu verdächtigen Personen, verurteilten Straftätern oder "potenziellen künftigen Straftätern", die mit unter das Mandat von Europol fallenden Straftaten (Schwerkriminalität, organisierte Kriminalität oder Terrorismus) zu tun haben, zu speichern, auszutauschen und abzugleichen. Es ermöglicht die Speicherung der ganzen Bandbreite von Daten und Beweisen im Zusammenhang mit den betreffenden Straftaten/Personen, z. B. zu Personen mit Aliasnamen, Unternehmen, Fernsprechnummern, E-Mail-Adressen, Fahrzeugen, Feuerwaffen, DNA, Lichtbildern, Fingerabdrücken, Bomben usw.). Das Europol-Informationssystem, das in erster Linie als ein System für den Abgleich dient, bietet einen Zugriff nach dem Treffer/kein-Treffer-Verfahren. Die Europol-Verordnung sieht einen uneingeschränkten Zugriff auf Daten vor, die zu Zwecken der strategischen oder themenbezogenen Analyse übermittelt wurden, aber nur einen Zugriff nach dem Treffer/kein-Treffer-Verfahren auf Daten, die für operative Analysen übermittelt wurden.

Das EIS ist faktisch ein Referenzsystem, mit dessen Hilfe festgestellt werden kann, ob gesuchte Informationen in einem der EU-Mitgliedstaaten, bei Kooperationspartnern oder bei Europol verfügbar sind oder nicht. Es ist in allen Mitgliedstaaten und für ordnungsgemäß ermächtigte Europol-Bedienstete verfügbar. Gegenwärtig können die Mitgliedstaaten auf drei verschiedene Arten Daten hochladen:

a) durch manuelle Aufnahme von Daten in das EIS oder über SIENA;

---

39 Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates, ABl. L 135 vom 24.5.2016, S. 53-114 (anwendbar seit dem 1. Mai 2017)

b) durch halbautomatischen Transfer, indem ein Batch-Upload im EIS durchgeführt wird;

c) durch automatischen Datentransfer, indem ein Datenloader verwendet wird.

Die Daten im EIS werden in den weitaus meisten Fällen über automatisierte Datenladesysteme eingegeben. Das Datenerhebungskonzept der Mitgliedstaaten hat sich gewandelt, denn der Schwerpunkt bei der Datenübermittlung hat sich auf Komponenten verlagert, zu denen ein Abgleich erfolgen kann, wie etwa Personen, Fahrzeuge, Fernsprechnummern und Feuerwaffen.

Drittstaaten können nicht direkt Daten in das EIS eingeben oder im EIS abgleichen, aber gemäß Artikel 23 Absatz 5 der Europol-Verordnung können sie die Daten an Europol senden. Europol wird zunächst prüfen müssen, ob die Daten unter das Europol-Mandat fallen, und nimmt nur in diesem Fall die Daten entgegen und führt den Abgleich der Daten durch.

Das EIS, das den Austausch hoch sensibler Informationen ermöglicht, verfügt über ein solides System, das Vertraulichkeit und Sicherheit gewährleistet. Die Sicherheit wird beispielsweise durch spezifische Bearbeitungscodes gewährleistet. Diese geben an, was mit bestimmten Informationen geschehen kann und wer Zugang zu ihnen hat. Die Bearbeitungscodes sind so konzipiert, dass die Informationsquelle geschützt bleibt und die Verarbeitung der Informationen entsprechend den Wünschen des Eigentümers der Informationen und gemäß dem nationalen Recht des Mitgliedstaats gewährleistet sind. Das EIS ist für die Verarbeitung von Informationen bis zum Geheimhaltungsgrad "EU RESTRICTED" (einschließlich) akkreditiert.

2.3. SIENA – die Europol-Netzanwendung für sicheren Datenaustausch

SIENA ist das sichere Kommunikationssystem von Europol, das von den Mitgliedstaaten, Europol und seinen Kooperationspartnern für den Austausch operativer und strategischer Informationen und Erkenntnisse in Bezug auf Straftaten, einschließlich operativer Daten zu Personen, verwendet wird. SIENA ist ein Mitteilungssystem, das verschiedene Arten von Mitteilungen zu verschiedenen Zwecken bietet, einschließlich des Datenaustauschs gemäß dem "schwedischen Rahmenbeschluss".

Bei Konzeption und Funktionsweise von SIENA wurde erheblicher Wert auf Sicherheit, Datenschutz und Vertraulichkeit gelegt. SIENA ist für den Austausch von Informationen des Geheimhaltungsgrads "EU CONFIDENTIAL" akkreditiert. Beim Datenaustausch über SIENA gibt es klare Verantwortlichkeiten für die Datenverarbeitung. Für jede abgehende SIENA-Meldung müssen die Klassifikation (Vertraulichkeit), die Bearbeitungscodes und die Zuverlässigkeit der Quellen und der Informationen angegeben werden.

Die Standardsprache der SIENA-Nutzerschnittstelle ist Englisch, die Schnittstelle ist aber mehrsprachig und ermöglicht damit den SIENA-Operatoren, in ihrer bzw. ihren eigenen Landessprache(n) zu arbeiten. Neben dem Austausch von Nachrichten können die SIENA-Operatoren Abfragen durchführen und statistische Berichte über die über SIENA ausgetauschten Daten erstellen.

SIENA unterstützt den bilateralen Datenaustausch zwischen Mitgliedstaaten und ermöglicht ihnen auch den Austausch von Daten außerhalb des Europol-Mandats. Erfolgt der Datenaustausch mit einem der Kooperationspartner von Europol, so erhalten die Mitgliedstaaten eine Meldung über SIENA, dass dieser Austausch nur stattfinden sollte, wenn er Straftaten betrifft, die unter das Europol-Mandat fallen.

Europol wird die über SIENA ausgetauschten Informationen nur dann für die Zwecke der operativen Datenverarbeitung bearbeiten, wenn Europol bei dem Datenaustausch als Adressat einbezogen wurde. Für Überprüfungszwecke sind alle über SIENA ausgetauschten Daten dem Datenschutzbeauftragten von Europol und den nationalen Überwachungsstellen zugänglich.

SIENA unterstützt den strukturierten Datenaustausch auf der Grundlage des UMF-Formats (Universal Message Format). Derzeit kann die UMF-Komponente PERSON in der SIENA-Netzanwendung selbst angelegt/angezeigt werden. Das gesamte UMF-Datenmodell wird bereits vom SIENA-Webservice unterstützt.

2.4. I-24/7 – das globale Polizeikommunikationssystem von Interpol

I-24/7, das globale Netz für den Austausch von polizeilichen Informationen verbindet das Generalsekretariat von Interpol in Lyon (Frankreich), die nationalen Zentralbüros (NCB) in 190 Ländern sowie die regionalen Büros.

Das Interpol-Informationssystem ermöglicht eine direkte Nachrichtenkommunikation zwischen den NCB. Alle Interpol-Datenbanken (mit Ausnahme der Datenbank mit Bildern betreffend die sexuelle Ausbeutung von Kindern) sind in Echtzeit über I- 24/7 zugänglich. I-24/7 ermöglicht es den Mitgliedstaaten auch, über eine direkte (B2B-)Verbindung auf die nationalen Datenbanken der anderen Mitgliedstaaten zuzugreifen. Die Mitgliedstaaten behalten und verwalten ihre eigenen nationalen strafrechtlich relevanten Daten und kontrollieren deren Vorlage, den Zugang anderer Länder zu den Daten und deren Vernichtung entsprechend ihrem nationalen Recht. Sie haben auch die Option, sie den internationalen Strafverfolgungsbehörden über I- 24/7 zugänglich zu machen.

2.4.1. Interpol: DNA-Gateway

Die DNA-Datenbank von Interpol umfasst eine internationale DNA-Datenbank, ein Formular für eine internationale Suchanfrage für den bilateralen Austausch und ein Mittel für die sichere standardisierte elektronische Übermittlung. Es werden keine namenbezogenen Daten aufbewahrt, die ein DNA-Profil mit einer bestimmten Person verknüpfen. Die DNA-Gateway ist mit dem automatisierten Datenaustausch im Prüm-Rahmen kompatibel.

Die Mitgliedstaaten haben Zugang zu der Datenbank, und auf Antrag kann der Zugang über die nationalen Zentralbüros hinaus auch gerichtsmedizinischen Stellen und Labors gewährt werden. Die Polizei in den Mitgliedstaaten kann DNA-Profile von Straftätern, Tatorten, vermissten Personen und nicht identifizierten Leichen einreichen.

2.4.2. Interpol-Fingerabdruckdatenbank

Ermächtigte Nutzer in den Mitgliedstaaten können über ein automatisiertes Fingerabdruck-Identifizierungssystem (AFIS) Dateien einsehen, einreichen und abgleichen. Die Dateien werden in dem vom US-amerikanischen Normeninstitut (National Institute of Standards and Technology/NIST) vorgegebenen Format gespeichert und ausgetauscht. Die Leitlinien für die Übermittlung von Fingerabdrücken und die Leitlinien für die Übermittlung von Fingerabdruck-Tatortspuren sind den Mitgliedstaaten bei der qualitativen und quantitativen Verbesserung der an das Interpol-AFIS übermittelten Fingerabdruckdateien behilflich.

2.4.3. Interpol-Datenbank gestohlener und verlorener Reisedokumente

Die Interpol-Datenbank gestohlener und verlorener Reisedokumente enthält Informationen über mehr als 45 Millionen Reisedokumente, die von 166 Ländern als verloren oder gestohlen gemeldet worden sind. Diese Datenbank ermöglicht es den NCB von Interpol und anderen ermächtigten Strafverfolgungsbehörden (etwa Einwanderungs- und Grenzschutzbeamten), sich Gewissheit über die Gültigkeit eines verdächtigen Reisedokuments zu verschaffen. Für die Zwecke der Verhütung und Bekämpfung der Schwerkriminalität und der organisierten Kriminalität tauschen die zuständigen Strafverfolgungsbehörden der Mitgliedstaaten Daten in Bezug auf Reisepässe mit Interpol aus[40].

2.4.4. Datenbank zur Erfassung von Ausschreibungen zugeordneten Reisedokumenten (TDAWN)

Die TDAWN enthält Informationen über Reisedokumente von Personen, die mit Interpol-Ausschreibungen gesucht werden.

2.4.5. Referenztabelle für Schusswaffen

Die Interpol-Referenztabelle für Schusswaffen ermöglicht es Ermittlern, die bei einer Straftat verwendeten Schusswaffen (nach Marke, Modell, Kaliber usw.) korrekt zu bestimmen. Die Tabelle enthält mehr als 250 000 Referenzen zu Schusswaffen und 57 000 Abbildungen in hoher Qualität. Das Interpol-Ballistik-Informationsnetz ist eine Plattform für den internationalen Austausch und Abgleich ballistischer Daten und weist mehr als 150 000 Dateien auf.

Die Interpol-Datenbank zur Aufspürung und Rückverfolgung illegaler Waffen (iARMS) ist eine IT-Anwendung, die den Informationsaustausch und die Zusammenarbeit der Strafverfolgungsbehörden in Bezug auf Straftaten erleichtert, bei denen Feuerwaffen eine Rolle gespielt haben.

---

[40] Gemeinsamer Standpunkt 2005/69/JI des Rates zum Austausch bestimmter Daten mit Interpol, ABl. L 27 vom 29.1.2005, S. 61.

2.5. Europäisches Strafregisterinformationssystem ECRIS[41]

Mit dem IT-basierten Europäischen Strafregisterinformationssystem (ECRIS)[42] werden die elektronischen Mittel für den Austausch von Informationen über Verurteilungen zwischen den Mitgliedstaaten in einem standardisierten Format bereitgestellt. Das ECRIS wird verwendet, um die Mitgliedstaaten über gegen ihre Staatsangehörigen ergangene Urteile zu unterrichten und Ersuchen um Strafregisterinformationen für die Zwecke von Strafverfahren und andere Zwecke wie Verwaltungs- oder Beschäftigungszwecke zu übermitteln. Es ist auch möglich, Ersuchen in Bezug auf Drittstaatsangehörige zu übermitteln, wenn Anlass zu der Vermutung besteht, dass der ersuchte Mitgliedstaat über Informationen zu der betreffenden Person verfügt.

ECRIS-Ersuchen sind innerhalb von 10 Arbeitstagen zu beantworten, wenn das Ersuchen Zwecke von Strafverfahren oder Beschäftigungszwecke betrifft, und innerhalb von 20 Arbeitstagen, wenn das Ersuchen von einer Person zu ihrer eigenen Unterrichtung gestellt wurde.

ECRIS ist nicht zur Einrichtung einer zentralen Strafregisterdatenbank ausgelegt und beruht auf einer dezentralen IT-Architektur, wobei alle Strafregisterdateien ausschließlich in von den Mitgliedstaaten betriebenen Datenbanken gespeichert sind. Die Daten werden elektronisch zwischen den benannten zentralen Behörden der Mitgliedstaaten ausgetauscht.

Die Informationen müssen von den Mitgliedstaaten gemäß den vereinbarten Regeln und in standardisierten Formaten übermittelt werden und so vollständig wie möglich sein, damit der empfangende Mitgliedstaat die Informationen richtig verarbeiten und die betreffende Person identifizieren kann. Die Nachrichten werden in den Amtssprachen der betreffenden Mitgliedstaaten oder in einer anderen, von beiden Mitgliedstaaten akzeptierten Sprache übermittelt.

---

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

42 Richtlinie (EU) 2019/884 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Änderung des Rahmenbeschlusses 2009/315/JI des Rates im Hinblick auf den Austausch von Informationen über Drittstaatsangehörige und auf das Europäische Strafregisterinformationssystem (ECRIS), sowie zur Ersetzung des Beschlusses 2009/316/JI des Rates, ABl. L 151 vom 7.6.2019, S. 143.

Ein nicht bindendes Handbuch für Rechtsanwender, in dem die Verfahren für den Informationsaustausch und die Koordinierung ihrer Maßnahmen für Entwicklung und Betrieb des ECRIS dargelegt sind, wird vom Generalsekretariat des Rates veröffentlicht und kann in elektronischem Format auf der Website des Rates und auf der bei der Kommission angesiedelten Website CIRCABC unter https://circabc.europa.eu abgerufen werden. Ersuchen um Zugang zu dem Leitfaden sind an das Ratssekretariat zu richten. Ersuchen um Zugang zu der engeren Interessengruppe "ECRIS Business and Technical Support" (ECRIS – Betrieb und technische Unterstützung) sind an die Europäische Kommission zu richten.

2.5.1. ECRIS für Drittstaatsangehörige[43]

Der Rechtsrahmen für ECRIS trägt den Besonderheiten von Anfragen zu Drittstaatsangehörigen nicht in ausreichendem Maße Rechnung. Innerhalb der Union werden Informationen zu Drittstaatsangehörigen nicht – wie bei Staatsangehörigen der Mitgliedstaaten im jeweiligen Herkunftsmitgliedstaat – erhoben, sondern nur in den Mitgliedstaaten gespeichert, in denen die Verurteilungen erfolgt sind. Mit dem ECRIS-TCN[44] kann die nationale Zentralbehörde feststellen, welche anderen Mitgliedstaaten über Strafregisterinformationen zu einem Drittstaatsangehörigen verfügen. Dann kann auf den bestehenden ECRIS-Rahmen zurückgegriffen werden, um die betreffenden Mitgliedstaaten gemäß dem Rahmenbeschluss 2009/315/JI um solche Informationen zu ersuchen.

Die Verordnung sieht Vorschriften über die Einrichtung eines zentralisierten Systems vor, in dem auf Unionsebene personenbezogenen Daten erfasst werden, und Vorschriften über die Aufteilung der Zuständigkeiten zwischen dem Mitgliedstaat und der Organisation, die für die Entwicklung und Wartung des zentralisierten Systems zuständig ist. Sie sorgt für einen insgesamt angemessenen Datenschutz, eine angemessene Datensicherheit und den Schutz der Grundrechte der betroffenen Personen.

---

43 Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) 2018/1726, ABl. L 135 vom 22.5.2019, S. 1.
Richtlinie (EU) 2019/884 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Änderung des Rahmenbeschlusses 2009/315/JI des Rates im Hinblick auf den Austausch von Informationen über Drittstaatsangehörige und auf das Europäische Strafregisterinformationssystem (ECRIS), sowie zur Ersetzung des Beschlusses 2009/316/JI des Rates, ABl. L 151 vom 7.6.2019 S. 143.

44 Die Kommission bestimmt den Zeitpunkt, zu dem das ECRIS-TCN seinen Betrieb aufnimmt, nachdem die Voraussetzungen gemäß Artikel 35 der Verordnung (EU) 2019/816 erfüllt sind.

Die Mitgliedstaaten sollten im ECRIS-TCN Datensätze über verurteilte Drittstaatsangehörige anlegen. Das sollte, soweit möglich, automatisch und unverzüglich nach Erfassung der Verurteilung im nationalen Strafregister erfolgen. Die Mitgliedstaaten sollten gemäß der Verordnung alphanumerische Daten und Fingerabdruckdaten im Zusammenhang mit Verurteilungen in das Zentralsystem eingeben, die nach dem Tag des Beginns der Dateneingabe in das ECRIS-TCN erfolgt sind. Ab demselben oder einem späteren Zeitpunkt sollten die Mitgliedstaaten Gesichtsbilder in das Zentralsystem eingeben können.

Im ECRIS-TCN ist die Verarbeitung von Fingerabdruckdaten vorgesehen, um festzustellen, in welchen Mitgliedstaaten Informationen über Strafregistereinträge eines Drittstaatsangehörigen vorliegen. Außerdem sollte es die Verarbeitung von Gesichtsbildern ermöglichen, um die Identität des Drittstaatsangehörigen zu bestätigen. Es ist wesentlich, dass die Eingabe und Verwendung von Fingerabdruckdaten und Gesichtsbildern nicht über das zur Erreichung des Ziels unbedingt erforderliche Maß hinausgehen, die Grundrechte und das Kindeswohl wahren und mit den anwendbaren Datenschutzvorschriften der Union im Einklang stehen.

Eurojust, Europol und die EUStA sollten Zugang zum ECRIS-TCN haben, damit sie ermitteln können, in welchen Mitgliedstaaten Strafregisterinformationen zu einem Drittstaatsangehörigen vorliegen, und somit ihre gesetzlichen Aufgaben effizienter erfüllen können.

Die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) ist mit der Entwicklung und dem Betrieb des ECRIS-TCN betraut.

2.6. Visa-Informationssystem (VIS)[45]

Das Visa-Informationssystem (VIS) ist hauptsächlich ein Einwanderungskontrollsystem. Es ist ein Werkzeug, das die Zusammenarbeit auf der Ebene der Konsulate und der Grenzkontrollen durch die elektronische Verifizierung und den elektronischen Austausch von Visa-Daten zwischen den Mitgliedstaaten erleichtert. Als solches zielt es auf visumspflichtige ausländische Staatsangehörige ab. Die benannten Behörden der Mitgliedstaaten (d. h. konsularische Vertretungen, Grenzkontrollstellen, Polizei- und Einwanderungsbehörden)[46] und Europol[47] – im Rahmen seiner Aufgaben – sind befugt zur Abfrage des VIS[48] zum Zwecke der Verhütung, Aufdeckung und Ermittlung

- terroristischer Straftaten, d. h. Straftaten nach innerstaatlichem Recht, die den in den Artikeln 1 bis 4 des Rahmenbeschlusses 2002/475/JI des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung genannten Straftaten entsprechen oder gleichwertig sind;

- schwerwiegender Straftaten, d. h. Straftaten, die den in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI (betreffend den Europäischen Haftbefehl) aufgeführten Straftaten entsprechen oder gleichwertig sind.

---

45 Entscheidung 2004/512/EG des Rates vom 8. Juni 2004 zur Einrichtung des Visa-Informationssystems (VIS), ABl. L 213 vom 15.6.2004, S. 5.

46 Liste der zuständigen Behörden, deren ordnungsgemäß ermächtigte Bedienstete Zugang zum Visa-Informationssystem (VIS) für die Eingabe, Änderung, Löschung oder Abfrage von Daten haben (2016/C 187/04), ABl. C 187 vom 26.5.2016, S. 4.

47 Beschluss 2008/633/JI des Rates über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten, ABl. L 218 vom 13.8.2008, S. 129; Beschluss 2013/392/EU des Rates zur Festlegung des Zeitpunkts, ab dem der Beschluss 2008/633/JI über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten gilt, ABl. L 198 vom 23.7.2013, S. 45.

48 Am 16. April 2015 hat der Europäische Gerichtshof den Beschluss 2013/392/EU des Rates vom 22. Juli 2013 zur Festlegung des Zeitpunkts, ab dem der Beschluss 2008/633/JI über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten gilt, für nichtig erklärt. Der Gerichtshof hat jedoch erklärt, dass die Wirkungen des Beschlusses 2013/392 bis zum Inkrafttreten eines neuen Rechtsakts, der ihn ersetzen soll, aufrechterhalten werden.

Entsprechend dem "schwedischen Rahmenbeschluss" können die im VIS enthaltenen Informationen dem Vereinigten Königreich und Irland von den zuständigen Behörden derjenigen Mitgliedstaaten, deren benannte Behörden Zugang zum VIS haben, bereitgestellt werden, und die in den Visaregistern des Vereinigten Königreichs und Irlands vorhandenen Informationen können den zuständigen Strafverfolgungsbehörden der anderen Mitgliedstaaten übermittelt werden.

Das VIS beruht auf einer zentralen Architektur und einer gemeinsamen Plattform mit SIS II. VIS-Daten werden in zwei Stufen verarbeitet. In der ersten Stufe umfassen die Daten alphanumerische Daten und Lichtbilder. In der zweiten Stufe werden biometrische Daten und eingescannte Dokumente verarbeitet und ins VIS eingegeben. Das VIS enthält Daten zu Visumanträgen, Lichtbildern, Fingerabdrücken, einschlägigen Entscheidungen von Visabehörden und Verknüpfungen zwischen zusammenhängenden Anträgen. Das VIS verwendet ein System für den biometrischen Abgleich, um zuverlässige Fingerabdruckvergleiche für folgende Zwecke sicherzustellen:

- entweder Verifizierung, d. h. die Klärung der Frage, ob am Grenzübergang gescannte Fingerabdrücke mit denen der auf dem Visum angebrachten biometrischen Darstellung übereinstimmen,

- oder Identifizierung, d. h. Abgleich der am Grenzübergang abgenommenen Fingerabdrücke mit der gesamten Datenbank.

In technischer Hinsicht besteht das VIS aus drei Ebenen, nämlich der zentralen, der nationalen und der lokalen Ebene, wobei letztere konsularische Vertretungen, Grenzkontrollstellen sowie Einwanderungs- und Polizeibehörden einschließt.
Im Mai 2018 hat die Kommission einen Gesetzgebungsvorschlag zur Änderung der VIS-Verordnung vorgelegt, mit dem unter anderem die Interoperabilität zwischen anderen Datenbanken im Bereich Justiz und Inneres gewährleistet werden soll. Das aktualisierte VIS wird voraussichtlich nicht vor Ende 2021 einsatzbereit sein.

2.7. Eurodac[49][50]

Entsprechend seiner ursprünglichen Zweckbestimmung leistet das europäische automatisierte Identifikationssystem für Fingerabdrücke (Eurodac) Hilfe bei der Bestimmung des zuständigen Mitgliedstaats für die Prüfung eines in einem Mitgliedstaat der Europäischen Gemeinschaften gestellten Asylantrags und bei der sonstigen Erleichterung der Anwendung des Dubliner Übereinkommens. Ein Zugang zu Eurodac für die Zwecke der Verhütung, Aufdeckung oder Ermittlung terroristischer Straftaten oder sonstiger schwerer Straftaten wird nur in ganz bestimmten Fällen gewährt.

In der Eurodac-Verordnung (EU) Nr. 603/2013 sind Regeln für die Übermittlung von Fingerabdruckdaten an die Zentraleinheit, die Speicherung der Fingerabdruckdaten und sonstiger relevanter Daten in der einschlägigen zentralen Datenbank, ihre Aufbewahrung, der Vergleich mit anderen Fingerabdruckdaten, die Übermittlung der Vergleichsergebnisse sowie die Sperrung und Löschung von gespeicherten Daten niedergelegt.

Die Eurodac-Systemarchitektur besteht aus a) einer rechnergestützten zentralen Fingerabdruck-Datenbank ("Zentralsystem") mit einer Zentraleinheit, einem Notfallplan und einem Notfallsystem und b) einer Infrastruktur für die Kommunikation zwischen dem Zentralsystem und den Mitgliedstaaten, wodurch ein dediziertes verschlüsseltes virtuelles Netz für Eurodac-Daten zur Verfügung gestellt wird ("Kommunikationsinfrastruktur").

Jeder Mitgliedstaat hat eine einzige nationale Zugangsstelle.

Die mit der Verordnung (EU) Nr. 1077/2011[51] errichtete eu-LISA ist für das Betriebsmanagement von Eurodac zuständig und gewährleistet in Zusammenarbeit mit den Mitgliedstaaten, dass vorbehaltlich einer Kosten-Nutzen-Analyse jederzeit die beste verfügbare und sicherste Technologie und Technik für das Zentralsystem zum Einsatz kommt.

---

49 Verordnung (EG) Nr. 2725/2000 des Rates vom 11. Dezember 2000 über die Einrichtung von "Eurodac" für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens, ABl. L 316 vom 15.12.2000, S. 1.

50 Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (Neufassung).

51 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 kann dem Zentralsystem Fingerabdrücke übermitteln, um zu überprüfen, ob ein mindestens 14 Jahre alter Ausländer, der sich illegal in seinem Hoheitsgebiet aufhält, bereits in einem anderen Mitgliedstaat einen Asylantrag gestellt hat. Die Zentraleinheit vergleicht diese Fingerabdrücke mit den von anderen Mitgliedstaaten übermittelten und bereits in der zentralen Datenbank gespeicherten Fingerabdruckdaten. Die Einheit teilt dem Mitgliedstaat, der die Daten übermittelt hat, mit, ob es einen "Treffer" gibt, d. h. das Ergebnis des Vergleichs zwischen den gespeicherten und den übermittelten Fingerabdrücken. Der Mitgliedstaat überprüft das Ergebnis und nimmt in Zusammenarbeit mit den betreffenden Mitgliedstaaten die endgültige Identifizierung vor.

Die Mitgliedstaaten müssen die Rechtmäßigkeit, Genauigkeit und Sicherheit der Eurodac-Daten sicherstellen. Jede Person oder jeder Mitgliedstaat, der oder dem durch die Nichteinhaltung der Eurodac-Vorschriften ein Schaden entstanden ist, hat das Recht, von dem für den erlittenen Schaden verantwortlichen Mitgliedstaat Schadenersatz zu verlangen.

In der Verordnung (EU) Nr. 603/2013 ist vorgesehen, dass die benannten Behörden der Mitgliedstaaten und Europol zu Strafverfolgungszwecken Zugang zu den Eurodac-Daten haben. Gemäß der Verordnung können die benannten Behörden nur dann einen begründeten Antrag in elektronischer Form auf Abgleich von Fingerabdruckdaten mit den Daten im Zentralsystem stellen, wenn der Abgleich mit den folgenden Datenbanken nicht zur Feststellung der Identität der betreffenden Person geführt hat:

– nationale Fingerabdruck-Datenbanken,

– automatisierte Fingerabdruck-Identifizierungssysteme (AFIS) aller anderen Mitgliedstaaten nach dem Beschluss 2008/615/JI ("Prüm-Beschluss"), wenn entsprechende Abgleiche technisch möglich sind, es sei denn, es liegen hinreichende Gründe für die Annahme vor, dass ein Abgleich mit dieses Systemen nicht zur Feststellung der Identität der betroffenen Person führen würde. Diese hinreichenden Gründe werden in den begründeten elektronischen Antrag auf einen Abgleich mit Eurodac-Daten aufgenommen, der von der benannten Behörde der Prüfstelle übermittelt wird, und

– Visa-Informationssystem, sofern die in dem Beschluss 2008/633/JHA niedergelegten Voraussetzungen für einen solchen Abgleich vorliegen.

Auch die nachstehenden kumulativen Voraussetzungen müssen erfüllt sein:

a) Der Abgleich ist für die Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten erforderlich, d. h., es besteht ein überwiegendes öffentliches Sicherheitsinteresse, aufgrund dessen die Abfrage der Datenbank verhältnismäßig ist.

b) Der Abgleich ist im Einzelfall erforderlich (d. h., es findet kein systematischer Abgleich statt).

c) Es liegen hinreichende Gründe zu der Annahme vor, dass der Abgleich wesentlich zur Verhütung, Aufdeckung oder Ermittlung einer der fraglichen Straftaten beitragen wird. Diese hinreichenden Gründe liegen insbesondere vor, wenn der begründete Verdacht besteht, dass der Verdächtige, der Täter oder das Opfer einer terroristischen Straftat oder einer sonstigen schweren Straftat einer Personenkategorie zugeordnet werden kann, die von der Verordnung (EU) Nr. 603/2013 erfasst wird.

2.8. ZIS – Zollinformationssystem[52]

Das Zollinformationssystem ergänzt das Neapel- II-Übereinkommen[53]. Das System stellt ab auf eine Verbesserung der Zollverwaltungen der Mitgliedstaaten durch einen schnellen Informationsaustausch im Hinblick auf die Verhütung, Ermittlung und Verfolgung schwerer Verstöße gegen das nationale und das Gemeinschaftsrecht. Mit dem Zollinformationssystem wird auch ein Aktennachweissystem für Zollzwecke (FIDE) zur Unterstützung von Zollermittlungen eingerichtet.

Das von der Kommission verwaltete ZIS ist ein zentralisiertes Informationssystem, auf das über Terminals in jedem Mitgliedstaat sowie bei der Kommission, bei Europol und Eurojust zugegriffen werden kann. Zugriff auf die ZIS-Daten haben die Zoll-, Steuer-, Agrar-, Gesundheits- und Polizeibehörden der Mitgliedstaaten sowie Europol und Eurojust. Nur die von den Mitgliedstaaten benannten Behörden[54] und die Kommission haben direkten Zugang zu den im ZIS gespeicherten Daten. Zur Verstärkung der Komplementarität haben Europol und Eurojust Lesezugriff auf ZIS und FIDE.

---

52 Beschluss 2009/917/JI des Rates vom 30. November 2009 über den Einsatz der Informationstechnologie im Zollbereich, ABl. L 323 vom 10.12.2009, S. 20.

53 Übereinkommen aufgrund von Artikel K.3 des Vertrags über die Europäische Union über gegenseitige Amtshilfe und Zusammenarbeit der Zollverwaltungen, ABl. C 24 vom 23.1.1998, S. 2.

54 Anwendung des Artikels 7 Absatz 2 und des Artikels 8 Absatz 3 des Beschlusses 2009/917/JI des Rates vom 30. November 2009 über den Einsatz der Informationstechnologie im Zollbereich – aktualisierte Liste der zuständigen Behörden, Dok. 13394/11 ENFOCUSTOM 85.

Das ZIS enthält personenbezogene Daten mit Bezug auf Ausgangsstoffe, Beförderungsmittel, Unternehmen, Personen und Waren sowie einbehaltenes, eingezogenes oder beschlagnahmtes Bargeld. Personenbezogene Daten dürfen nur für Risikomanagement- oder operative Analysen vom ZIS in andere Datenverarbeitungssysteme kopiert werden, zu denen nur die von den Mitgliedstaaten benannten Analyseexperten Zugang haben.

Wenn sie eine Ermittlungsakte anlegen, können die für Zollermittlungen zuständigen nationalen Behörden anhand von FIDE feststellen, ob andere Behörden bereits Ermittlungen zu einer bestimmten Person oder einem bestimmten Unternehmen durchgeführt haben.

2.9. Gefälschte und echte Dokumente online – FADO[55]

Ein auf Internet-Technologie beruhendes computergestütztes Bildarchivierungssystem, das gefälschte und echte Dokumente enthält, ermöglicht einen schnellen und sicheren Informationsaustausch zwischen dem Generalsekretariat des Rates der Europäischen Union und den Dokumentenkontrollen durchführenden Personen in allen Mitgliedstaaten sowie in Island, Norwegen und in der Schweiz. Das System ermöglicht es, auf dem Bildschirm einen Vergleich zwischen dem Original und einem falschen oder gefälschten Dokument vorzunehmen. In erster Linie enthält es Dokumente der Mitgliedstaaten sowie Dokumente von Drittländern, aus denen regelmäßig ein Migrationsstrom zu den Mitgliedstaaten festzustellen ist. Die durch FADO eingerichtete Datenbank schließt folgende Daten ein:

- Abbildungen echter Dokumente,
- Informationen über Sicherheitstechniken (Sicherheitsmerkmale),
- Abbildungen typischer falscher und gefälschter Dokumente,
- Informationen über Fälschungstechniken und
- statistische Angaben zu entdeckten falschen und gefälschten Dokumenten und Fällen von Identitätsbetrug.

---

55 Gemeinsame Maßnahme 98/700/JI vom 3. Dezember 1998 – vom Rat aufgrund von Artikel K.3 des Vertrags über die Europäische Union angenommen – betreffend die Errichtung eines Europäischen Bildspeicherungssystems (FADO), ABl. L 333 vom 9.12.1998, S. 4.

Das System nutzt spezielle Datenübermittlungsleitungen zwischen dem Generalsekretariat des Rates und den Zentraldiensten in den Mitgliedstaaten. Innerhalb jedes Mitgliedstaats wird das System über eine sichere Internetverbindung von einem Zentraldienst abgefragt. Ein Mitgliedstaat kann das System in seinem Hoheitsgebiet intern nutzen, d. h., dass verschiedene Arbeitsplätze an den einzelnen Grenzkontrollstellen oder bei anderen zuständigen Behörden angeschlossen werden. Es gibt jedoch keine direkte Verbindung zwischen einem Arbeitsplatz – außer beim nationalen Zentraldienst – und der Zentralstelle im Generalsekretariat.

FADO ist derzeit in 22 Amtssprachen der Europäischen Union verfügbar. Die Dokumente werden von Dokumentenexperten in einer beliebigen Amtssprache eingegeben und die Standardbeschreibungen werden automatisch übersetzt. Daher sind die Dokumente sofort in allen unterstützten Sprachen verfügbar. Zusätzliche als Freitext eingegebene Informationen werden anschließend beim Generalsekretariat des Rates von Fachübersetzern übersetzt.

2.10. Öffentliches Online-Register echter Identitäts- und Reisedokumente – PRADO

Während der Zugang zu FADO auf Dokumentenkontrollen durchführende Personen beschränkt und ausschließlich für eine amtliche Nutzung bestimmt ist, enthält das beim Rat der Europäischen Union geführte öffentliche Online-Register echter Identitäts- und Reisedokumente (**P**ublic **R**egister of **A**uthentic Travel and Identity **D**ocuments **O**nline/PRADO) eine für die allgemeine Öffentlichkeit zugängliche Teilmenge der FADO-Informationen. Die Website[56] wird vom Generalsekretariat des Rates der Europäischen Union in den Amtssprachen der EU aus Transparenzgründen veröffentlicht und stellt für viele Nutzer in Europa – insbesondere für nichtstaatliche Organisationen, die Identitäten überprüfen müssen oder rechtlich dazu verpflichtet sind – eine wichtige Dienstleistung dar.

Die Website enthält technische Beschreibungen – darunter auch Informationen über Sicherheitsmerkmale – echter Identitäts- und Reisedokumente. Die Informationen werden von Dokumentenexperten aus den EU-Mitgliedstaaten sowie Island, Norwegen und der Schweiz ausgewählt und bereitgestellt.

Bei PRADO können die Nutzer auch Links zu Websites mit von einigen Mitgliedstaaten sowie Drittstaaten bereitgestellten Informationen über ungültige Dokumentennummern sowie andere nützliche Informationen über Identitäts- und Dokumentenüberprüfungen und -betrug finden.

---

56 http://www.prado.consilium.europa.eu/

2.11. Einreise-/Ausreisesystem (EES)

Das Einreise-/Ausreisesystem[57] (EES) dient hauptsächlich der Verbesserung des Außengrenzenmanagements der Union[58]. Mit diesem System werden der Zeitpunkt und der Ort der Ein- und Ausreise bestimmter Drittstaatsangehöriger, die für einen Kurzaufenthalt im Hoheitsgebiet der Mitgliedstaaten zugelassen sind, elektronisch erfasst und die Dauer des zulässigen Aufenthalts berechnet.

Zusätzlich sind die nationalen Strafverfolgungsbehörden nur unter den in der Verordnung festgelegten Bedingungen zur Abfrage des EES berechtigt, um terroristische und sonstige schwerwiegende Straftaten zu verhüten, aufzudecken und zu ermitteln.

Die Verordnung enthält strenge Vorschriften für den Zugang zum EES. Außerdem wird darin festgelegt, dass Einzelpersonen das Recht auf Auskunft, Berichtigung, Vervollständigung, Löschung und Regress haben, insbesondere das Recht, bei Gericht einen Rechtsbehelf einzulegen, und dass die Datenverarbeitung von unabhängigen Behörden überwacht wird. Die Verordnung steht im Einklang mit den Grundrechten und Grundsätzen, die mit der Charta der Grundrechte der EU anerkannt wurden.

Das EES besteht aus

- einem Zentralsystem (Zentralsystem des EES), mit dem eine computergestützte zentrale Datenbank für biometrische (Fingerabdrücke und Gesichtsbilder) und alphanumerische Daten betrieben wird,
- einer einheitlichen nationalen Schnittstelle in jedem Mitgliedstaat,
- einer sicheren und verschlüsselten Kommunikationsinfrastruktur für die Verbindung zwischen dem Zentralsystem des EES und den einheitlichen nationalen Schnittstellen,
- einem sicheren Kommunikationskanal für die Verbindung zwischen dem Zentralsystem des EES und dem Zentralsystem des Visa-Informationssystems zum Zwecke der Abfrage.

---

[57] Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten der Europäischen Union und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011, ABl. L 327 vom 9.12.2017, S. 20.

[58] Die Kommission bestimmt den Zeitpunkt, zu dem das EES seinen Betrieb aufnimmt, nachdem die Voraussetzungen nach Artikel 66 der Verordnung (EU) 2017/2226 erfüllt sind.

In der Verordnung wird bestimmt, welche nationalen Behörden zum Zugang zum EES berechtigt sind, um Daten für die festgelegten Zwecke des EES einzugeben, zu ändern, zu löschen oder abzufragen, soweit dies der Erfüllung ihrer Aufgaben dient. Jede Verarbeitung von EES-Daten sollte in einem angemessenen Verhältnis zu den verfolgten Zielen stehen und für die Erfüllung der Aufgaben der zuständigen Behörden erforderlich sein.

Die Bedingungen für den Zugang zum EES für die nationalen Strafverfolgungsbehörden ermöglichen diesen Behörden, Fälle aufzuklären, in denen Verdächtige mehrere Identitäten verwenden. Die Verwendung biometrischer Daten ist trotz des Eingriffs in die Privatsphäre der Reisenden gerechtfertigt, um Reisende ohne Reisedokumente oder sonstige Identitätsnachweise zu identifizieren. Solche Daten können auch verwendet werden, um die Reiserouten einer Person, die der Begehung einer Straftat verdächtig oder Opfer einer Straftat ist, nachzuverfolgen und somit Beweismaterial zusammenzutragen.

Der Zugang zu EES-Daten zu Gefahrenabwehr- und Strafverfolgungszwecken stellt einen Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten der Personen dar, deren personenbezogene Daten im EES verarbeitet werden. Diese Verarbeitung unterliegt den Bestimmungen der Richtlinie (EU) 2016/680 (Polizei-Richtlinie)[59].

Bei der Wahrnehmung ihrer Aufgaben dürfen Strafverfolgungsbehörden eine Fingerabdruckspur ("latente Fingerspur"), die gegebenenfalls an einem Tatort gefunden wurde, in denjenigen Fällen mit den im EES gespeicherten Fingerabdruckdaten abgleichen, in denen hinreichende Gründe zu der Annahme bestehen, dass der Täter oder das Opfer im EES erfasst ist. Allerdings ist der Zugang zum EES für die Strafverfolgungsbehörden zwecks Identifizierung von unbekannten Verdächtigen, Tätern oder Opfern terroristischer oder sonstiger schwerer Straftaten unter der Voraussetzung gestattet, dass Abfragen der nationalen Datenbanken durchgeführt wurden und die Abfrage der Fingerabdrücke nach dem Beschluss 2008/615/JI des Rates[60] ("Prüm-Beschluss") vollständig durchgeführt oder die Abfrage nicht innerhalb von zwei Tagen, nachdem sie gestartet wurde, vollständig abgeschlossen wurde.

---

59 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2019 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.

60 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.

Ähnlich den Verfahren und Bedingungen für den Zugang von nationalen Strafverfolgungsbehörden stehen die EES-Daten auch Europol unter den in der Verordnung festgelegten Bedingungen und Einschränkungen zur Verfügung. Europol verarbeitet die durch Abfrage von EES-Daten erlangten Informationen nur mit Zustimmung des Herkunftsmitgliedstaats. Die Zustimmung ist über die nationale Europol-Stelle des betreffenden Mitgliedstaats einzuholen. Der Europäische Datenschutzbeauftragte sollte die Datenverarbeitung durch Europol überwachen und die vollständige Einhaltung der geltenden Datenschutzvorschriften sicherstellen.

2.12. Europäisches Reiseinformations- und -genehmigungssystem (ETIAS)[61]

Der Informationsaustausch im Bereich des Grenzmanagements, der Strafverfolgung und der Terrorismusbekämpfung wird durch ETIAS unterstützt[62]. Das System dient dazu, vor der Einreise eines von der Visumpflicht befreiten Drittstaatsangehörigen in den Schengen-Raum und vor seiner Ankunft an Außengrenzübergangsstellen festzustellen, ob dieser zur Einreise berechtigt ist. ETIAS stellt eine Reisegenehmigung bereit, die sich von Natur aus von einem Visa unterscheidet, jedoch eine Voraussetzung für die Einreise und den Aufenthalt darstellt und anzeigt, dass mit dem Antragsteller kein Risiko für die Sicherheit, kein Risiko der illegalen Einwanderung und kein hohes Epidemierisiko verbunden ist. Erteilte Reisegenehmigungen sollten annulliert oder aufgehoben werden, sobald sich herausstellt, dass die Bedingungen für ihre Erteilung nicht erfüllt waren oder nicht mehr erfüllt sind.

ETIAS besteht aus

- einem IT-Großsystem, d. h. dem ETIAS-Informationssystem, das von eu-LISA konzipiert, entwickelt und technisch verwaltet wird,

- der ETIAS-Zentralstelle, die zur Europäischen Agentur für die Grenz- und Küstenwache gehört,

---

61 Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystem (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226, ABl. L 236 vom 19.9.2018, S. 1;
Verordnung (EU) 2018/1241 des Europäischen Parlaments und des Rates vom 12. September 2018 zur Änderung der Verordnung (EU) 2016/794 für die Zwecke der Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS), ABl. L 236 vom 19.9.2018, S. 72.

62 Die Kommission bestimmt den Zeitpunkt, zu dem das ETIAS seinen Betrieb aufnimmt, nachdem die Voraussetzungen gemäß Artikel 88 der Verordnung (EU) 2018/1240 erfüllt sind.

- den nationalen ETIAS-Stellen, die für die Prüfung der Anträge zuständig sind und über die Erteilung, Verweigerung, Annullierung oder Aufhebung von Reisegenehmigungen entscheiden. Bei der Beurteilung der Anträge sollten die nationalen ETIAS-Stellen miteinander und mit Europol kooperieren.

Die vom Antragsteller mitgeteilten personenbezogenen Daten werden durch ETIAS ausschließlich zum Zwecke der Beurteilung verarbeitet, ob mit der Einreise des Antragstellers in die Union ein Risiko für die Sicherheit, ein Risiko der illegalen Einwanderung oder ein hohes Epidemierisiko in der Union verbunden sein könnte. Zur Bewertung der Risiken sollten die bereitgestellten personenbezogenen Daten mit den Daten in den Dossiers, Datensätzen oder Ausschreibungen, die in einem Informationssystem bzw. einer Datenbank der EU (ETIAS-Zentralsystem, SIS, Visa-Informationssystem (VIS), Einreise-/Ausreisesystem (EES) oder Eurodac), den Europol-Daten oder den Interpol-Datenbanken (Interpol-Datenbank für gestohlene und verlorene Reisedokumente (SLTD) oder Interpol-Datenbank zur Erfassung von Ausschreibungen zugeordneten Reisedokumenten (Interpol-TDAWN)) erfasst sind, abgeglichen werden. Die personenbezogenen Daten sollten auch mit der ETIAS-Überwachungsliste und in Bezug auf spezifische Risikoindikatoren abgeglichen werden.

Der Abgleich erfolgt im Rahmen eines automatisierten Verfahrens. Sollte es einen "Treffer" geben, bei dem es sich um eine Übereinstimmung zwischen personenbezogenen Daten in dem Antrag und den spezifischen Risikoindikatoren oder den personenbezogenen Daten entweder in einem Dossier, einem Datensatz oder einer Ausschreibung in den oben genannten Informationssystemen oder in der Überwachungsliste handelt, so sollte der Antrag von der nationalen Stelle des zuständigen Mitgliedstaats manuell bearbeitet werden. Die Entscheidung zur Erteilung oder Verweigerung der Reisegenehmigung sollte auf der Grundlage einer solchen Bewertung getroffen werden.

Um die Gesamtziele des ETIAS zu erreichen, ist die Verarbeitung großer Mengen personenbezogener Daten erforderlich. Die Verordnung steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden. Daher gibt es geeignete Garantien, mit denen der Eingriff in das Recht auf Schutz des Privatlebens und in das Recht auf Schutz personenbezogener Daten auf das in einer demokratischen Gesellschaft notwendige und als verhältnismäßig geltende Maß beschränkt werden soll. Aus demselben Grund dürfen als Kriterien für die Festlegung der spezifischen Risikoindikatoren unter keinen Umständen sensible personenbezogene Daten dienen[63].

---

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

Der Zugriff auf pesonenbezogene Daten im ETIAS sollte ausdrücklich dazu ermächtigtem Personal vorbehalten sein und unter keinen Umständen dazu genutzt werden, Entscheidungen auf der Grundlage einer Form von Diskriminierung zu treffen. Was die Strafverfolgungsbehörden anbelangt, so sollten im ETIAS-Zentralsystem gespeicherte personenbezogene Daten nur in bestimmten Fällen und nur dann verarbeitet werden, wenn dies zur Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten erforderlich ist. Die benannten Behörden und Europol sollten den Zugang zum ETIAS nur beantragen, wenn sie hinreichende Gründe zu der Annahme haben, dass dieser Zugang Informationen erbringt, die einen Beitrag zur Verhütung, Aufdeckung oder Untersuchung einer terroristischen oder sonstigen schweren Straftat leisten.

2.13. Gesamtüberblick über die für den Informationsaustausch auf EU-Ebene verwendeten Informationssysteme

IT-Systeme und Datenbanken	Rechtsgrundlage	Zweck	Betroffene Personen	Gemeinsame Nutzung von Daten
Schengener Informationssystem der zweiten Generation – **SIS II**	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	• Innere Sicherheit • Grenzkontrolle • Justizielle Zusammenarbeit • Strafrechtliche Ermittlungen	• Unionsbürger • Drittstaatsangehörige	• VIS • Europol • Eurojust • Interpol
	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 23.12.2006, S. 4	• Einreise- oder Aufenthaltsverweigerung • Asyl-, Einwanderungs- und Rückkehrpolitik	• Drittstaatsangehörige, die kein Recht auf Freizügigkeit genießen, das demjenigen der Unionsbürger gleichwertig ist	
Europol **EIS**	Beschluss 2009/371/JI des Rates vom 6. April 2009 zur Errichtung des europäischen Polizeiamts (Europol), Artikel 11 bis 13 ABl. L 121 vom 15.5.2009, S. 37	• Schwerkriminalität • Einwanderung • Innere Sicherheit • Terrorismusbekämpfung	• Unionsbürger • Drittstaatsangehörige	• SIS II
Interpol **I-24/7**	Interpol-Statuten		• Unionsbürger • Drittstaatsangehörige	• SIS II • Europol • VIS

Interpol **Verlorene/gestohlene Reisedokumente (SLTD)**	Gemeinsamer Standpunkt 2005/69/JI des Rates zum Austausch bestimmter Daten mit Interpol ABl. L 27 vom 29.1.2005, S. 61	• Internationale und organisierte Kriminalität • Innere Sicherheit	• Unionsbürger • Drittstaatsangehörige	
ECRIS	Richtlinie (EU) 2019/884 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Änderung des Rahmenbeschlusses 2009/315/JI des Rates im Hinblick auf den Austausch von Informationen über Drittstaatsangehörige und auf das Europäische Strafregisterinformationssystem (ECRIS), sowie zur Ersetzung des Beschlusses 2009/316/JI des Rates ABl. L 151 vom 7.6.2019, S. 143	Strafverfahren	• Unionsbürger • Drittstaatsangehörige	
ECRIS-TCN	Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) 2018/1726 ABl. L 135 vom 22.5.2019, S. 1 Richtlinie (EU) 2019/884 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Änderung des Rahmenbeschlusses 2009/315/JI des Rates im Hinblick auf den Austausch von Informationen über Drittstaatsangehörige und auf das Europäische Strafregisterinformationssystem (ECRIS), sowie zur Ersetzung des Beschlusses 2009/316/JI des Rates ABl. L 151 vom 7.6.2019, S. 143	Strafverfahren	• Drittstaatsangehörige	• Europol • Eurojust • EUStA

VIS	Entscheidung 2004/512/EG des Rates vom 8. Juni 2004 zur Einrichtung des Visa-Informationssystems (VIS) ABl. L 213 vom 15.6.2004, S. 5 Beschluss 2008/633/JI des Rates über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten ABl. L 218 vom 13.8.2008, S. 129 Beschluss 2013/392/EU des Rates zur Festlegung des Zeitpunkts, ab dem der Beschluss 2008/633/JI über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten gilt ABl. L 198 vom 23.7.2013, S. 45	• Schwerkriminalität • Innere Sicherheit • Terrorismusbekämpfung	• Drittstaatsangehörige	• SIS II • Europol • Interpol

Eurodac	Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT- Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (Neufassung) ABl. L 180 vom 29.6.2013, S. 1 Verordnung (EU) Nr. 604/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist ABl. L 180 vom 29.6.2013, S. 31	• Einwanderung • Schwerkriminalität • Innere Sicherheit • Terrorismusbekämpfung	• Drittstaatsangehörige	Europol

Fluggastdatensätze (PNR)	Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität ABl. L 119 vom 4.5.2016, S. 132	• Schwerkriminalität • Innere Sicherheit • Terrorismusbekämpfung	• Unionsbürger • Drittstaatsangehörige	Europol
Vorab übermittelte Fluggastdaten (API-Daten)	Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln ABl. L 261 vom 6.8.2004, S. 24	• Grenzkontrolle • Einwanderung	• Drittstaatsangehörige	
ETIAS	Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226[64] ABl. L 236 vom 19.9.2018, S. 1 Verordnung (EU) 2018/1241 des Europäischen Parlaments und des Rates vom 12. September 2018 zur Änderung der Verordnung (EU) 2016/794 für die Zwecke der Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) ABl. L 236 vom 19.9.2018, S. 72	• Grenzkontrolle • Einwanderung • Schwerkriminalität • Innere Sicherheit • Terrorismusbekämpfung	• Drittstaatsangehörige	• SIS • VIS • EES • Eurodac • Europol • Interpol • ETIAS-Überwachungsliste

[64] Die Kommission bestimmt den Zeitpunkt, zu dem das ETIAS seinen Betrieb aufnimmt, nachdem die Voraussetzungen gemäß Artikel 88 der Verordnung erfüllt sind.

EES	Verordnung (EU) 2017/2225 des Europäischen Parlaments und des Rates vom 30. November 2017 zur Änderung der Verordnung (EU) 2016/399 in Bezug auf die Nutzung des Einreise-/Ausreisesystems ABl. L 327 vom 9.12.2017, S. 1 Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten der Europäischen Union und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011[65] ABl. L 327 vom 9.12.2017, S. 20	• Grenzmanagement • Schwerkriminalität • Terrorismusbekämpfung	• Drittstaatsangehörige	• VIS • Europol • Prüm-Beschluss
CIS	Beschluss 2009/917/JI des Rates vom 30. November 2009 über den Einsatz der Informationstechnologie im Zollbereich ABl. L 323 vom 10.12.2009, S. 20	• Bekämpfung des illegalen Handels	• Unionsbürger • Drittstaatsangehörige	Europol

[65] Die Kommission bestimmt den Zeitpunkt, zu dem das ETIAS seinen Betrieb aufnimmt, nachdem die Voraussetzungen gemäß Artikel 66 der Verordnung erfüllt sind.

FADO	Gemeinsame Maßnahme 98/700/JI vom 3. Dezember 1998 – vom Rat aufgrund von Artikel K.3 des Vertrags über die Europäische Union angenommen – betreffend die Errichtung eines Europäischen Bildspeicherungssystems (FADO) ABl. L 333 vom 9.12.1998, S. 4	• Bekämpfung gefälschter Dokumente • Einwanderungspolitik • Polizeizusammenarbeit	• Unionsbürger • Drittstaatsangehörige	

3. RECHTSVORSCHRIFTEN – RECHTLICHER KONTEXT SOWIE REGELN UND LEITLINIEN FÜR DIE WICHTIGSTEN KOMMUNIKATIONSVERFAHREN UND -SYSTEME

3.1. Datenschutzrichtlinie[66]

Richtlinie (EU) 2016/680 zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates[67] und zur Festlegung spezifischer Vorschriften im Zusammenhang mit

- dem Schutz natürlicher Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts bei der Verarbeitung der personenbezogenen Daten mit oder ohne Hilfe automatisierter Verfahren durch die Polizei oder andere Strafverfolgungsbehörden im Rahmen ihrer Tätigkeiten und

- dem Austausch personenbezogener Daten innerhalb der Union durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung.

Sie soll gewährleisten, dass natürliche Personen auf der Grundlage unionsweit durchsetzbarer Rechte das gleiche Maß an Schutz genießen und unterschiedliche Verfahren, die den Austausch personenbezogener Daten zwischen den zuständigen Behörden behindern könnten, beseitigt werden.

Die Frist für die Umsetzung der Richtlinie durch die Mitgliedstaaten läuft am 6. Mai 2018 ab. Sollte dies jedoch mit einem unverhältnismäßigen Aufwand verbunden sein, so können die Mitgliedstaaten ausnahmsweise vorsehen, dass sie die maßgeblichen Überwachungsvorschriften für Vorgänge in vor dem 6. Mai 2016 eingerichteten automatisierten Verarbeitungssystemen bis zum 6. Mai 2023 umsetzen.

---

66 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.

67 Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350 vom 30.12.2008, S. 60. Der Rahmenbeschluss wird mit Wirkung vom 6. Mai 2018 aufgehoben.

Der Begriff "zuständige Behörden" deckt staatliche Stellen wie die Justizbehörden, die Polizei oder andere Strafverfolgungsbehörden sowie alle anderen Stellen oder Einrichtungen ab, denen durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse für die Zwecke dieser Richtlinie übertragen wurde. Die Tätigkeiten der Strafverfolgungsbehörden sind hauptsächlich auf die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten ausgerichtet. Solche Tätigkeiten können ferner polizeiliche Tätigkeiten bei Demonstrationen, großen Sportveranstaltungen und Ausschreitungen umfassen. Sie umfassen auch die Aufrechterhaltung der öffentlichen Ordnung als Aufgabe, die ihnen übertragen wurde, soweit dies zum Zweck des Schutzes vor und der Abwehr von Bedrohungen der öffentlichen Sicherheit und Bedrohungen für grundlegende Interessen der Gesellschaft, die zu einer Straftat führen können, erforderlich ist.

Die Verarbeitung personenbezogener Daten für Zwecke außerhalb des Geltungsbereichs der oben genannten Tätigkeiten, mit denen die Mitgliedstaaten die Strafverfolgungsbehörden zusätzlich betrauen können, sowie die Verarbeitung personenbezogener Daten, die in den Anwendungsbereich der Rechtsvorschriften der Union fällt, wird durch die Verordnung (EU) 2016/679[68] geregelt. Zudem gilt die Richtlinie (EU) 2016/680 nicht für die Verarbeitung personenbezogener Daten im Hinblick auf Tätigkeiten im Zusammenhang mit der nationalen Sicherheit, Tätigkeiten von Agenturen oder Stellen, die mit Fragen der nationalen Sicherheit befasst sind, oder die Verarbeitung personenbezogener Daten, die von den Mitgliedstaaten bei Tätigkeiten im Zusammenhang mit der gemeinsamen Außen- und Sicherheitspolitik[69] vorgenommen wird.

Im Sinne der Datenschutz-Richtlinie bezeichnet der Ausdruck

- **"personenbezogene Daten"** alle Informationen, die sich auf eine identifizierte natürliche Person (im Folgenden "betroffene Person") oder eine insbesondere mittels Zuordnung zu 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, direkt oder indirekt identifizierbare natürliche Person beziehen.

  Die Mitgliedstaaten sehen vor, dass die zuständigen Behörden, die personenbezogene Daten verarbeiten, gegebenenfalls und so weit wie möglich klar zwischen den personenbezogenen Daten der einzelnen Kategorien betroffener Personen wie a) Verdächtige, b) verurteilte Straftäter, c) Opfer und d) andere Parteien, beispielsweise Zeugen, unterscheiden;

---

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

69 Titel V Kapitel 2 des Vertrags über die Europäische Union (EUV).

- **"Verarbeitung"** jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, 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, das Löschen oder die Vernichtung.

Personenbezogene Daten müssen auf rechtmäßige Weise und nach dem Grundsatz von Treu und Glauben und dürfen nur für bestimmte, durch Rechtsvorschriften geregelte Zwecke verarbeitet werden. Diese Verarbeitung sollte nur dann als rechtmäßig gelten, wenn sie zur Wahrnehmung einer Aufgabe erforderlich ist, die eine zuständige Behörde zu den oben genannten Zwecken der Strafverfolgung ausführt. Der Datenschutzgrundsatz der Verarbeitung nach Treu und Glauben ist ein anderes Konzept als das Recht auf ein faires Verfahren im Sinne des Artikels 47 der Charta und des Artikels 6 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten. Die personenbezogenen Daten müssen für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sein.

Die Verarbeitung besonders sensibler personenbezogener Daten, aus denen die Rasse oder die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten ausschließlich zum Zwecke der Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung ist nur dann erlaubt, wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person und unter genau festgelegten restriktiven Bedingungen erfolgt.

Die Einrichtung nationaler Aufsichtsbehörden, die ihre Aufgaben völlig unabhängig erfüllen können, ist ein wesentlicher Bestandteil des Schutzes natürlicher Personen bei der Verarbeitung ihrer Daten. Die Aufsichtsbehörden sollten die Anwendung der nach der Richtlinie erlassenen Vorschriften überwachen und zu ihrer einheitlichen Anwendung in der gesamten Union beitragen. Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der zuständigen nationalen Behörden und der Auftragsverarbeiter bedarf es – auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden – einer klaren Zuteilung der Verantwortlichkeiten.

Wenn personenbezogene Daten in ein anderes Land übermittelt werden, kann dies natürliche Personen daran hindern, sich rechtlich gegen eine unrechtmäßige Nutzung oder Offenlegung dieser Daten zu schützen. Ebenso kann es vorkommen, dass Aufsichtsbehörden Beschwerden nicht nachgehen oder Untersuchungen nicht durchführen können, die einen Bezug zu Tätigkeiten außerhalb der Grenzen ihres Mitgliedstaats haben. Ihre Bemühungen um grenzübergreifende Zusammenarbeit können auch durch unzureichende Präventiv- und Abhilfebefugnisse und durch widersprüchliche Rechtsordnungen behindert werden. Die Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden muss daher gefördert werden, um ihnen den Informationsaustausch mit Aufsichtsbehörden in anderen Ländern zu erleichtern.

3.2. "Schwedischer Rahmenbeschluss"[70]

Als Weiterentwicklung des Schengen-Besitzstands enthält der Rahmenbeschluss 2006/960/JI des Rates (der sogenannte "schwedische Rahmenbeschluss") insbesondere die Bestimmungen über Fristen und Standardformblätter für den grenzüberschreitenden Informationsaustausch[71] – auf Antrag oder eigene Initiative – zwischen den benannten zuständigen Strafverfolgungsbehörden der Mitgliedstaaten für folgende Zwecke:

- Verhütung, Aufdeckung und Aufklärung von Straftaten oder kriminellen Aktivitäten, die den im Europäischen Haftbefehl aufgeführten Handlungen entsprechen oder mit diesen übereinstimmen[72], oder

- Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit.

Die benannten Behörden sind verpflichtet, in dringenden Fällen innerhalb von höchstens acht Stunden zu antworten, sofern die erbetenen Informationen oder Erkenntnisse den Strafverfolgungsbehörden unmittelbar zugänglich sind. Informationen dürfen nicht bereitgestellt werden, wenn

- die nationale Sicherheit gefährdet ist;

- laufende Ermittlungen beeinträchtigt werden können;

---

70 Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, ABl. L 386 vom 29.12.2006, S. 89; Korrigendum in ABl. L 75 vom 15.3.2007, S. 26.

71 Siehe Abbildung 1.

72 Dok. 8216/2/08 REV 2: Endgültige Fassung des Europäischen Handbuchs mit Hinweisen zum Ausstellen eines Europäischen Haftbefehls. In Artikel 2 des Rahmenbeschlusses 2002/584/JI über den Europäischen Haftbefehl ist der Anwendungsbereich des Europäischen Haftbefehls festgelegt.

- das Ersuchen eine Straftat betrifft, die nach dem Recht des ersuchten Mitgliedstaats mit einer Freiheitsstrafe von höchstens einem Jahr bedroht ist;

- die zuständige Justizbehörde den Zugang zu den Informationen versagt.

Der Ausdruck "Informationen und/oder Erkenntnisse" erfasst die beiden folgenden Kategorien:

– alle Arten von Informationen oder Angaben, die bei Strafverfolgungsbehörden vorhanden sind, und

– alle Arten von Informationen oder Angaben, die bei Behörden oder privaten Stellen vorhanden und für die Strafverfolgungsbehörden ohne das Ergreifen von Zwangsmaßnahmen verfügbar sind.

Der Inhalt dieser Kategorien hängt von den nationalen Rechtsvorschriften ab. Die Art der in jedem Mitgliedstaat zugänglichen Informationen ist in den diesem Leitfaden beigefügten nationalen Merkblättern angegeben.

Daten sind mit Europol insoweit auszutauschen, als die ausgetauschten Informationen oder Erkenntnisse sich auf eine unter das Mandat von Europol fallende Straftat oder kriminelle Aktivität beziehen. Informationen und Erkenntnisse werden entsprechend den einschlägigen Bearbeitungscodes von Europol verarbeitet. Mit SIENA, der Europol-Netzanwendung für sicheren Datenaustausch, wird der Informationsaustausch gemäß dem "schwedischen Rahmenbeschluss" unterstützt.

Die Mitgliedstaaten sorgen dafür, dass die Bedingungen für den grenzüberschreitenden Informationsaustausch nicht strenger als die für einen internen Fall geltenden Bedingungen sind. Die zuständigen Strafverfolgungsbehörden sind insbesondere nicht verpflichtet, vor dem grenzüberschreitenden Informationsaustausch die Zustimmung oder Genehmigung einer Justizbehörde einzuholen, wenn die erbetenen Informationen auf nationaler Ebene ohne eine solche Zustimmung oder Genehmigung verfügbar sind. Sollte jedoch die Genehmigung einer Justizbehörde erforderlich sein, so ist diese bei Erlass ihrer Entscheidung verpflichtet, in einem grenzüberschreitenden Fall dieselben Regeln anzuwenden wie in einem rein innerstaatlichen Fall. Auf Informationen, für deren Austausch die Genehmigung einer Justizbehörde erforderlich ist, wird in den nationalen Merkblättern hingewiesen.

Da das Standardantragsformular von den Anwendern in der Praxis als zu umständlich empfunden wurde, ist ein nicht verbindliches Antragsformular für Informationen und Erkenntnisse[73] ausgearbeitet worden. Ist es nicht möglich, dieses vereinfachte Formblatt zu verwenden, so ist vorzugsweise ein anderes Formblatt oder ein nicht strukturiertes Format unter Verwendung von Freitext zu benutzen.

---

[73] Siehe Abbildung 2.

Diese Ersuchen müssen jedoch in jedem Fall den Anforderungen von Artikel 5 des "schwedischen Rahmenbeschlusses" entsprechen und mindestens die folgenden verpflichtenden Angaben enthalten:

- Verwaltungsinformationen, d. h. ersuchender Mitgliedstaat, ersuchende Behörde, Datum, Aktenzeichen, ersuchter Mitgliedstaat/ersuchte Mitgliedstaaten;
- ob dringende Bearbeitung erbeten wird und, wenn ja, mit welcher Begründung;
- Angabe, um welche Informationen oder Erkenntnisse ersucht wird;
- Identität/Identitäten (soweit bekannt) der Person(en) oder Sache(n), die Gegenstand der strafrechtlichen Ermittlungen oder des polizeilichen Erkenntnisgewinnungsverfahrens sind und auf die sich das Ersuchen um Bereitstellung von Informationen oder Erkenntnissen bezieht (beispielsweise Beschreibung der Straftat/en, Umstände der Tatbegehung usw.);
- Zweck, zu dem die Informationen und Erkenntnisse erbeten werden;
- Zusammenhang zwischen dem Zweck und der Person, auf die sich diese Informationen oder Erkenntnisse beziehen;
- Gründe für die Annahme, dass die Informationen oder Erkenntnisse in dem ersuchten Mitgliedstaat vorliegen;
- Beschränkungen hinsichtlich der Verwendung der in dem Ersuchen enthaltenen Informationen ("Bearbeitungscodes").

Der ersuchende Mitgliedstaat kann zwischen allen bestehenden Kanälen für die internationale Strafverfolgungskommunikation (SIRENE, Europol, Interpol, bilaterale Kontaktstellen) frei wählen. Der antwortende Mitgliedstaat antwortet in der Regel über den gleichen Kanal, der auch für das Ersuchen verwendet wurde. Antwortet der ersuchte Mitgliedstaat aus berechtigten Gründen jedoch über einen anderen Kanal, so wird die ersuchende Behörde hierüber in Kenntnis gesetzt. Für das Ersuchen und die Informationsübermittlung ist die Sprache zu verwenden, die für den jeweils benutzten Kommunikationsweg gilt.

Eine Übersicht über die **beibehaltenen bilateralen oder sonstigen Übereinkünfte** ist in der Anlage enthalten.

Abbildung 1

ANHANG A

INFORMATIONSAUSTAUSCH GEMÄSS DEM RAHMENBESCHLUSS 2006/960/JI DES RATES VOM ERSUCHTEN MITGLIEDSTAAT BEI DER ÜBERMITTLUNG VON INFORMATIONEN ODER IM FALLE EINER VERZÖGERUNG ODER ABLEHNUNG DER INFORMATIONSÜBERMITTLUNG ZU VERWENDENDES FORMBLATT

Dieses Formblatt ist zu verwenden, um die erbetenen Informationen und/oder Erkenntnisse zu übermitteln oder um der ersuchenden Behörde mitzuteilen, dass die reguläre Frist nicht eingehalten werden kann, dass das Ersuchen einer Justizbehörde zur Genehmigung vorgelegt werden muss oder dass die Übermittlung der Informationen verweigert wird.

Dieses Formblatt kann im Verfahrensverlauf mehr als einmal verwendet werden (z.B. wenn das Ersuchen zunächst einer Justizbehörde unterbreitet werden muss und sich dann erweist, dass die Erledigung des Ersuchens abgelehnt werden muss).

Ersuchte Behörde (Name, Anschrift, Telefon, Fax, E-Mail, Mitgliedstaat)	
Angaben zum Sachbearbeiter (fakultativ)	
Aktenzeichen dieser Antwort	
Datum und Aktenzeichen der früheren Antwort	

Antwort an folgende ersuchende Behörde	
Datum und Uhrzeit des Ersuchens	
Aktenzeichen des Ersuchens	

Reguläre Frist nach Artikel 4 des Rahmenbeschlusses 2006/960/JI		
Die Straftat fällt unter Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI und die erbetenen Informationen oder Erkenntnisse sind in einer Datenbank verfügbar, auf die eine Strafverfolgungsbehörde im ersuchten Mitgliedstaat unmittelbar zugreifen kann	Dringende Bearbeitung erbeten	➔ ❑ 8 Stunden
	Keine dringende Bearbeitung erbeten	➔ ❑ 1 Woche
Sonstige Fälle		➔ ❑ 14 Tage

Gemäß dem Rahmenbeschluss 2006/960/JI übermittelte Informationen: Zur Verfügung gestellte Informationen und Erkenntnisse

1. Verwendung der übermittelten Informationen oder Erkenntnisse

❑ dürfen nur für die Zwecke, für die sie übermittelt wurden, oder zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit verwendet werden
❑ dürfen auch zu anderen Zwecken verwendet werden, wenn die folgenden Voraussetzungen erfüllt sind (fakultativ):

2. Verlässlichkeit der Quelle

❑ zuverlässig
❑ sehr zuverlässig
❑ nicht zuverlässig
❑ kann nicht bewertet werden

3. Genauigkeit der Informationen oder Erkenntnisse

❑ sicher
❑ von der Quelle festgestellt
❑ vom Hörensagen – bestätigt
❑ vom Hörensagen – nicht bestätigt

4. Das Ergebnis der strafrechtlichen Ermittlungen oder des polizeilichen Erkenntnisgewinnungsverfahrens, in deren bzw. in dessen Rahmen der Informationsaustausch erfolgt ist, ist der übermittelnden Behörde mitzuteilen

❑ nein
❑ ja

5. Im Falle eines spontanen Austausches: Gründe der Annahme, dass die Informationen oder Erkenntnisse zur Aufdeckung, Verhütung oder Aufklärung von Straftaten nach Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI beitragen könnten:

VERZÖGERUNG — Es kann nicht innerhalb der nach Artikel 4 des Rahmenbeschlusses 2006/960/JI festgesetzten Frist geantwortet werden

Die Informationen oder Erkenntnisse können aus folgenden Gründen nicht innerhalb der festgesetzten Frist zur Verfügung gestellt werden:

Sie können voraussichtlich binnen

❑ 1 Tages ❑ 2 Tagen ❑ 3 Tagen
❑ .... Wochen
❑ 1 Monat

übermittelt werden.

❑ Es wurde um die Genehmigung einer Justizbehörde ersucht.
Das Verfahren bis zur Erteilung/Verweigerung der Genehmigung dauert voraussichtlich ... Wochen.

ABLEHNUNG — Die Informationen oder Erkenntnisse
❑ konnten auf nationaler Ebene nicht zur Verfügung gestellt oder erbeten werden oder
❑ können aus einem oder mehreren der nachstehenden Gründe nicht zur Verfügung gestellt werden:

A — Gründe im Zusammenhang mit der gerichtlichen Kontrolle, die die Übermittlung verhindern oder die Inanspruchnahme der Rechtshilfe erforderlich machen

❑ die zuständige Justizbehörde hat den Zugang zu den Informationen oder Erkenntnissen und deren Austausch nicht genehmigt

❑ die erbetenen Informationen oder Erkenntnisse wurden zuvor durch Zwangsmaßnahmen erlangt und ihre Zurverfügungstellung ist nach nationalem Recht nicht zulässig

❑ die Informationen oder Erkenntnisse sind nicht vorhanden bei

- Strafverfolgungsbehörden oder
- Behörden oder privaten Stellen in einer Weise, dass sie für die Strafverfolgungsbehörden ohne das Ergreifen von Zwangsmaßnahmen verfügbar sind.

❑ B — Die Zurverfügungstellung der erbetenen Informationen oder Erkenntnisse würde wesentliche nationale Sicherheitsinteressen beeinträchtigen oder den Erfolg laufender Ermittlungen oder eines laufenden polizeilichen Erkenntnisgewinnungsverfahrens oder die Sicherheit von Personen gefährden oder eindeutig in keinem Verhältnis zu den Zwecken stehen, für die um sie nachgesucht wurde, oder für diese Zwecke irrelevant sein.

Bei der Berufung auf Fall A oder B Angabe — soweit für erforderlich gehalten — zusätzlicher Informationen oder der Gründe (...) der Ablehnung (fakultativ):

❑ D — Die ersuchte Behörde beschließt, von der Möglichkeit Gebrauch zu machen, die Erledigung des Ersuchens abzulehnen, da sich das Ersuchen nach dem Recht des ersuchten Mitgliedstaats auf folgende Straftat bezieht (Angabe der Art der strafbaren Handlung und ihrer rechtlichen Einstufung) ....., die mit Freiheitsstrafe von einem Jahr oder weniger bedroht ist.

❑ E — Die erbetenen Informationen oder Erkenntnisse sind nicht verfügbar.

❑ F — Die erbetenen Informationen oder Erkenntnisse wurden von einem anderen Mitgliedstaat oder von einem Drittstaat erlangt und unterliegen dem Grundsatz der Spezialität und der betreffende Mitgliedstaat oder Drittstaat hat der Zurverfügungstellung der Informationen oder Erkenntnisse nicht zugestimmt.

ANHANG B

INFORMATIONSAUSTAUSCH GEMÄSS DEM RAHMENBESCHLUSS 2006/960/JI DES RATES VOM ERSUCHENDEN MITGLIEDSTAAT ZU VERWENDENDES FORMBLATT FÜR EIN ERSUCHEN UM INFORMATIONEN UND ERKENNTNISSE

Dieses Formblatt ist für ein Ersuchen um Informationen und Erkenntnisse gemäß dem Rahmenbeschluss 2006/960/JI des Rates zu verwenden.

I — Verwaltungsinformationen

Ersuchende Behörde (Name, Anschrift, Telefon, Fax, E-Mail, Mitgliedstaat):	
Angaben zum Sachbearbeiter (fakultativ):	
Ersuchen an folgenden Mitgliedstaat:	
Datum und Uhrzeit dieses Ersuchens:	
Aktenzeichen dieses Ersuchens:	

Frühere Ersuchen				
❑ Dies ist das erste Ersuchen in diesem Fall				
❑ Dieses Ersuchen folgt auf frühere Ersuchen in demselben Fall				
Frühere(s) Ersuchen			Antwort(en)	
	Datum	Aktenzeichen (im ersuchenden Mitgliedstaat)	Datum	Aktenzeichen (im ersuchten Mitgliedstaat)
1.				
2.				
3.				
4.				

Falls das Ersuchen an mehr als eine Behörde im ersuchten Mitgliedstaat gerichtet wird, geben Sie bitte alle genutzten Kanäle an:	
❑ Nationale Europol-Stelle/Verbindungsbeamter Europol	❑ Zu Informationszwecken ❑ Zu Vollstreckungszwecken
❑ Nationale Interpolstelle	❑ Zu Informationszwecken ❑ Zu Vollstreckungszwecken
❑ Sirene	❑ Zu Informationszwecken ❑ Zu Vollstreckungszwecken
❑ Verbindungsbeamter	❑ Zu Informationszwecken ❑ Zu Vollstreckungszwecken
❑ Sonstige (bitte angeben):	❑ Zu Informationszwecken ❑ Zu Vollstreckungszwecken
Falls das Ersuchen an andere Mitgliedstaaten gerichtet wird, bitte geben Sie an, um welchen/welche Mitgliedstaat/en es sich handelt und welche Kanäle genutzt wurden (fakultativ)	

II — Fristen

Hinweis: Fristen nach Artikel 4 des Rahmenbeschlusses 2006/960/JI

A – Die Straftat fällt unter Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI

und

die erbetenen Informationen oder Erkenntnisse sind in einer Datenbank verfügbar, auf die eine Strafverfolgungsbehörde unmittelbar zugreifen kann

→ Das Ersuchen ist dringend → Frist: 8 Stunden mit Verlängerungsmöglichkeit

→ Das Ersuchen ist nicht dringend → Frist: 1 Woche

B – Sonstige Fälle: Frist: 14 Tage

❑ **Dringende Bearbeitung IST erbeten**
❑ **Dringende Bearbeitung ist NICHT erbeten**
Gründe für dringende Bearbeitung (z.B. Verdächtige werden in Haft gehalten, der Fall muss vor Ablauf einer bestimmten Frist vor Gericht gebracht werden):
Erbetene Informationen oder Erkenntnisse

ART DER STRAFTAT(EN) ODER KRIMINELLEN AKTIVITÄT(EN), DIE GEGENSTAND DER ERMITTLUNGEN IST (SIND)
Beschreibung der Umstände, unter denen die Straftat(en) begangen wurde(n), einschließlich Tatzeit, Tatort und Art der Beteiligung der Person, auf die sich das Ersuchen um Informationen oder Erkenntnisse bezieht, an der(den) Straftat(en):

Art der Straftat(en)

A – Anwendung von Artikel 4 Absätze 1 oder 3 des Rahmenbeschlusses 2006/960/JI

❑ A.1. Die Straftat ist im ersuchenden Mitgliedstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht
UND
A.2. Bei der Tat handelt es sich um eine (oder mehrere) der folgenden Straftaten:

- ❑ Beteiligung an einer kriminellen Vereinigung
- ❑ Terrorismus
- ❑ Menschenhandel
- ❑ Sexuelle Ausbeutung von Kindern und Kinderpornografie
- ❑ Illegaler Handel mit Drogen und psychotropen Stoffen
- ❑ Illegaler Handel mit Waffen, Munition und Sprengstoffen
- ❑ Korruption
- ❑ Betrugsdelikte, einschließlich Betrug zum Nachteil der finanziellen Interessen der Europäischen Gemeinschaften im Sinne des Übereinkommens vom 26. Juli 1995 über den Schutz der finanziellen Interessen der Europäischen Gemeinschaften
- ❑ Diebstahl in organisierter Form oder mit Waffen
- ❑ Illegaler Handel mit Kulturgütern, einschließlich Antiquitäten und Kunstgegenstände
- ❑ Betrug
- ❑ Erpressung und Schutzgelderpressung
- ❑ Nachahmung und Produktpiraterie
- ❑ Fälschung von amtlichen Dokumenten und Handel damit
- ❑ Fälschung von Zahlungsmitteln
- ❑ Illegaler Handel mit Hormonen und anderen Wachstumsförderern
- ❑ Wäsche von Erträgen aus Straftaten
- ❑ Geldfälschung, einschließlich Euro-Fälschung
- ❑ Cyberkriminalität
- ❑ Umweltkriminalität, einschließlich illegalen Handels mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten
- ❑ Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt
- ❑ Vorsätzliche Tötung, schwere Körperverletzung
- ❑ Illegaler Handel mit Organen und menschlichem Gewebe
- ❑ Entführung, Freiheitsberaubung und Geiselnahme
- ❑ Rassismus und Fremdenfeindlichkeit
- ❑ Illegaler Handel mit nuklearen und radioaktiven Substanzen
- ❑ Handel mit gestohlenen Kraftfahrzeugen
- ❑ Vergewaltigung
- ❑ Brandstiftung
- ❑ Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen
- ❑ Flugzeug-/Schiffsentführung
- ❑ Sabotage

→ Die Straftat fällt somit unter Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI. → Hinsichtlich der für die Beantwortung dieses Ersuchens einzuhaltenden Fristen findet daher Artikel 4 Absatz 1 (dringende Fälle) und Absatz 3 (nicht dringende Fälle) des Rahmenbeschlusses 2006/960/JI Anwendung.

❑ B – Die Straftat(en) fällt (fallen) nicht unter Abschnitt A.
In diesem Fall ist (sind) die Straftat(en) zu beschreiben:

Zweck, zu dem die Informationen oder Erkenntnisse erbeten werden

Zusammenhang zwischen dem Zweck, zu dem die Informationen oder Erkenntnisse erbeten werden, und der Person, auf die sich diese Informationen oder Erkenntnisse beziehen

Identität(en) (soweit bekannt) der Person(en), auf die sich die strafrechtlichen Ermittlungen oder das polizeiliche Erkenntnisgewinnungsverfahren, die bzw. das dem Ersuchen auf Zurverfügungstellung von Informationen oder Erkenntnissen zugrunde liegen bzw. liegt, hauptsächlich bezieht

Gründe zu der Annahme, dass die Informationen oder Erkenntnisse in dem ersuchten Mitgliedstaat vorliegen

Beschränkungen hinsichtlich der Verwendung der in diesem Formblatt enthaltenen Informationen zu anderen Zwecken als zu jenen, für die sie erteilt wurden, oder zur Abwendung einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit

- ❑ Verwendung gestattet
- ❑ Verwendung gestattet, doch ohne Nennung desjenigen, der die Informationen zur Verfügung gestellt hat
- ❑ Verwendung nur nach Genehmigung durch denjenigen, der die Informationen zur Verfügung gestellt hat, gestattet
- ❑ Verwendung nicht gestattet

Abbildung 2

ERSUCHEN UM INFORMATIONEN UND ERKENNTNISSE

gemäß dem Rahmenbeschluss 2006/960/JI des Rates

I – Verwaltungsinformationen

Ersuchender Mitgliedstaat:	
Ersuchende Behörde (Name, Anschrift, Telefon, Fax, E-Mail):	
Angaben zum Sachbearbeiter *(fakultativ)***:**	
Datum und Uhrzeit des Ersuchens:	
Aktenzeichen des Ersuchens:	
Frühere Aktenzeichen:	

Ersuchter/ersuchte Mitgliedstaat/en:		
Kanal:		
☐Nationale Europol-Stelle/Verbindungsbeamter Europol	☐Zu Informationszwecken	☐Zu Vollstreckungszwecken
☐Nationales Zentralbüro von Interpol	☐Zu Informationszwecken	☐Zu Vollstreckungszwecken
☐SIRENE	☐Zu Informationszwecken	☐Zu Vollstreckungszwecken
☐Verbindungsbeamter	☐Zu Informationszwecken	☐Zu Vollstreckungszwecken
☐Sonstiges (genauer anzugeben)	☐Zu Informationszwecken	☐Zu Vollstreckungszwecken

II – Dringlichkeit

Dringende Bearbeitung erbeten	☐ Ja ☐ Nein
Gründe für dringende Bearbeitung (z. B. Verdächtige werden in Haft gehalten, der Fall muss vor Ablauf einer bestimmten Frist vor Gericht gebracht werden): Anwendung von Artikel	
Straftat fällt unter Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI über den Europäischen Haftbefehl	☐ Ja ☐ Nein

III – Zweck

Art der Straftat(en) oder kriminellen Aktivität(en), die Gegenstand der Ermittlungen ist (sind):
Beschreibung - der Umstände der Tatbegehung (beispielsweise Tatzeit und -ort, Art der Tatbeteiligung der Person, auf die sich das Ersuchen um Informationen oder Erkenntnisse bezieht) - der Gründe zu der Annahme, dass die Informationen oder Erkenntnisse in dem ersuchten Mitgliedstaat vorliegen, - des Zusammenhangs zwischen dem Zweck, zu dem die Informationen oder Erkenntnisse erbeten werden, und der Person, auf die sich diese Informationen oder Erkenntnisse beziehen
☐ Ersuchen um Verwendung der Informationen zu Beweiszwecken, sofern nach einzelstaatlichen Rechtsvorschriften möglich *(fakultativ)*

IV – Art der Informationen

Identität/en (soweit bekannt) der Person/en oder Sache/n	
Person	Sache/n
Familienname: Geburtsname: Vorname: Geburtsdatum: Geburtsort: Geschlecht: ☐Männlich ☐weiblich ☐unbekannt Staatsangehörigkeit: Weitere Angaben:	Seriennummer der Waffe: Dokumentennummer: Sonstige Identifizierungsnummer oder Bezeichnung: Fahrzeugkennzeichen: Fahrzeugidentifizierungsnummer (FIN): Art des Dokuments: Kontaktangaben des Unternehmens (Telefon, E-Mail, Anschrift, Website (www…)): Weitere Angaben:

Erbetene Informationen oder Erkenntnisse		
Person	Fahrzeug	Sonstiges
☐ Überprüfung der Identität ☐ Datenbankabfrage ☐ Feststellung der Anschrift / des Aufenthaltsortes	☐ Ergänzung von Identifizierungsdaten ☐ Feststellung des Fahrzeughalters ☐ Feststellung des Fahrzeugführers ☐ Datenbankabfrage	☐ Feststellung eines Unternehmens ☐ Abfrage eines Unternehmens in Datenbanken ☐ Abfrage von Dokumenten in Datenbanken ☐ Feststellung des Inhabers einer Telefon-/Faxnummer ☐ Feststellung des Inhabers einer E-Mail-Adresse ☐ Abfrage einer Anschrift ☐ Abfrage von Waffen ☐ Verkaufsweg einer Waffe
Sonstiges:		

V – Bearbeitungscodes

Beschränkungen hinsichtlich der Verwendung der in diesem Formblatt enthaltenen Informationen zu anderen Zwecken als zu jenen, für die sie erteilt wurden, oder zur Abwendung einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit
☐ Nur für polizeiliche Zwecke, nicht zur Verwendung in Gerichtsverfahren ☐ Vor einer Verwendung Rücksprache mit demjenigen, der die Informationen zur Verfügung gestellt hat ☐ Sonstige Beschränkungen

3.3. Schengen – SIS- II-Datenaustausch und nicht über SIS II laufender Datenaustausch

Das am 14. Juni 1985 unterzeichnete Schengener Übereinkommen wurde 1990 durch das Übereinkommen zur Durchführung des Übereinkommens von Schengen (Schengener Durchführungsübereinkommen/SDÜ)[74] ergänzt, mit dem durch die Abschaffung der Grenzkontrollen zwischen den Schengen-Staaten, gemeinsame Visavorschriften und die polizeiliche und justizielle Zusammenarbeit der Schengen-Raum geschaffen wurde. Das SDÜ legt allgemeine Anforderungen für die polizeiliche Zusammenarbeit fest und ermächtigt die Polizeibehörden, im Rahmen ihrer jeweiligen nationalen Rechtsordnung Informationen auszutauschen.

Mit dem Inkrafttreten des Vertrags von Amsterdam im Jahr 1999 wurden die bisher im Schengen-Rahmen angesiedelten Kooperationsmaßnahmen in den Rechtsrahmen der Europäischen Union einbezogen, und Angelegenheiten mit Schengen-Bezug werden nunmehr von den Gesetzgebungsorganen der EU behandelt. Im Schengen-Protokoll, das dem Vertrag von Amsterdam beigefügt ist, sind ausführliche Regelungen für diesen Integrationsprozess niedergelegt.

Das Schengener Informationssystem (SIS) wurde gemäß den Bestimmungen von Titel IV des Übereinkommens vom 19. Juni 1990 eingerichtet. Es stellt ein wichtiges Instrument für die Anwendung des Schengen-Besitzstands dar. Es ist auch eine Maßnahme, mit der darauf abgezielt wird, den Wegfall der Personenkontrollen an den Binnengrenzen im Schengen-Raum durch ein Instrument für den Informationsaustausch zwischen zuständigen Behörden zu kompensieren.

Obwohl der Rechtsrahmen für das SIS gegenwärtig aus zwei verschiedenen Instrumenten besteht, nämlich einer Verordnung für die Anwendung des SIS an Grenzen und einem Ratsbeschluss über die polizeiliche Zusammenarbeit, stellt das SIS ein einziges Informationssystem dar.

---

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

Rechtsvorschriften

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

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

Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates, ABl. L 135 vom 22.5.2019, S. 27

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

Kernbestimmungen

Das Schengener Informationssystem (SIS) ist sowohl ein System der polizeilichen Zusammenarbeit als auch ein Grenzkontrollsystem und unterstützt die operative Zusammenarbeit zwischen Polizei- und Justizbehörden in Strafsachen. Benannte Polizei-, Grenzschutz- und Zollbeamte sowie Visum- und Justizbehörden im ganzen Schengen-Raum können das SIS konsultieren[75].

Das Schengener Informationssystem der zweiten Generation ("SIS II") ist gegenwärtig in 26 EU-Mitgliedstaaten sowie in vier mit der Schengen-Zusammenarbeit assoziierten Nicht-EU-Staaten (Norwegen, Island, Schweiz und Liechtenstein) in Betrieb.

[75] Eine konsolidierte Liste nationaler zuständiger Behörden, in der angegeben wird, welche Daten sie jeweils für welche Zwecke abrufen dürfen, wird jährlich im Amtsblatt der EU gemäß Artikel 31 Absatz 8 der SIS-Verordnung und Artikel 46 Absatz 8 des SIS-II-Beschlusses veröffentlicht.

- Was die polizeiliche Zusammenarbeit anbelangt, so haben das Vereinigte Königreich und Irland beantragt, an der Zusammenarbeit teilnehmen zu dürfen, aber nur dem Vereinigten Königreich ist 2015 gestattet worden, vorläufig Daten aus diesem Teil des SIS hochzuladen[76]; dies ist ein erster Schritt, nach dem eine Bewertung erfolgt, bevor ein endgültiger Beschluss über die Inkraftsetzung erfolgt. Das Vereinigte Königreich und Irland nehmen nicht an der Anwendung des SIS für den Zweck der Grenzkontrolle teil.

- Bulgarien, Rumänien[77] und Kroatien[78] wenden die Bestimmungen des Schengen-Besitzstands hinsichtlich der polizeilichen Zusammenarbeit und der Grenzkontrolle an. Ihnen wurde für die Bewertung der korrekten Anwendung der Bestimmungen des Schengen-Besitzstands hinsichtlich des SIS Echtzeitzugang zum SIS gewährt. Sobald die Bewertungen mit zufriedenstellendem Ergebnis durchgeführt worden sind, ergeht ein gesonderter Ratsbeschluss, in dem ein Datum für die Aufhebung der Kontrollen an den Binnengrenzen festgelegt wird. Bis zu diesem Zeitpunkt bleiben bestimmte Einschränkungen der Nutzung des SIS weiterhin in Kraft.

- Zypern hat noch keinen Zugriff auf das SIS.

SIS-II-Daten können (unter Einhaltung strenger Datenschutzvorschriften) rund um die Uhr über die SIRENE-Büros, an den Grenzübergangsstellen, innerhalb des nationalen Hoheitsgebiets und im Ausland in den konsularischen Vertretungen online abgefragt werden. Die Daten werden als Ausschreibungen bezeichnet, wobei unter Ausschreibungen Datensätze zu verstehen sind, die den Behörden die Identifizierung von **Personen** (d. h. Unionsbürger und Drittstaatsangehörige) oder **Gegenständen** ermöglichen, sodass sie geeignete Maßnahmen für die Zwecke der Bekämpfung der Kriminalität und der irregulären Einwanderung ergreifen können.

Besonders ermächtigte Bedienstete von Europol haben das Recht, im Rahmen ihres Mandats in das SIS II eingegebene Daten direkt abzufragen, und können um weitere Informationen des betreffenden Mitgliedstaats ersuchen.

Die nationalen Eurojust-Mitglieder und ihre Assistenten haben das Recht, im Rahmen ihres Mandats auf die in das SIS II eingegebenen Daten zuzugreifen und solche Daten abzufragen.

---

76 Durchführungsbeschluss (EU) 2015/215 des Rates vom 10. Februar 2015 zur Inkraftsetzung der Bestimmungen des Schengen-Besitzstands über Datenschutz und zur vorläufigen Inkraftsetzung von Teilen der Bestimmungen des Schengen-Besitzstands über das Schengener Informationssystem für das Vereinigte Königreich Großbritannien und Nordirland, ABl. L 36 vom 12.2.2015, S. 8.

77 Beschluss 2010/365/EU des Rates vom 29. Juni 2010 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).

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

Nach Maßgabe des Artikels 47 SDÜ sind die zu Polizeidienststellen in anderen Schengen-Staaten entsandten Verbindungsbeamten verantwortlich für den Informationsaustausch gemäß

- Artikel 39 Absätze 1, 2 und 3 im Einklang mit dem nationalen Recht für die Zwecke der Verhütung und Aufdeckung von Straftaten;

- Artikel 46, auch aus eigener Initiative, für die Zwecke der Verhütung von Straftaten gegen die öffentliche Sicherheit und Ordnung oder zur Abwehr entsprechender Bedrohungen.

Es sei darauf hingewiesen, dass die Bestimmungen des Artikels 39 Absätze 1, 2 und 3 sowie des Artikels 46, soweit sie den Austausch von Informationen und Erkenntnissen in Bezug auf Schwerkriminalität betreffen, durch die entsprechenden Bestimmungen des Rahmenbeschlusses 2006/960/JI des Rates, des sogenannten "schwedischen Rahmenbeschlusses", ersetzt werden. Die Bestimmungen des Artikels 39 Absätze 1, 2 und 3 sowie des Artikels 46 behalten jedoch in Bezug auf Straftaten, die mit einer Freiheitsstrafe von weniger als 12 Monaten bedroht sind, ihre Gültigkeit.

3.4. Europol

Rechtsvorschriften

Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates, ABl. L 135 vom 24.5.2016, S. 53-114 (anwendbar seit dem 1. Mai 2017)

Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates, ABl. L 135 vom 22.5.2019, S. 27

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

Kernbestimmungen

Europol hat zum Ziel, die Tätigkeit der für Prävention und Bekämpfung von Kriminalität zuständigen Behörden der Mitgliedstaaten sowie deren Zusammenarbeit bei der Prävention und Bekämpfung von organisierter Kriminalität, Terrorismus und anderen Formen schwerer Kriminalität zu unterstützen und zu verstärken, wenn zwei oder mehr Mitgliedstaaten betroffen sind. Zu diesem Zweck sammelt, speichert, verarbeitet und analysiert Europol Informationen und kriminalpolizeiliche Erkenntnisse und tauscht sie aus.

Jeder Mitgliedstaat benennt eine nationale Stelle (ENU), die als Verbindungsstelle zwischen Europol und den zuständigen Behörden der Mitgliedstaaten fungiert. Die ENU ist mit Aufgaben in Bezug auf die Weitergabe relevanter Informationen und Erkenntnisse betraut. Jede nationale Stelle entsendet mindestens einen Verbindungsbeamten, der das nationale Verbindungsbüro bei Europol bildet und die Interessen der nationalen Stelle vertritt. Die Verbindungsbeamten sind zum einen mit der Informationsweitergabe zwischen den Mitgliedstaaten und Europol und zum anderen mit der bilateralen Weitergabe von Informationen zwischen anderen Ländern betraut. Dieser bilaterale Austausch kann sich auch auf Straftaten erstrecken, die über das Europol-Mandat hinausgehen.

Mit der Europol-Verordnung wird ein neues Konzept für die Datenverarbeitung, das als Konzept zur integrierten Datenverwaltung (Integrated Data Management Concept – IDMC) bezeichnet wird, eingeführt. Das IDMC kann als die Möglichkeit definiert werden, Kriminalität betreffende Informationen zu vielfältigen Geschäftszwecken wie vom Dateneigentümer angegeben zu nutzen; dadurch wird die Verwaltung und die Verarbeitung in integrierter und technologieneutraler Weise ermöglicht. Nach dem Europol-Beschluss des Rates war die Datenverarbeitung nach Systemen strukturiert. Die Europol-Verordnung enthält nicht mehr Bezugnahmen auf Systeme, sondern schreibt stattdessen vor, dass Verarbeitungszwecke angegeben werden. Damit ein reibungsloser Übergang gewährleistet wird, können die Nutzer weiterhin mit den vorhandenen Systemen auf eine Weise arbeiten, die mit dem neuen Rechtsrahmen vereinbar ist.

Die nationale Stelle ist verantwortlich für die Kommunikation mit dem Europol-Informationssystem (EIS), das zur Verarbeitung der für die Erfüllung der Aufgaben von Europol erforderlichen Daten verwendet wird. Die nationale Stelle, die Verbindungsbeamten und ordnungsgemäß ermächtigtes Personal von Europol haben das Recht, Daten in die Systeme einzugeben und von dort abzurufen. Informationen, die in das EIS eingegeben werden, gelten im Allgemeinen als zum Zwecke eines Abgleichs (Artikel 18 Absatz 2 Buchstabe a der Verordnung) und einer strategischen/thematischen Analyse (Artikel 18 Absatz 2 Buchstabe b der Verordnung) zur Verfügung gestellt.

3.5. Interpol

Rechtsvorschriften

Interpol-Statuten[79]

Vorschriften für die Verarbeitung von Informationen[80]

Vorschriften über die Kontrolle von Informationen und den Zugang zu den Dateien von Interpol

Kernbestimmungen

Aufgabe von Interpol ist es, die internationale polizeiliche Zusammenarbeit im Hinblick auf die Verhütung und Bekämpfung der Kriminalität durch verstärkte Zusammenarbeit und Innovation in den Polizei- und Sicherheitsangelegenheiten zu erleichtern. Interpol handelt im Rahmen der in den Mitgliedstaaten geltenden Rechtsvorschriften und im Geiste der Allgemeinen Erklärung der Menschenrechte. Jeder der 190 Mitgliedstaaten unterhält ein nationales Zentralbüro (NCB), das mit seinen eigenen hochqualifizierten Strafverfolgungsbeamten besetzt ist.

Die Interpol-Statuten sind eine internationale Übereinkunft, die alle die Länder, die 1956 an seiner Verabschiedung teilgenommen haben, als Mitglieder bestätigt und das Verfahren zur Beantragung des Beitritts zu Interpol für die Länder festlegt, die 1956 noch keine Mitglieder waren.

Als wichtigstes Rechtsdokument legen die Interpol-Statuten die Zielsetzungen von Interpol fest. In ihnen ist das Mandat der Organisation niedergelegt, das darin besteht, eine möglichst weitgehende Zusammenarbeit zwischen allen Kriminalpolizeibehörden sicherzustellen und Straftaten des allgemeinen Strafrechts zu bekämpfen.

Über die Statuten hinaus wird der rechtliche Rahmen von Interpol von einer Reihe von grundlegenden Texten gebildet. Es sind mehrere Kontrollebenen eingerichtet worden, um die Einhaltung der Vorschriften zu gewährleisten. Diese Ebenen betreffen Kontrollen durch die nationalen Zentralbüros (NCB), das Generalsekretariat und das unabhängige Aufsichtsgremium, das als "Commission for the Control of Interpol's Files" (Kommission für die Kontrolle der Interpol-Dossiers) bekannt ist.

---

79 http://www.interpol.int
80 http://www.interpol.int

3.6. Verbindungsbeamte

Rechtsvorschriften

Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 19. Juni 1990 (SDÜ)[81], Artikel 47

Beschluss 2003/170/JI des Rates vom 27. Februar 2003 über die gemeinsame Inanspruchnahme von Verbindungsbeamten, die von den Strafverfolgungsbehörden der Mitgliedstaaten entsandt sind[82]

Beschluss 2006/560/JI des Rates vom 24. Juli 2006 zur Änderung des Beschlusses 2003/170/JI über die gemeinsame Inanspruchnahme von Verbindungsbeamten, die von den Strafverfolgungsbehörden der Mitgliedstaaten entsandt sind[83]

Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates, ABl. L 135 vom 24.5.2016, S. 53-114 (anwendbar seit dem 1. Mai 2017)

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

Bilaterale Vereinbarungen

Kernbestimmungen

Gemäß Artikel 47 SDÜ können die Mitgliedstaaten "bilaterale Absprachen über die befristete oder unbefristete Entsendung von Verbindungsbeamten [eines Mitgliedstaats] zu Polizeidienststellen [eines anderen Mitgliedstaats] treffen". Die Verbindungsbeamten sind nicht befugt, eigenständig polizeiliche Maßnahmen durchzuführen, und in Artikel 47 ist bestimmt, dass die Entsendung zum Ziel hat, "die Zusammenarbeit (...) zu fördern und zu beschleunigen, insbesondere durch

a) Unterstützung des Informationsaustausches zur präventiven und repressiven Verbrechensbekämpfung;

---

81 Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 19. Juni 1990 (SDÜ), ABl. L 239 vom 22.9.2000, S. 19.

82 Beschluss 2003/170/JI des Rates vom 27. Februar 2003, ABl. L 67 vom 12.3.2003, S. 27.

83 Beschluss 2006/560/JI des Rates vom 24. Juli 2006, ABl. L 219 vom 10.8.2006, S. 31.

b) Unterstützung bei polizeilicher und justizieller Rechtshilfe in Strafsachen;

c) Unterstützung der grenzüberwachenden Behörden an den Außengrenzen".

Weitere Informationen über derartige Entsendungen finden sich im Fußballhandbuch[84] und in der Empfehlung des Rates vom 6. Dezember 2007 betreffend einen Leitfaden für die Polizei- und Sicherheitsbehörden zur Zusammenarbeit bei Großveranstaltungen mit internationaler Dimension[85].

Die Bestimmung des SDÜ, wonach nationale Verbindungsbeame auch die Interessen eines oder mehrerer anderer Mitgliedstaaten vertreten dürfen, ist durch den Beschluss des Rates über die gemeinsame Inanspruchnahme von Verbindungsbeamten, die von den Strafverfolgungsbehörden der Mitgliedstaaten entsandt sind (2006 geändert), weiterentwickelt worden. Ferner wurden Vorkehrungen für die Verbesserung der Zusammenarbeit zwischen den Verbindungsbeamten verschiedener Mitgliedstaaten am Ort ihrer Entsendung getroffen. In verschiedenen Gremien wurde hervorgehoben, dass diese Zusammenarbeit gefördert werden sollte.

Entsprechend der Europol-Verordnung bestimmt jeder Mitgliedstaat eine nationale Stelle (ENU), die als Verbindungsstelle zwischen Europol und den für die Verhütung und Bekämpfung von Straftaten zuständigen Behörden der Mitgliedstaaten fungiert. Die ENU ist mit Aufgaben in Bezug auf die Weitergabe relevanter Informationen und Erkenntnisse betraut. Jede nationale Stelle entsendet mindestens einen Verbindungsbeamten, der das nationale Verbindungsbüro bei Europol bildet und die Interessen der nationalen Stelle vertritt. Die Verbindungsbeamten sind zum einen mit der Informationsweitergabe zwischen den nationalen Stellen und Europol und zum anderen mit der bilateralen Weitergabe von Informationen zwischen anderen nationalen Stellen betraut. Dieser bilaterale Austausch kann sich auch auf Straftaten erstrecken, die über das Europol-Mandat hinausgehen.

In den Artikeln 17 und 18 des Beschlusses 2008/615/JI des Rates ("Prümer Beschluss") ist die Entsendung nationaler Beamter für die Zwecke der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung und zur Verhinderung von Straftaten vorgesehen.

---

84 Entschließung des Rates vom 3. Juni 2010 betreffend ein aktualisiertes Handbuch mit Empfehlungen für die internationale polizeiliche Zusammenarbeit und Maßnahmen zur Vorbeugung und Bekämpfung von Gewalttätigkeiten und Störungen im Zusammenhang mit Fußballspielen von internationaler Dimension, die zumindest einen Mitgliedstaat betreffen, ABl. C 444 vom 29.11.2016, S. 1.

85 ABl. C 314 vom 22.12.2007, S. 4.

3.7. "Prüm"- Datenaustausch

Rechtsvorschriften

- Beschluss 615/2008/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität

- 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

Kernbestimmungen

Die Mitgliedstaaten gewähren sich gegenseitig den grenzüberschreitenden Online-Zugang zu den Fundstellendatensätzen ihrer DNA-Analyse-Dateien und automatisierten Fingerabdruck-Identifizierungssystemen (AFIS) sowie zu Fahrzeugregisterdaten (VRD) (siehe Kapitel 2 des Beschlusses 2008/615/JHA des Rates).

In jedem Mitgliedstaat muss eine spezielle nationale Kontaktstelle benannt werden. Den Datenschutz- und Datensicherheitsvorschriften ist in den nationalen Rechtvorschriften angemessen Rechnung zu tragen. Der automatisierte Abgleich anonymer biometrischer Profile beruht auf einem "Treffer/kein Treffer"-System, außer bei VRD, bei denen die erbetenen den Eigentümer/Halter betreffenden Daten automatisch ausgegeben werden.

Im Falle einer Übereinstimmung biometrischer Daten erhält die nationale Kontaktstelle des ersuchenden Mitgliedstaats automatisch die Bezugsdaten, mit denen die Übereinstimmung erzielt wurde.

Zusätzliche spezifische personenbezogene Daten und weitere Informationen zu den Fundstellendatensätzen können dann im Wege der Amtshilfeverfahren – auch im Wege der gemäß dem "schwedischen Rahmenbeschluss" angenommenen – angefordert werden.

Die Bereitstellung solcher zusätzlichen Daten richtet sich nach dem nationalen Recht – einschließlich der Vorschriften über die Rechtshilfe – des ersuchten Mitgliedstaats. Es gilt, dass die Bereitstellung personenbezogener Daten ein angemessenes Datenschutzniveau seitens der empfangenden Mitgliedstaaten voraussetzt[86].

Für die Verhütung von Straftaten und im Interesse der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung bei Großveranstaltungen mit grenzüberschreitender Dimension können die Mitgliedstaaten auf Antrag oder auch auf eigene Initiative einander nicht-personenbezogene Daten sowie personenbezogene Daten bereitstellen. Zu diesem Zweck werden spezielle nationale Kontaktstellen benannt (siehe Kapitel 3 des Beschlusses 2008/615/JI des Rates).

Zur Verhütung terroristischer Straftaten können die Mitgliedstaaten einander unter bestimmten Umständen personenbezogene Daten bereitstellen. Zu diesem Zweck werden spezielle nationale Kontaktstellen benannt (siehe Kapitel 4 des Beschlusses 2008/615/JI des Rates).

3.8. Visa-Informationssystem (VIS)

Rechtsvorschriften

Entscheidung 2004/512/EG des Rates vom 8. Juni 2004 zur Einrichtung des Visa-Informationssystems (VIS), ABl. L 213 vom 15.6.2004, S. 5.

Beschluss 2013/392/EU des Rates zur Festlegung des Zeitpunkts, ab dem der Beschluss 2008/633/JI über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten gilt, ABl. L 198 vom 23.7.2013, S. 45[87]

---

[86] Der Beschluss 2008/615/JI des Rates befolgt das für die Verarbeitung personenbezogener Daten festgelegte Schutzniveau gemäß dem Übereinkommen des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, dem Zusatzprotokoll vom 8. November 2001 zu dem Übereinkommen und den Grundsätzen der Empfehlung Nr. R (87) 15 des Europarats über die Nutzung personenbezogener Daten im Polizeibereich.

[87] Am 16. April 2015 hat der Europäische Gerichtshof den Beschluss 2013/392/EU des Rates vom 22. Juli 2013 zur Festlegung des Zeitpunkts, ab dem der Beschluss 2008/633/JI über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten gilt, für nichtig erklärt. Der Gerichtshof hat jedoch erklärt, dass die Wirkungen des Beschlusses 2013/392 bis zum Inkrafttreten eines neuen Rechtsakts, der ihn ersetzen soll, aufrechterhalten werden.

Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates, ABl. L 135 vom 22.5.2019, S. 27

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

Kernbestimmungen

Das VIS ist ein System, das den zuständigen nationalen Behörden ermöglicht, Daten für ein (sogenanntes Schengen-)Visum für einen kurzfristigen Aufenthalt einzugeben und zu aktualisieren und diese Daten elektronisch abzufragen. Es beruht auf einer zentralisierten Architektur und besteht aus einem zentralen Informationssystem, dem zentralen Visa-Informationssystem (CS-VIS), einer nationalen Schnittstelle in jedem Mitgliedstaat (NI-VIS) und der Infrastruktur für die Kommunikation zwischen CS-VIS und NI-VIS. Gemäß dem Beschluss 2008/633/JHA kann das VIS zur Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten eingesetzt werden. Der Beschluss ermöglicht den benannten Strafverfolgungsbehörden (wie etwa Behörden, die für die Bekämpfung von Terrorismus oder schweren Straftaten, z. B. Drogenhandel oder Menschenhandel, zuständig sind) in den Ländern des Schengen-Raums und Europol den Zugang zum VIS. Die benannten nationalen Behörden müssen ein Verfahren für den Zugang zum VIS befolgen, nachdem alle Bedingungen für den Zugang erfüllt sind.

Im Mai 2018 hat die Kommission einen Gesetzgebungsvorschlag zur Änderung der VIS-Verordnung vorgelegt, mit dem unter anderem die Interoperabilität zwischen anderen Datenbanken im Bereich Justiz und Inneres, über die Visa für den längerfristigen Aufenthalt und Aufenthaltstitel im VIS registriert werden, gewährleistet werden soll. Der Vorschlag enthält zudem Vorschriften über den Zugang der Strafverfolgungsbehörden zum VIS, die weiterentwickelt werden, und hebt den Beschluss 2008/633/JHA auf.

Das aktualisierte VIS wird voraussichtlich nicht vor Ende 2021 einsatzbereit sein.

3.9. Eurodac

Rechtsvorschriften

Das europäische automatisierte Fingerabdruck-Identifizierungssystem (Eurodac) ist ein Computersystem, das ursprünglich die wirksame Anwendung des Dubliner Übereinkommens erleichtern sollte. Das am 15. Juni 1990 unterzeichnete Dubliner Übereinkommen wurde ersetzt durch die Verordnung (EG) Nr. 343/2003 des Rates vom 18. Februar 2003 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen in einem Mitgliedstaat gestellten Asylantrags zuständig ist.

Im Anschluss an Änderungen an den Eurodac-Verordnungen wurden diese mit den folgenden Verordnungen neu gefasst:

Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist, und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (Neufassung), ABl. L 180 vom 29.6.2013, S. 1;

Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates, ABl. L 135 vom 22.5.2019, S. 27;

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

Kernbestimmungen

In der Verordnung (EU) Nr. 603/2013 sind der Zweck von Eurodac und die Voraussetzungen für den Zugang benannter nationaler Strafverfolgungsbehörden und von Europol zu den Eurodac-Daten zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer[88] und sonstiger schwerwiegender Straftaten[89] niedergelegt.

3.10. Neapel- II-Übereinkommen

Rechtsvorschriften

Rechtsakt des Rates vom 18. Dezember 1997 über die Ausarbeitung des Übereinkommens aufgrund von Artikel K.3 des Vertrags über die Europäische Union über gegenseitige Amtshilfe und Zusammenarbeit der Zollverwaltungen, ABl. C 24 vom 23.1.1998, S. 1

Kernbestimmungen

Die Mitgliedstaaten unterstützen einander, um Verstöße gegen nationale Zollvorschriften zu verhüten und aufzuspüren und Verstöße gegen gemeinschaftliche und nationale Zollvorschriften zu verfolgen und zu bestrafen. Für strafrechtliche Ermittlungen sind im Neapel- II-Übereinkommen Verfahren festgelegt, die es den Zollverwaltungen ermöglichen, gemeinsam zu handeln und auf eigene Initiative oder auf Antrag Daten über illegale Handelsvorgänge auszutauschen.

Ersuchen werden schriftlich in einer Amtssprache des Mitgliedstaats der ersuchten Behörde oder in einer von dieser akzeptierten Sprache gestellt. In einem Formular ist der Standard für die Informationsübermittlung vorgegeben. Die betreffenden Behörden übermitteln alle Informationen, die für die Verhütung, Aufklärung und Verfolgung von Verstößen hilfreich sein können. Sie tauschen personenbezogene Daten aus, d. h. alle Informationen über eine bestimmte oder bestimmbare natürliche Person.

Bei der erbetenen Amtshilfe verfährt die ersuchte Behörde oder die von ihr befasste zuständige Behörde so, als ob sie in Erfüllung eigener Aufgaben oder auf Ersuchen einer anderen Behörde ihres eigenen Mitgliedstaats handeln würde.

---

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

89 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).

3.10.1. Zollinformationssystem – ZIS[90]

Das Zollinformationssystem ergänzt das Neapel- II-Übereinkommen[91]. Das von der Kommission verwaltete zentralisierte Informationssystem stellt ab auf eine Verbesserung der Zollverwaltungen der Mitgliedstaaten durch einen schnellen Informationsaustausch im Hinblick auf die Verhütung, Ermittlung und Verfolgung schwerer Verstöße gegen das nationale und das Gemeinschaftsrecht. Mit dem Zollinformationssystem wird auch ein Aktennachweissystem für Zollzwecke (FIDE) zur Unterstützung von Zollermittlungen eingerichtet.

Die von den Mitgliedstaaten benannten Behörden[92] haben direkten Zugang zu den im ZIS gespeicherten Daten. Zur Verstärkung der Komplementarität haben Europol und Eurojust Lesezugriff auf ZIS und FIDE.

Das ZIS enthält personenbezogene Daten mit Bezug auf Ausgangsstoffe, Beförderungsmittel, Unternehmen, Personen und Waren sowie einbehaltenes, eingezogenes oder beschlagnahmtes Bargeld. Personenbezogene Daten dürfen nur für Risikomanagement- oder operative Analysen vom ZIS in andere Datenverarbeitungssysteme kopiert werden, zu denen nur die von den Mitgliedstaaten benannten Analyseexperten Zugang haben.

Wenn sie eine Ermittlungsakte anlegen, können die für Zollermittlungen zuständigen nationalen Behörden anhand von FIDE feststellen, ob andere Behörden bereits Ermittlungen zu einer bestimmten Person oder einem bestimmten Unternehmen durchgeführt haben.

3.11. Nationale Vermögensabschöpfungsstellen (ARO) und CARIN

Rechtsvorschriften

Beschluss 2007/845/JI des Rates vom 6. Dezember 2007 über die Zusammenarbeit zwischen den Vermögensabschöpfungsstellen der Mitgliedstaaten auf dem Gebiet des Aufspürens und der Ermittlung von Erträgen aus Straftaten oder anderen Vermögensgegenständen im Zusammenhang mit Straftaten, ABl. L 332 vom 18.12.2007, S. 103

Das Camdener zwischenstaatliche Netz der Vermögensabschöpfungsstellen (CARIN) wurde von Österreich, Belgien, Deutschland, Irland, den Niederlanden und dem Vereinigten Königreich am 22./23. September 2004 in Den Haag eingerichtet.

---

90 Beschluss 2009/917/JI des Rates vom 30. November 2009 über den Einsatz der Informationstechnologie im Zollbereich, ABl. L 323 vom 10.12.2009, S. 20.

91 Übereinkommen aufgrund von Artikel K.3 des Vertrags über die Europäische Union über gegenseitige Amtshilfe und Zusammenarbeit der Zollverwaltungen, ABl. C 24 vom 23.1.1998, S. 2.

92 Anwendung des Artikels 7 Absatz 2 und des Artikels 8 Absatz 3 des Beschlusses 2009/917/JI des Rates vom 30. November 2009 über den Einsatz der Informationstechnologie im Zollbereich – aktualisierte Liste der zuständigen Behörden, Dok. 13394/11 ENFOCUSTOM 85.

Kernbestimmungen

Seit der Annahme des Beschlusses 2007/845/JI[93] des Rates haben alle Mitgliedstaaten Vermögensabschöpfungsstellen (ARO) eingerichtet und benannt. Sie können über das SIENA-System direkt Informationen über Angelegenheiten in Bezug auf die Abschöpfung von Vermögenswerten austauschen. Unter der Schirmherrschaft der Europäischen Kommission und Europols erleichtert das ARO-Netz die Zusammenarbeit zwischen den Vermögensabschöpfungsstellen der Mitgliedstaaten und die strategische Erörterung und den Austausch bewährter Verfahren. Das Europol-Büro für Erträge aus Straftaten (ECAB) fungiert als Zentralstelle für die Abschöpfung von Vermögenswerten innerhalb der EU.

Mit der Richtlinie 2014/42/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Sicherstellung und Einziehung von Tatwerkzeugen und Erträgen aus Straftaten in der Europäischen Union[94] soll die Wirksamkeit der Zusammenarbeit zwischen den Vermögensabschöpfungsstellen innerhalb der Europäischen Union weiter verbessert werden. Die Mitgliedstaaten sind aufgefordert, die Richtlinie bis zum 4. Oktober 2016 umzusetzen.

Das Camdener zwischenstaatliche Netz der Vermögensabschöpfungsstellen (CARIN), das 2004 eingerichtet wurde, um die grenzüberschreitende Ermittlung, Einfrierung, Beschlagnahme und Einziehung von Vermögenswerten im Zusammenhang mit Straftaten zu unterstützen, verbessert den gegenseitigen Austausch von Informationen über verschiedene über die EU hinausreichende nationale Ansätze.

Seit 2015 umfasst das CARIN Angehörige der Rechtsberufe aus 53 Hoheitsgebieten und 9 internationalen Organisationen, die als Kontaktstellen für die Zwecke eines raschen – auf Antrag oder auf eigene Initiative erfolgenden – grenzüberschreitenden Informationsaustauschs dienen. Die nationalen Geldabschöpfungsstellen arbeiten untereinander oder mit anderen Behörden, die das Aufspüren und die Ermittlung von Erträgen aus Straftaten erleichtern, zusammen. Zwar haben alle Mitgliedstaaten eine Geldabschöpfungsstelle eingerichtet, aber es bestehen noch größere Unterschiede zwischen den Mitgliedstaaten in Bezug auf Organisationsstruktur, Ressourcen und Tätigkeiten.

---

93 Beschluss 2007/845/JI des Rates vom 6. Dezember 2007 über die Zusammenarbeit zwischen den Vermögensabschöpfungsstellen der Mitgliedstaaten auf dem Gebiet des Aufspürens und der Ermittlung von Erträgen aus Straftaten oder anderen Vermögensgegenständen im Zusammenhang mit Straftaten, ABl. L 332 vom 18.12.2007, S. 103.

94 Richtlinie 2014/42/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Sicherstellung und Einziehung von Tatwerkzeugen und Erträgen aus Straftaten in der Europäischen Union, ABl. L 127 vom 29.4.2014, S. 39.

Die ausgetauschten Informationen können entsprechend den Datenschutzvorschriften des empfangenden Mitgliedstaaten verwendet werden und unterliegen den gleichen Datenschutzvorschriften, die auch gelten würden, wenn die Informationen im empfangenden Mitgliedstaat erhoben worden wären. Der spontane Informationsaustausch nach dem betreffenden Beschluss unter Einhaltung der im schwedischen Rahmenbeschluss vorgesehenen Verfahren und Fristen muss gefördert werden.

3.12. Zentrale Meldestellen für Geldwäsche-Verdachtsanzeigen (FIU)

Rechtsvorschriften

Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission
ABl. L 141 vom 5.6.2015, S. 73

Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Festlegung von Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten und zur Aufhebung des Beschlusses 2000/642/JI des Rates
ABl. L 186 vom 11.7.2019, S. 122

Kernbestimmungen

Nach der Richtlinie 2015/849 (4. Geldwäscherichtlinie, geändert durch die Richtlinie 2018/843) richtet jeder Mitgliedstaat eine zentrale Meldestelle ein, um Geldwäsche und Terrorismusfinanzierung zu verhindern, aufzudecken und wirksam zu bekämpfen. Als zentrale nationale Stelle ist die zentrale Meldestelle dafür zuständig, Meldungen über verdächtige Transaktionen und sonstige Informationen, die im Hinblick auf Geldwäsche, damit zusammenhängende Vortaten oder Terrorismusfinanzierung von Belang sind, entgegenzunehmen und zu analysieren. Ihr obliegt es, bei begründetem Verdacht auf Geldwäsche, damit zusammenhängende Vortaten oder Terrorismusfinanzierung die Ergebnisse ihrer Analysen und alle zusätzlichen relevanten Informationen an die zuständigen Behörden weiterzugeben. Sie muss in der Lage sein, von den Verpflichteten zusätzliche Informationen einzuholen. Die zentralen Meldestellen müssen in der Lage sein, Auskunftsersuchen der zuständigen Behörden ihres jeweiligen Mitgliedstaats zu beantworten, sofern die Auskunftsersuchen auf Belangen im Zusammenhang mit Geldwäsche, damit im Zusammenhang stehenden Vortaten oder Terrorismusfinanzierung beruhen.

Über den oben beschriebenen Austausch in Bezug auf Geldwäsche und Terrorismusfinanzierung hinaus ist in der Richtlinie (EU) 2019/1153 vorgesehen, dass jeder Mitgliedstaat sicherstellt, dass seine nationale zentrale Meldestelle auch zur Zusammenarbeit mit den benannten Strafverfolgungsbehörden des Mitgliedstaats verpflichtet und in der Lage ist, begründete Ersuchen dieser benannten zuständigen Behörden um Finanzinformationen oder Finanzanalysen zu beantworten, wenn diese Ersuchen auf Belangen im Zusammenhang mit der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von in Anhang I der Europol-Verordnung (Verordnung (EU) 2016/794) aufgeführten schweren Straftaten beruhen.

In beiden Fällen kann die zentrale Meldestelle die Bereitstellung von Informationen verweigern, wenn es objektive Gründe für die Annahme gibt, dass sich die Bereitstellung negativ auf laufende Ermittlungen auswirken würde, oder wenn die Weitergabe der Informationen im Verhältnis zu den rechtmäßigen Interessen einer natürlichen oder juristischen Person eindeutig unverhältnismäßig wäre oder die Informationen für die Zwecke, zu denen sie angefordert wurden, irrelevant sind.

Nach der Richtlinie (EU) 2015/849 (Geldwäsche-Richtlinie) sorgen die Mitgliedstaaten dafür, dass die zentralen Meldestellen spontan oder auf Ersuchen sämtliche Informationen untereinander austauschen, die für die zentralen Meldestellen bei der Verarbeitung oder Auswertung von Informationen im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung und bezüglich der beteiligten natürlichen oder juristischen Personen von Belang sein können, selbst wenn zum Zeitpunkt des Austauschs die Art der Vortaten, die damit im Zusammenhang stehen können, nicht feststeht, und unabhängig von der Art dieser Vortaten. Eine zentrale Meldestelle kann den Informationsaustausch nur in Ausnahmefällen verweigern, wenn der Austausch im Widerspruch zu den Grundprinzipien ihres nationalen Rechts stehen könnte. Die Mitgliedstaaten stellen sicher, dass die gemäß den Artikeln 52 und 53 ausgetauschten Informationen nur zu dem Zweck verwendet werden, zu dem sie verlangt oder zur Verfügung gestellt wurden.

Zusätzlich zu dem Austausch zwischen den zentralen Meldestellen (FIU) verschiedener Mitgliedstaaten gemäß der Richtlinie (EU) 2015/849 ist in der Richtlinie (EU) 2019/1153 nunmehr vorgesehen, dass die zentralen Meldestellen in Ausnahme- und Dringlichkeitsfällen auch befugt sind, Finanzinformationen oder Finanzanalysen auszutauschen, die für die Verarbeitung oder Analyse von Informationen im Zusammenhang mit Terrorismus oder organisierter Kriminalität mit Bezug zu Terrorismus von Belang sein können. Nach der Richtlinie (EU) 2019/1153 ist zudem der Informationsaustausch zwischen den zentralen Meldestellen und Europol gestattet.

Beim Netz FIU.NET handelt es sich um ein dezentrales Computernetz für den Austausch von Informationen zwischen zentralen Meldestellen.

FIU.NET, das ursprünglich die Stellung der zentralen Meldestellen stärken sollte, hat sich in den letzten Jahren von einem sicheren Basiswerkzeug für einen strukturierten bilateralen Informationsaustausch zu einem sicheren Multifunktionswerkzeug für den multilateralen Informationsaustausch entwickelt, das auch über Fallverwaltungsfunktionen sowie eine halbautomatische Standardisierung der Prozesse verfügt. Im FIU.NET sind jede neue Funktion und die automatische Verarbeitung optional, ohne Auflagen. Die einzelne zentrale Meldestelle kann entscheiden, welche der vom FIU.NET gebotenen Möglichkeiten und Funktionen sie nutzen will; sie nutzt die Funktionen, mit denen sie gut zurecht kommt, und schließt die Funktionen aus, die sie nicht nutzen muss oder will.

3.13. Abkommen EU-USA über das Programm zum Aufspüren der Finanzierung des Terrorismus (TFTP-Abkommen)

Rechtsvorschriften

Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus

ABl. L 195 vom 27.7.2010, S. 5

Kernbestimmungen

Im Gefolge des 11. Septembers beschlossen die EU und die USA, eng zusammenzuarbeiten, und schlossen das Abkommen über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (EU-USA-TFTP-Abkommen). Entsprechend dem Abkommen stellt das US-Finanzministerium TFTP-Informationen auch Strafverfolgungsbehörden, Behörden der inneren Sicherheit oder Terrorismusbekämpfungsbehörden der betreffenden Mitgliedstaaten und gegebenenfalls Europol und Eurojust zur Verfügung.

Das TFTP verfügt über solide Kontrollmechanismen, mit denen sichergestellt werden soll, dass Schutzbestimmungen – auch in Bezug auf den Schutz personenbezogener Daten – eingehalten werden. Die Daten werden ausschließlich für die Zwecke der Verhütung, Aufklärung, Aufdeckung oder Verfolgung des Terrorismus und der Terrorismusfinanzierung verarbeitet. Für die Zwecke des Abkommens darf das US-Finanzministerium Zahlungsverkehrsdaten und damit zusammenhängende Daten, die im Gebiet der EU gespeichert sind, von bezeichneten Anbietern internationaler Zahlungsverkehrsdatendienste anfordern.

Der Nutzen der TFTP-Daten für die Mitgliedstaaten, Europol und Eurojust wird dadurch beschränkt, dass sich die TFTP-Analyse grenzüberschreitender Zahlungsvorgänge ausschließlich auf FIN-Nachrichten (Financial Institution Transfer/Übermittlung für Finanzinstitute), eine von der SWIFT entwickelte Nachrichtenart zur Übermittlung von Finanzinformationen zwischen Finanzinstituten, stützt. Andere Zahlungsmethoden werden nicht berücksichtigt. Das TFTP ist jedoch der einzige Mechanismus, der es ermöglicht, innerhalb sehr kurzer Zeit zur Verstärkung der inneren Sicherheit Transaktionen zu erfassen und deren Profil zu erstellen, bei denen der Verdacht besteht, dass sie mit Terrorismus oder Terrorismusfinanzierung in Zusammenhang stehen. Aufgrund einer stärkeren Sensibilisierung für die Gegenseitigkeitsklauseln dieses Abkommens wenden die EU-Behörden zunehmend diesen Mechanismus an, um aus dem Datenaustausch mit den USA Nutzen zu ziehen. Es sei in diesem Zusammenhang darauf hingewiesen, dass alle Suchanfragen von EU-Behörden im Rahmen des TFTP den Anforderungen des Artikels 10 des Abkommens entsprechen müssen.

Auch wenn das Abkommen nicht vorsieht, dass die Mitgliedstaaten über Europol um eine Abfrage einschlägiger Informationen, die über das TFTP erlangt wurden, ersuchen, wäre es sinnvoll, dass die Mitgliedstaaten Europol über ihre Direktersuchen nach Artikel 10 zumindest systematisch und frühzeitig unterrichten, um die Reaktion der EU auf den Terrorismus und seine Finanzierung zu verbessern. Um die Mitgliedstaaten bei der Bündelung ihrer TFTP-Suchanfragen zu unterstützen, hat Europol eine einzige Anlaufstelle (SPOC) eingerichtet, und aufgrund seiner Analysedatei-Umgebung und der gut funktionierenden Zusammenarbeit mit dem Schatzamt ist Europol in der Lage, die Anfragen der Mitgliedstaaten wirksam zu bearbeiten.

3.14. Austausch von Strafregisterinformationen (ECRIS)

Rechtsvorschriften

Rahmenbeschluss 2009/315/JI des Rates vom 26. Februar 2009 über die Durchführung und den Inhalt des Austauschs von Informationen aus dem Strafregister zwischen den Mitgliedstaaten, ABl. L 93 vom 7.4.2009, S. 23. Mit diesem Rahmenbeschluss wird der Beschluss 2005/876/JI des Rates vom 21. November 2005 über den Austausch von Informationen aus dem Strafregister (ABl. L 322 vom 9.12.2005, S. 33) aufgehoben.

Richtlinie (EU) 2019/884 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Änderung des Rahmenbeschlusses 2009/315/JI des Rates im Hinblick auf den Austausch von Informationen über Drittstaatsangehörige und auf das Europäische Strafregisterinformationssystem (ECRIS), sowie zur Ersetzung des Beschlusses 2009/316/JI des Rates, ABl. L 171 vom 7.6.2019 S. 143

Kernbestimmungen

Der Rahmenbeschluss 2009/315/JI des Rates verpflichtet einen Urteilsmitgliedstaat, alle in sein Strafregister eingetragenen Verurteilungen sowie alle etwa daran vorgenommenen Änderungen und Streichungen so rasch wie möglich dem bzw. den Herkunftsmitgliedstaat(en) der betreffenden Person zu übermitteln. Der Herkunftsmitgliedstaat ist verpflichtet, die Informationen für die Zwecke der Weiterübermittlung zu speichern. Jede Änderung oder Streichung im Urteilsmitgliedstaat hat eine identische Änderung oder Streichung im Strafregister des Herkunftsmitgliedstaats zur Folge. Um Informationen über Verurteilungen darf vom Herkunftsmitgliedstaat zum Zwecke eines Strafverfahrens oder zu andere Zwecken als einem Strafverfahren, wie der Vorbeugung einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit, ersucht werden. Allerdings kann die Verwendung der aufgrund dieses Beschlusses übermittelten Informationen zu anderen Zwecken als einem Strafverfahren nach Maßgabe des innerstaatlichen Rechts des ersuchten und des ersuchenden Mitgliedstaats beschränkt werden, um nicht die Chancen des Verurteilten auf soziale Wiedereingliederung zu behindern.

Der Beschluss 2009/316/JI des Rates legt die Modalitäten fest, nach denen ein Mitgliedstaat solche Informationen zu übermitteln hat. Der Ratsbeschluss gibt den Rahmen für ein computergestütztes System für den Austausch von Strafregisterinformationen vor. Die Zentralbehörden der Mitgliedstaaten verwenden die im Anhang zum Rahmenbeschluss enthaltenen speziellen Antrags- und Antwortformblätter für die elektronische Übermittlung entsprechend den Rechtsvorschriften.

3.14.1. Austausch von Strafregisterinformationen zu Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN)

Rechtsvorschriften

Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) 2018/1726, ABl. L 135 vom 22.5.2019, S. 1

Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates, ABl. L 135 vom 22.5.2019, S. 27

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

Richtlinie (EU) 2019/884 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Änderung des Rahmenbeschlusses 2009/315/JI des Rates im Hinblick auf den Austausch von Informationen über Drittstaatsangehörige und auf das Europäische Strafregisterinformationssystem (ECRIS), sowie zur Ersetzung des Beschlusses 2009/316/JI des Rates, ABl. L 151 vom 7.6.2019 S. 143

Kernbestimmungen

Die Verordnung gilt für die Verarbeitung von Identitätsangaben zu in Mitgliedstaaten verurteilten Drittstaatsangehörigen. Der Ausdruck "Drittstaatsangehöriger" bezeichnet eine Person, die kein Bürger der Union im Sinne des Artikels 20 Absatz 1 AEUV ist, oder eine staatenlose Person oder eine Person, deren Staatsangehörigkeit nicht bekannt ist. Strafregisterinformationen über diese Personen werden im Urteilsmitgliedstaat gespeichert. Mit dem ECRIS-TCN[95] soll festgestellt werden, welche anderen Mitgliedstaaten über solche Strafregisterinformationen verfügen. Auf den bestehenden ECRIS-Rahmen kann zurückgegriffen werden, um die betreffenden Mitgliedstaaten gemäß dem Rahmenbeschluss 2009/315/JI um solche Informationen zu ersuchen.

Die Verordnung sieht Vorschriften über die Einrichtung eines Systems vor, in dem personenbezogene Daten erfasst werden, das von eu-Lisa entwickelt und gewartet wird und das auf Unionsebene zentralisiert ist, und Vorschriften über die Aufteilung der Zuständigkeiten zwischen dem Mitgliedstaat und der Organisation, die für die Entwicklung und Wartung des zentralisierten Systems zuständig ist. Sie sorgt für einen insgesamt angemessenen Datenschutz, eine angemessene Datensicherheit und den Schutz der Grundrechte der betroffenen Personen.

---

95 Die Kommission bestimmt den Zeitpunkt, zu dem das ECRIS-TCN seinen Betrieb aufnimmt, nachdem die Voraussetzungen gemäß Artikel 35 der Verordnung (EU) 2019/816 erfüllt sind.

Eurojust, Europol und die EUStA sollten Zugang zum ECRIS-TCN haben, damit sie ermitteln können, in welchen Mitgliedstaaten Strafregisterinformationen zu einem Drittstaatsangehörigen vorliegen, und somit ihre gesetzlichen Aufgaben effizienter erfüllen können.

3.15. Vorratsspeicherung von Telekommunikationsdaten

Rechtsvorschriften

Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG[96]

Kernbestimmungen

Die Richtlinie gilt für die Anbieter elektronischer Kommunikationsdienste. In der Richtlinie heißt es, dass die Anbieter Verkehrs- und Standortdaten sowie die damit in Zusammenhang stehenden Daten, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind, auf Vorrat speichern sollten. Die Mitgliedstaaten verpflichten die Anbieter elektronischer Kommunikationsdienste oder Betreiber öffentlicher Kommunikationsnetze, zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten auf Vorrat die Kategorien von Daten zu speichern, die erforderlich sind zur Bestimmung

- der Quelle einer Nachricht,
- des Adressaten einer Nachricht,
- von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung,
- der Art einer Nachrichtenübermittlung,
- der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern und
- des Standorts mobiler Geräte.

Es dürfen keine Daten, die Aufschluss über den Inhalt einer Kommunikation geben, auf Vorrat gespeichert werden.

---

[96] Der Gerichtshof der Europäischen Union hat mit Urteil vom 8. April 2014 die Richtlinie für nichtig erklärt.

3.16. PNR (Fluggastdatensätze)-Richtlinie

Rechtsvorschriften

Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität

Kernbestimmungen

Mit der Richtlinie wird auf Unionsebene ein gemeinsamer Rechtsrahmen für die Übermittlung und Verarbeitung von PNR-Daten geschaffen und Folgendes geregelt:

a) die Übermittlung von Fluggastdatensätzen (PNR-Daten) zu Fluggästen von Drittstaatsflügen durch Fluggesellschaften[97]. Wenn ein Mitgliedstaat entscheidet, die Richtlinie auf EU-Flüge anzuwenden, so gelten alle Bestimmungen für EU-Flüge so, als handele es sich um Drittstaatsflüge.

b) die Verarbeitung von PNR-Daten, unter anderem ihre Erhebung, Verwendung und Speicherung durch die Mitgliedstaaten, sowie der Austausch dieser Daten zwischen den Mitgliedstaaten.

Für die Zwecke der Verarbeitung von PNR-Daten errichtet oder benennt jeder Mitgliedstaat eine zuständige Behörde, die als seine PNR-Zentralstelle handelt. Zwei oder mehr Mitgliedstaaten können gemeinsam eine einzige Behörde errichten oder benennen, die als ihre gemeinsame PNR-Zentralstelle handelt.

Die in Anhang I der Richtlinie aufgeführten PNR-Daten sind an die PNR-Zentralstellen zu übermitteln, soweit die Fluggesellschaften solche Daten im Rahmen ihrer normalen Geschäftstätigkeit bereits erhoben haben. Einige Fluggesellschaften bewahren vorab übermittelte Fluggastdaten (API-Daten) als Teil der PNR-Daten auf, während andere dies nicht tun. Unabhängig von der Art und Weise, wie die Fluggesellschaften API-Daten erheben, müssen sie diese an die PNR-Zentralstellen übermitteln, die sie auf die gleiche Weise wie PNR-Daten verarbeiten. Anhang II der Richtlinie enthält die Liste der schwerwiegenden Straftaten, die in den Anwendungsbereich der Richtlinie fallen.

---

97 Die Richtlinie hindert die Mitgliedstaaten nicht daran, nach ihrem jeweiligen nationalen Recht eine Regelung zur Erhebung und Verarbeitung von PNR-Daten durch Wirtschaftsteilnehmer, die keine Beförderungsunternehmen sind, wie etwa Reisebüros oder Reiseveranstalter, die Dienstleistungen im Zusammenhang mit Reisen – einschließlich Flugbuchungen – erbringen, für die sie PNR-Daten erheben und verarbeiten, oder durch andere als in der Richtlinie angegebene Beförderungsunternehmen vorzusehen, sofern dieses nationale Recht mit dem Unionsrecht in Einklang steht.

Die Verarbeitung von PNR-Daten dient der Überprüfung von Fluggästen vor ihrer Ankunft in einem Mitgliedstaat oder vor ihrem Abflug von einem Mitgliedstaat, um diejenigen Personen zu ermitteln, die von den für die Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität zuständigen nationalen Behörden und gegebenenfalls von Europol im Rahmen seiner Zuständigkeiten und zur Ausübung seiner Aufgaben genauer überprüft werden müssen.

Zur Durchführung der Überprüfung dürfen die PNR-Zentralstellen

a) die PNR-Daten mit Datenbanken, die zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität maßgeblich sind, einschließlich Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind, unter Einhaltung der für solche Datenbanken einschlägigen nationalen, internationalen und Unionsvorschriften abgleichen; oder

b) die PNR-Daten anhand von im Voraus festgelegten Kriterien verarbeiten.

Auf nationaler Ebene übermitteln die PNR-Zentralstellen PNR-Daten oder die Ergebnisse der Verarbeitung dieser Daten den zuständigen nationalen Strafverfolgungsbehörden, die berechtigt sind, das Dossier zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität einer weiteren Prüfung zu unterziehen oder geeignete Maßnahmen zu treffen. Die PNR-Zentralstellen sind zwar der wichtigste Kanal für den grenzüberschreitenden Informationsaustausch, die zuständigen Behörden können sich im Notfall und unter genau festgelegten Bedingungen aber auch direkt an eine PNR-Zentralstelle eines anderen Mitgliedstaats wenden.

Auf Ebene der Union tauschen die PNR-Zentralstellen sowohl bei den Fluggesellschaften erhobene PNR-Daten als auch die Ergebnisse der Verarbeitung dieser Daten untereinander und mit Europol aus, das berechtigt ist, im Rahmen seiner Zuständigkeiten und zur Ausübung seiner Aufgaben solche Daten von den PNR-Zentralstellen anzufordern.

Die PNR-Daten müssen für einen Zeitraum von fünf Jahren ab ihrer Übermittlung von der PNR-Zentralstelle des Mitgliedstaats, in dessen Hoheitsgebiet der Flug angekommen beziehungsweise von dem er abgegangen ist, in einer bei dieser PNR-Zentralstelle angesiedelten Datenbank aufbewahrt werden. Nach Ablauf einer Frist von sechs Monaten werden jedoch alle PNR-Daten depersonalisiert, indem alle Datenelemente, mit denen die Identität des Fluggasts, auf den sich die Daten beziehen, unmittelbar festgestellt werden könnte, unkenntlich gemacht werden. Die Richtlinie enthält eine Liste der PNR-Daten, die unkenntlich zu machen sind. Nach fünf Jahren sind die PNR-Daten zu löschen, es sei denn, sie wurden zum Zwecke der Verhütung, Aufdeckung, Ermittlung oder Verfolgung terroristischer Straftaten oder schwerer Kriminalität an eine zuständige Behörde übermittelt; in diesem Fall richtet sich die Frist für ihre Speicherung nach nationalem Recht.

Gemäß den Rechtsvorschriften der Union auf dem Gebiet des Datenschutzes verbietet die PNR-Richtlinie die Verarbeitung sensibler Daten betreffend Rasse oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, eine Gewerkschaftszugehörigkeit, den Gesundheitszustand, das Sexualleben oder die sexuelle Orientierung.

3.17. Vorab übermittelte Fluggastdaten (API-Daten)

Rechtsvorschriften

Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln

Kernbestimmungen

Zweck dieser Richtlinie ist es, die Grenzkontrollen zu verbessern und die illegale Einwanderung zu bekämpfen. Dazu müssen die Mitgliedstaaten die Fluggesellschaften gemäß der Richtlinie dazu verpflichten, bestimmte Informationen über ihre Fluggäste vor ihrer Einreise in die Europäische Union zu übermitteln. Diese Informationen werden vorab übermittelte Fluggastdaten (API-Daten) genannt. Unter bestimmten Bedingungen und Umständen können die Mitgliedstaaten API-Daten auch zu Strafverfolgungszwecken verwenden.

Die Informationen werden auf Ersuchen der Behörden bereitgestellt, die für die Durchführung der Personenkontrollen an den Außengrenzen der EU zuständig sind.

Die Fluggesellschaften übermitteln die API-Daten auf elektronischem oder, sollte die Übertragung nicht gelingen, auf jedem anderen geeigneten Weg an die Behörden, die mit der Durchführung der Grenzkontrollen an der Grenzübergangsstelle beauftragt sind, über die der Fluggast in die EU einreisen wird. Die API-Daten werden mit nationalen und europäischen Datenbanken wie dem Schengener Informationssystem (SIS) und dem Visa-Informationssystem (VIS) abgeglichen.

Stimmen die API-Daten mit einem Eintrag in einer Datenbank überein, erhält die Grenzpolizei eine Ausschreibung und der betreffende Fluggast wird bei Ankunft einer Kontrolle unterzogen.

Die erhobenen und übermittelten API-Daten müssen von den Fluggesellschaften und den Behörden binnen 24 Stunden nach Übermittlung bzw. nach Ankunft gelöscht werden. Die Grenzbehörden können die vorläufigen Dateien jedoch länger als 24 Stunden aufbewahren, wenn die Daten später zur Wahrnehmung der gesetzlichen Aufgaben durch die Grenzbehörden oder zur Durchsetzung von Rechtsvorschriften und Regelungen im Bereich der Einreise und der Einwanderung einschließlich der darin enthaltenen Bestimmungen zum Schutz der öffentlichen Ordnung und der nationalen Sicherheit benötigt werden.

3.18. Straßenverkehrsgefährdende Verkehrsdelikte

Rechtsvorschriften

Richtlinie (EU) 2015/413 des Europäischen Parlaments und des Rates vom 11. März 2015 zur Erleichterung des grenzüberschreitenden Austauschs von Informationen über die Straßenverkehrssicherheit gefährdende Verkehrsdelikte, ABl. L 68 vom 13.3.2015, S. 9

Kernbestimmungen

Die Mitgliedstaaten gewähren einander den Online-Zugang zu ihren nationalen Fahrzeugregisterdaten (VRD) im Hinblick auf die Durchsetzung von Sanktionen für die Straßenverkehrssicherheit gefährdende Verkehrsdelikte, wenn die Delikte mit einem in einem anderen Mitgliedstaat als dem Deliktsmitgliedstaat zugelassenen Fahrzeug begangen wurden. Der Deliktsmitgliedstaat verwendet die erhaltenen Daten, um die Person festzustellen, die persönlich für das Verkehrsdelikt haftbar ist. Der Informationsaustausch erstreckt sich auf folgende Delikte:

- Geschwindigkeitsübertretung,
- Nichtanlegen des Sicherheitsgurts,
- Überfahren eines roten Lichtzeichens,
- Trunkenheit im Straßenverkehr,
- Fahren unter Drogeneinfluss,
- Nichttragen eines Schutzhelms,
- unbefugte Benutzung eines Fahrstreifens,
- rechtswidrige Benutzung eines Mobiltelefons oder anderer Kommunikationsgeräte beim Fahren.

Anhand der speziellen Softwareanwendung EUCARIS gestatten die Mitgliedstaaten ihren benannten nationalen Kontaktstellen (NCP) den gegenseitigen Zugriff auf ihre nationalen Fahrzeugregisterdaten (VRD), wobei zu folgenden Daten eine automatisierte Suche erfolgen kann:

a) Daten zum Fahrzeug und

b) Daten zum Eigentümer oder Halter des Fahrzeugs.

3.19. Einreise-/Ausreisesystem (EES)

Rechtsvorschriften

Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten der Europäischen Union und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011, ABl. L 327 vom 9.12.2017, S. 20

Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates, ABl. L 135 vom 22.5.2019, S. 27

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

Die Verordnung stellt eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands dar.

Dänemark hat mitgeteilt, dass es nach Artikel 4 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 22 über die Position Dänemarks beschlossen hat, die oben aufgeführten Verordnungen in dänisches Recht umzusetzen. Dieser Beschluss begründet eine Verpflichtung nach dem Völkerrecht zwischen Dänemark und den übrigen Mitgliedstaaten, für die die Maßnahme bindend ist.

Das Vereinigte Königreich und Irland beteiligen sich nicht am Schengen-Besitzstand und sind daher weder durch die Verordnung gebunden noch zu ihrer Anwendung verpflichtet.

Island, Norwegen, Liechtenstein und die Schweiz sind durch den Besitzstand im Sinne der jeweiligen Übereinkünfte bzw. Protokolle betreffend den Schengen-Besitzstand gebunden.

Für Zypern, Bulgarien, Rumänien und Kroatien stellen die Bestimmungen der Verordnung über das SIS und das VIS auf dem Schengen-Besitzstand aufbauende oder anderweitig damit zusammenhängende Bestimmungen im Sinne der jeweiligen Beitrittsakte dar.

Kernbestimmungen

In der Verordnung[98] werden die Ziele des EES, die Kategorien der in das EES einzugebenden Daten, die Verwendungszwecke der Daten, die Eingabekriterien, die zum Zugang zu den Daten berechtigten Behörden, weitere Regelungen zur Datenverarbeitung und zum Schutz personenbezogener Daten sowie die technische Architektur des EES, Vorschriften für seinen Betrieb und seine Anwendung, und die Interoperabilität mit anderen Informationssystemen präzisiert bzw. festgelegt. Mit dem EES soll das Außengrenzenmanagement verbessert, die irreguläre Einwanderung verhindert und die Steuerung der Migrationsströme erleichtert werden. Zu diesem Zweck ist das EES in der Lage, den Zeitpunkt und den Ort der Ein- und der Ausreise bestimmter Drittstaatsangehöriger, die die Grenzen der Mitgliedstaaten, an denen das EES eingesetzt wird, überschreiten, zu erfassen und zu speichern. Zudem sind die nationalen Strafverfolgungsbehörden zur Abfrage des EES berechtigt, um terroristische und sonstige schwerwiegende Straftaten zu verhüten, aufzudecken und zu ermitteln[99].

Das EES besteht aus einem Zentralsystem (Zentralsystem des EES), mit dem eine computergestützte zentrale Datenbank für biometrische und alphanumerische Daten betrieben wird, und einer einheitlichen nationalen Schnittstelle in jedem Mitgliedstaat. Dabei verbindet ein sicherer Kommunikationskanal das Zentralsystem des EES mit dem Zentralsystem des Visa-Informationssystems (Zentralsystem des VIS) und eine sichere und verschlüsselte Kommunikationsinfrastruktur das Zentralsystem des EES mit den einheitlichen nationalen Schnittstellen. Die Interoperabilität zwischen dem EES und dem VIS wird durch einen direkten Kommunikationskanal zwischen ihren Zentralsystemen hergestellt, damit die Grenzbehörden mithilfe des EES eine VIS-Abfrage und die Visumbehörden mithilfe des VIS eine EES-Abfrage durchführen können.

---

98 Die Kommission bestimmt den Zeitpunkt, zu dem das EES seinen Betrieb aufnimmt, nachdem die Voraussetzungen nach Artikel 66 der Verordnung (EU) Nr. 2017/2226 erfüllt sind

99 Der Ausdruck "terroristische Straftat" bezeichnet eine Straftat, die den in der Richtlinie (EU) 2017/541 aufgeführten Straftaten entspricht oder gleichwertig ist; der Ausdruck "schwere Straftat" bezeichnet eine Straftat, die den in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI über den Europäischen Haftbefehl aufgeführten Straftaten entspricht oder diesen gleichwertig ist, wenn die Straftat nach dem nationalen Recht mit einer freiheitsentziehenden Strafe oder Sicherungsmaßnahme für eine Höchstdauer von mindestens drei Jahren geahndet werden kann.

Die Verordnung enthält strenge Vorschriften für den Zugang zum EES. Außerdem wird darin festgelegt, dass Einzelpersonen das Recht auf Auskunft, Berichtigung, Vervollständigung, Löschung und Regress haben, insbesondere das Recht, bei Gericht einen Rechtsbehelf einzulegen, und dass die Datenverarbeitung von unabhängigen Behörden überwacht wird.

Die Verordnung steht im Einklang mit den Grundrechten und Grundsätzen, die mit der Charta der Grundrechte der Europäischen Union anerkannt wurden. Unbeschadet spezifischerer Vorschriften in der Verordnung für die Verarbeitung personenbezogener Daten findet die Verordnung (EU) 2016/679[100] (Datenschutz-Grundverordnung) Anwendung auf die nach Maßgabe dieser Verordnung durchgeführte Verarbeitung personenbezogener Daten, es sei denn, diese Verarbeitung erfolgt durch die benannten Strafverfolgungsbehörden oder zentralen Zugangsstellen der Mitgliedstaaten, wobei in diesen Fällen die Richtlinie (EU) 2016/680[101] (Polizei-Richtlinie) Anwendung findet.

3.20. Europäisches Reiseinformations- und -genehmigungssystem (ETIAS)

Rechtsvorschriften

Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399 (EU) 2016/1624 und (EU) 2017/2226, ABl. L 236 vom 19.9.2018, S. 1

Verordnung (EU) 2018/1241 des Europäischen Parlaments und des Rates vom 12. September 2018 zur Änderung der Verordnung (EU) 2016/794 für die Zwecke der Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS), ABl. L 236 vom 19.9.2018, S. 72

---

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

101 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2019 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.

In der Verordnung 2018/1240[102] sind die Ziele des ETIAS und seine System- und Organisationsarchitektur sowie Bestimmungen über den Systembetrieb und die Verwendung der vom Antragsteller in das System einzugebenden Daten, über die Erteilung oder Verweigerung einer Reisegenehmigung und die Datenverarbeitungszwecke festgelegt und die Behörden benannt, die berechtigt sind, auf die Daten zuzugreifen und den Schutz personenbezogener Daten sicherzustellen.

Die Verordnung stellt eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands dar. Das Vereinigte Königreich und Irland beteiligen sich nicht am Schengen-Besitzstand und sind daher weder durch die Verordnung gebunden noch zu ihrer Anwendung verpflichtet. Island, Norwegen, Liechtenstein und die Schweiz sind durch den Besitzstand im Sinne der jeweiligen Übereinkünfte bzw. Protokolle betreffend den Schengen-Besitzstand gebunden.

Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates, ABl. L 135 vom 22.5.2019, S. 27

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

Kernbestimmungen

ETIAS stellt eine Reisegenehmigung bereit, die sich von Natur aus von einem Visa unterscheidet, jedoch eine Voraussetzung für die Einreise und den Aufenthalt in den Schengen-Raum darstellt und anzeigt, dass mit dem Antragsteller für eine Reisegenehmigung kein Risiko für die Sicherheit, kein Risiko der illegalen Einwanderung und kein hohes Epidemierisiko verbunden ist.

ETIAS besteht aus

- einem IT-Großsystem, d. h. dem ETIAS-Informationssystem, das von eu-LISA konzipiert, entwickelt und technisch verwaltet wird,

---

102 Die Kommission bestimmt den Zeitpunkt, zu dem das ETIAS seinen Betrieb aufnimmt, nachdem die Voraussetzungen gemäß Artikel 88 der Verordnung (EU) 2018/1240 erfüllt sind.

- der ETIAS-Zentralstelle, die zur Europäischen Agentur für die Grenz- und Küstenwache gehört,

- den nationalen ETIAS-Stellen, die für die Prüfung der Anträge zuständig sind und über die Erteilung, Verweigerung, Annullierung oder Aufhebung von Reisegenehmigungen entscheiden. Bei der Beurteilung der Anträge sollten die nationalen ETIAS-Stellen miteinander und mit Europol kooperieren.

Der Zugriff auf personenbezogene Daten im ETIAS sollte ausdrücklich dazu ermächtigtem Personal vorbehalten sein und unter keinen Umständen dazu genutzt werden, um Entscheidungen auf der Grundlage einer Form von Diskriminierung zu treffen. Was die von den Mitgliedstaaten benannten Strafverfolgungsbehörden anbelangt, sollten im ETIAS-Zentralsystem gespeicherte personenbezogene Daten nur in bestimmten Fällen und nur dann verarbeitet werden, wenn dies zur Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten erforderlich ist. Die benannten Behörden und Europol sollten den Zugang zum ETIAS nur beantragen, wenn sie hinreichende Gründe zu der Annahme haben, dass dieser Zugang Informationen erbringt, die einen Beitrag zur Verhütung, Aufdeckung oder Untersuchung einer terroristischen oder sonstigen schweren Straftat leisten.

Die Verordnung steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden. Im Zusammenhang mit der Verarbeitung personenbezogener Daten gibt es geeignete Garantien, mit denen der Eingriff in das Recht auf Schutz des Privatlebens und in das Recht auf Schutz personenbezogener Daten auf das in einer demokratischen Gesellschaft notwendige und als verhältnismäßig geltende Maß beschränkt werden soll.

Die Verordnung (EU) 2016/679[103] (Datenschutz-Grundverordnung) findet Anwendung auf die nach Maßgabe dieser Verordnung durchgeführte Verarbeitung personenbezogener Daten, es sei denn, diese Verarbeitung erfolgt durch die benannten Strafverfolgungsbehörden oder zentralen Zugangsstellen der Mitgliedstaaten, wobei in diesen Fällen die Richtlinie (EU) 2016/680[104] (Polizei-Richtlinie) gilt.

---

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

104 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2019 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.

3.21. Rechtsvorschriften zur Interoperabilität

Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates, ABl. L 135 vom 22.5.2019, S. 27

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

Kernbestimmungen

Die Verordnung (EU) 2019/817 und die Verordnung (EU) 2019/818 bilden das "Interoperabilitätspaket" und legen den Schwerpunkt auf personenbezogene Daten, die in auf EU-Ebene zentralisierten Informationssystemen gespeichert werden. Mit den beiden Verordnungen soll die Datenverwaltungsarchitektur der Union im Bereich des Grenzmanagements und der Sicherheit verbessert werden. Der Rahmen des "Interoperabilitätspakets" gilt daher sowohl in den Bereichen Grenzen und Visa als auch in den Bereichen polizeiliche und justizielle Zusammenarbeit sowie Asyl und Migration. Die zugrundeliegenden Informationssysteme sollten so miteinander verbunden werden, dass sie einander ergänzen, um ihre jeweiligen Zwecke besser erfüllen zu können.

Dies Verordnungen regeln ferner die Verfahren und Bedingungen für den Zugang der benannten Behörden und von Europol zum EES, zum VIS, zum ETIAS und zu Eurodac zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer und sonstiger schwerer Straftaten.

Die technischen Interoperabilitätskomponenten erstrecken sich auf EES (siehe Nr. 3.19), VIS (siehe Nr. 3.8), ETIAS (siehe Nr. 3.20), Eurodac (siehe Nr. 3.9), SIS (siehe Nr. 3.2) und ECRIS-TCN (siehe Nr. 3.14.1). Die Interoperabilitätskomponenten[105] umfassen

- das Europäische Suchportal (ESP), bei dem es sich um eine einzige Schnittstelle ("Fenster") handelt, die eine parallel erfolgende Abfrage der oben aufgeführten EU-Instrumente, der Europol-Daten und der Interpol-Datenbanken ermöglicht. Die Datenabfragen sind beschränkt sich auf Daten, die sich auf Personen oder Reisedokumente beziehen;

[105] Die Kommission wird den Zeitpunkt bestimmen, ab dem die Vorschriften der Verordnungen über das ESP, den gemeinsamen Dienst BMS, den CIR und den MID Anwendung finden.

- den gemeinsamen Dienst für den Abgleich biometrischer Daten(BMS), dessen Hauptzweck darin besteht, die Identifizierung einer in mehreren Datenbanken erfassten Person unter Rückgriff auf eine einzige technologische Komponente anhand eines systemübergreifenden Abgleichs ihrer biometrischen Daten zu ermöglichen. Die AFIS-Templates sollten im BMS an einem einzigen Ort zusammengefasst und gespeichert werden;

- einen gemeinsamen Speicher für Identitätsdaten (CIR), bei dem es sich um eine gemeinsame Speichereinheit für Identitätsdaten, Reisedokumente und biometrische Daten von im EES, im VIS, im ETIAS, in Eurodac und im ECRIS-TCN erfassten Personen handelt. Diese Daten können sich auf unterschiedliche oder unvollständige Identitäten ein und derselben Person beziehen. Eine genauere Identifizierung sollte durch den automatischen Ver- und Abgleich solcher Daten erreicht werden. Der CIR ermöglicht Identitätsprüfungen durch benannte Strafverfolgungsbehörden und unterstützt dadurch ihr Vorgehen bei der Identifizierung einer Person;

- einen Detektor für Mehrfachidentitäten (MID), der das Funktionieren des CIR unterstützt.

Die in den Verordnungen vorgesehenen neuen Datenverarbeitungsverfahren bedeuten einen Eingriff in die nach den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union geschützten Grundrechte. Da die EU-Informationssysteme nur im Falle einer korrekten Identifizierung der betroffenen Person wirksam genutzt werden können, steht ein solcher Eingriff im Einklang mit den Zielen, zu deren Erreichung die einzelnen EU-Informationssysteme errichtet wurden (wirksames Management der Unionsgrenzen, Wahrung der inneren Sicherheit der Union und wirksame Umsetzung der Asyl- und der Visapolitik der Union).

Die Verordnung (EU) 2016/679 findet auf die Verarbeitung personenbezogener Daten zum Zwecke der Interoperabilität Anwendung, sofern diese Verarbeitung nicht durch benannte Strafverfolgungsbehörden oder zentrale Anlaufstellen der Mitgliedstaaten zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten erfolgt. In diesem Fall findet die Verordnung (EU) 2016/680 (siehe Nummer 3.0) Anwendung.

Die Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 oder der Richtlinie (EU) 2016/680 sollten die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten überwachen. Der Europäische Datenschutzbeauftragte sollte die Tätigkeiten der Organe und Einrichtungen der Union bei der Verarbeitung personenbezogener Daten überwachen.