Rat der
Europäischen Union

Brüssel, den 7. März 2016
(OR. en)

6704/16

LIMITE

JAI 177
DAPIX 29
ENFOPOL 53
COMIX 173
ENFOCUSTOM 31
CRIMORG 11
SCHENGEN 5
VISA 54
SIRIS 32
COPEN 65
ASIM 21
FRONT 105

VERMERK

Absender:	Vorsitz
Empfänger:	Gruppe "Informationsaustausch und Datenschutz" (DAPIX)
Nr. Vordok.:	ST 7779/1/15 REV 1
Betr.:	Leitfaden für den Austausch von strafverfolgungsrelevanten Informationen

FÜR DIE ÖFFENTLICHKEIT TEILWEISE ZUGÄNGLICHES DOKUMENT (15.09.2016)

1. Einleitung

Mit dem Leitfaden für den Austausch von strafverfolgungsrelevanten Informationen soll das Handbuch für grenzüberschreitende Einsätze (Dokument 10505/4/09 REV4 ENFOPOL 157 ENFOCUSTOM 55 CRIMORG 90 COMIX 465) 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.

Es wurde vereinbart, den Leitfaden zweimal jährlich zu aktualisieren und dabei gegebenenfalls neue Rechtsvorschriften, Erfahrungen aus der Praxis oder geänderte Kontaktangaben der betreffenden Behörden zu berücksichtigen. Die vorliegende Fassung ist die erste Fassung im Jahr 2016; die Änderungen betreffen im Wesentlichen die Kontaktangaben in den nationalen Merkblättern.

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.

Schließlich wird der Leitfaden durch **nationale Merkblätter** ergänzt, die die für den grenzüberschreitenden Austausch zur Verfügung stehenden 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.

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" (Dokument 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 Handbuchs 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.

Schließlich wird der Leitfaden durch eine Sammlung **nationaler Merkblätter** zu den einzelnen Mitgliedstaaten mit **praktischen Angaben zu den** für den grenzübergreifenden Informationsaustausch zuständigen **Anlaufstellen** ergänzt.

4. Überblick und Ausblick

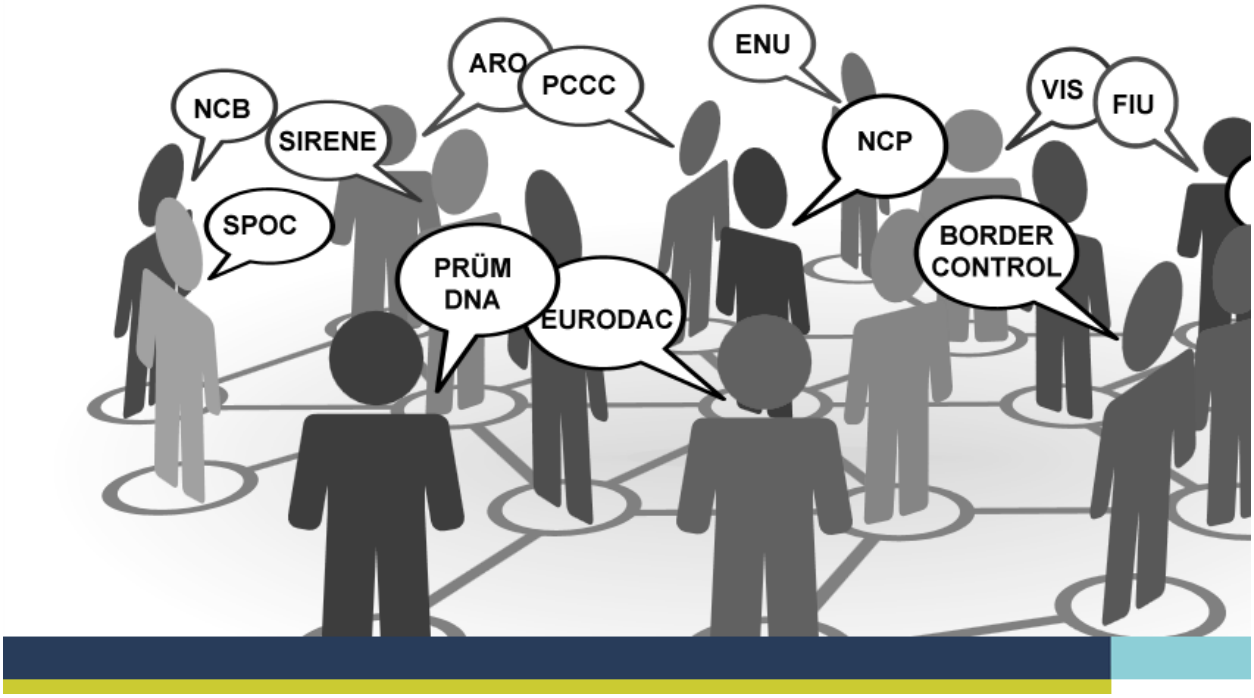
Die Ausarbeitung des vorgeschlagenen Leitfadens war als Maßnahme im dritten Maßnahmenkatalog der Strategie für das Informationsmanagement (IMS) enthalten; die aktuelle Fassung des Handbuchs wurde unter irischem, zyprischem, griechischem, italienischem und lettischem Vorsitz erstellt.

Unter irischem Vorsitz wurde 2013 eine Untergruppe aus den in der DAPIX-Gruppe vertretenen Delegationen eingesetzt, um auf der Grundlage der Reaktionen der Mitgliedstaaten – insbesondere bei dem im März 2013 in Budapest abgehaltenen Infopolex-Seminar – mit der Ausarbeitung zu beginnen.

Der Vorsitz unterbreitet den Delegationen den Leitfadenentwurf und ersucht sie, diesen Entwurf zu billigen.

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

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 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 in drei Teile:

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.

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 straf-verfolgungsrelevanten 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" **–** enthält die nationalen Merkblätter mit ausführlichen Angaben zu den Anlaufstellen für alle in diesem Dokument angesprochenen Aspekte des grenzüber-schreitenden 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 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 **S**upplementary **I**nformation **R**equest 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 Durchführungs-bestimmungen für das Schengener Informations-system der zweiten Generation (SIS II) (Bekanntgegeben unter Aktenzeichen C(2015) 326).

Europol/ Europol-Informationssystem (EIS) – EIS-Indexsystem Arbeitsdateien zu Analysezwecken (AWF) – AWF	Nationale Europol-Stellen (ENU)	Beschluss 2009/371/JI des Rates ABl. L 121 vom 15.5.2009, S. 37 Beschluss 2009/936/JI des Rates ABl. L 325 vom 11.12.2009, S. 14 Beschluss 2009/968/JI des Rates vom 30. November 2009 zur Annahme der Vertraulichkeitsregeln für Europol-Informationen ABl. L 332 vom 17.12.2009, S. 17	
Interpol/I-24/7	NCB (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, 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-Identifizierungs-systems (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	
Visa-Informationssystem (VIS)	Zentrale nationale Zugangsstellen	Entscheidung 2004/512/EG des Rates ABl. L 213 vom 15.6.2004, S. 5 Beschluss 2008/633/JI des Rates ABl. L 218 vom 13.8.2008, S. 126 Erklärungen betreffend die benannten Behörden der Mitgliedstaaten und die benannte(n) zentrale(n) Zugangsstelle(n), die für Datenabfragen Zugang zum Visa-Informationssystem hat/haben im Sinne von Artikel 3 Absatz 2 und Artikel 3 Absatz 3 des Beschlusses 2008/633/JI des Rates (ABl. C 236 vom 14.8.2013, S. 1)	

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	Beschluss 2009/316/JI des Rates ABl. L 93 vom 7.4.2009, S. 33	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)	Beschluss 2000/642/JI des Rates vom 17. Oktober 2000 über Vereinbarungen für eine Zusammenarbeit zwischen den zentralen Meldestellen der Mitgliedstaaten beim Austausch von Informationen ABl. L 271 vom 24.1.2000, S. 4.	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 **S**upplementary **I**nformation **R**equest 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) – AWF	Nationale Europol-Stellen (ENU)	Beschluss 2009/371/JI des Rates ABl. L 121 vom 15.5.2009, S. 37 Beschluss 2009/936/JI des Rates ABl. L 325 vom 11.12.2009, S. 14	

		Beschluss 2009/968/JI des Rates vom 30. November 2009 zur Annahme der Vertraulichkeitsregeln für Europol-Informationen ABl. L 332 vom 17.12.2009, S. 17	
Interpol/I-24/7	NCB (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-Identifizierungs-systems (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")	

Fahrzeugzulassungsdaten (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	
Visa-Informationssystem (VIS)	Zentrale nationale Zugangsstelle	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 Erklärungen betreffend die benannten Behörden der Mitgliedstaaten und die benannte(n) zentrale(n) Zugangsstelle(n), die für Datenabfragen Zugang zum Visa-Informationssystem hat/haben im Sinne von Artikel 3 Absatz 2 und Artikel 3 Absatz 3 des Beschlusses 2008/633/JI des Rates ABl. C 236 vom 14.8.2013, S. 1	

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	Beschluss 2009/316/JI des Rates ABl. L 93 vom 7.4.2009, S. 33	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	
FIU.NET	Zentrale Meldestellen für Geldwäsche-Verdachtsanzeigen (FIU)	Beschluss 2000/642/JI des Rates vom 17. Oktober 2000 über Vereinbarungen für eine Zusammenarbeit zwischen den zentralen Meldestellen der Mitgliedstaaten beim Austausch von Informationen ABl. L 271 vom 24.1.2000, S. 4	

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 4. Dezember 2006 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 (2006/C 322/01) ABl. C 322 vom 29.12.2006, 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 10478/13 ENFOPOL 173

Zentren der Polizei- und Zollzusammenarbeit	PCCC	Bilaterale Vereinbarungen	

TEIL II - ALLGEMEINE INFORMATIONEN

1. KONTAKTKANÄLE[1]

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 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 und dass
- 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, und dass,
- 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").

[1] Nationale Stellen, die mit dem Austausch von strafverfolgungsrelevanten Informationen befasst sind

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)[2] 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[3] 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.

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;

---

[2] Schlussfolgerungen des Rates im Anschluss an die Mitteilung der Kommission über das Europäische Modell für den Informationsaustausch (EIXM) (811/13 JAI 400 DAPIX 82 CRIMORG 76 ENFOCUSTOM 88 ENFOPOL 146), am 6. Juni 2013 angenommen.

[3] 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), am 6. Juni 2014 vom Rat angenommen.

- 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.CO.Pol),

Plattform für den Informationsaustausch

Die Zentralstelle für operative Polizeizusammenarbeit (S.C.CO.Pol) ist eine ***ministerien-übergreifende*** *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.CO.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

In allen Mitgliedstaaten sind als Teil des Schengen-Besitzstands ständige SIRENE-Büros als benannte Behörden eingerichtet[4] (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. Diese Büros tauschen rund um die Uhr Daten in Bezug auf SIS-II-Ausschreibungen aus[5], 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 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.

Der Austausch von Zusatzinformationen erfolgt im Einklang mit den Bestimmungen des SIRENE-Handbuchs[6] über die Kommunikationsinfrastruktur[7].

---

4 Siehe Schengener Durchführungsübereinkommen (ABl. L 239 vom 22.9.2000).

5 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).

6 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).

7 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.

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.

Europol[8] 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. Im Ratsbeschluss zur Errichtung von Europol 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 (NCB)

Die **Nationalen Zentralbüros (NCB)** 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;

[8] Beschluss 2009/371/JI des Rates vom 6. national police headquartersApril 2009 zur Errichtung des Europäischen Polizeiamts (Europol) (ABl. L 121 vom 15.5.2009, S. 37). Über eine neue Rechtsgrundlage für Europol wird derzeit verhandelt.

- direkte Abfrage dieser Datenbanken;

- Nutzung der Interpol-Ausschreibungen und -Rundschreiben für die Übermittlung von Kooperationsersuchen und internationalen Ausschreibungen.

Die NCB können Daten rasch abfragen und abgleichen gestohlene Reisedokumente, gestohlene Kraftfahrzeuge, gestohlene Kunstwerke usw. enthalten.

So weit wie möglichen sollten die Nationalen Zentral, 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 büros den an der internationalen Polizeizusammenarbeit beteiligten Strafverfolgungsbehörden ihrer Länder den Zugang zum Informationssystem von Interpol ermöglichen. Die NCB 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[9] 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[10]. 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.

---

[9] 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).

[10] 5010/15 JAI 1 DAPIX 1 ENFOPOL 1 CRIMORG 1.

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.

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, 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 Mitgliedtaaten 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 der eine 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[11]

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)[12]

Über die nationale Prüm-Kontaktstelle für Großveranstaltungen hinaus und mit besonderer Berücksichtigung internationaler Fußballspiele ist in jedem Mitgliedstaat eine nationale Fußball-informationsstelle (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.

---

[11] 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).

[12] 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[13] im Anhang des Fußballhandbuchs erfolgen.

1.6.1. Fußballhandbuch[14]

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-NCB, nationale Europol-Stellen, SIRENE-Büros).

---

13 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).

14 Entschließung des Rates vom 4. Dezember 2006 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 (2006/C 322/01) (ABl. C 322 vom 29.12.2006, 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.

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-Einheit 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, selbständig 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[15], 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.

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.*

[15] "Update of the Compendium on law enforcement liaison officers (2014)" (Dok. 11996/14 ENFOPOL 221 JAIEX 55 COMIX 384).

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[16].

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[17] 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.

Die Bestimmungen 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[18] werden die Wirksamkeit der Zusammenarbeit zwischen den Vermögensabschöpfungsstellen innerhalb der Europäischen Union weiter verbessern. Die Mitgliedstaaten sind aufgefordert, die Richtlinie bis zum 4. Oktober 2016 umzusetzen.

---

16 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).

17 Beschluss 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.

18 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)[19]

Einschlägige Informationen über alle Tatsachen, die ein Indiz für Geldwäsche sein könnten, sollten von den nationalen zentralen Meldestellen (FIU) gesammelt, analysiert und untersucht werden. Die zentralen Meldestellen analysieren Finanztransaktionen auf Einzelfallgrundlage im Anschluss an Meldungen über verdächtige Transaktionen.

Die zentralen Meldestellen dienen 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.

Die Mitgliedstaaten sollten jedoch möglichst sicherstellen, dass die zentralen Meldestellen genutzt werden, um alle verfügbaren Informationen über Geldwäsche und die daran beteiligten natürlichen oder juristischen Personen auszutauschen.

---

[19] Siehe Beschluss 2000/642/JI des Rates vom 17. Oktober 2000 über Vereinbarungen für eine Zusammenarbeit zwischen den zentralen Meldestellen der Mitgliedstaaten beim Austausch von Informationen (ABl. L 271 vom 24.1.2000, S. 4).

Bei den Ersuchen der Mitgliedstaaten um über die zentralen Meldestellen auszutauschende Informationen gilt eine Reihe von Vorschriften über die Verwendung von Informationen der zentralen Meldestellen.

Alle 28 zentralen Meldestellen sind an das Netz FIU.NET angeschlossen, bei dem es sich um ein dezentrales Computernetz für den Austausch von Informationen zwischen zentralen Meldestellen handelt. 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[20]

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 natürlichen Person, die identifiziert wurde oder identifiziert werden kann.

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.

---

[20] 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. Wahl des Kommunikationskanals – allgemein verwendete Kriterien

In einem Mitgliedstaat erfüllt eine einzige Anlaufstelle[21] 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:

- 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;

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

- **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)[22]

Am 9. April 2013 wurde das Schengener Informationssystem der zweiten Generation ("SIS II") in 24 EU-Mitgliedstaaten sowie in vier mit der Schengen-Zusammenarbeit assoziierten Nicht-EU-Staaten (Norwegen, Island, Schweiz und Liechtenstein) in Betrieb genommen. 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[23].
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, so dass 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;

---

[22] 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).

[23] 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[24]

Das Europol-Informationssystem (EIS) 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.).

[24] Artikel 11 bis 13 des Beschlusses 2009/371/JI des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol) (ABl. L 121 vom 15.5.2009, S. 37).

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. Die "Treffer/kein Treffer"-Version kann auf benannte zuständige Behörden in den Mitgliedstaaten ausgeweitet werden. Einzelheiten zur Nutzung des EIS finden sich in Artikel 13 des Europol-Beschlusses des Rates. Die unterschiedlichen Kategorien der Daten des EIS sind in Artikel 12 aufgeführt. Die Vorschriften für die Nutzung der Daten und die Fristen für Speicherung und Löschung der Daten sind in Artikel 19 bzw. 20 enthalten.

Die Daten im EIS werden in den weitaus meisten Fällen über automatisierte Datenladesysteme eingegeben. Datenladeanwendungen ermöglichen die halbautomatische Eingabe von Massendaten aus dem nationalen System in das EIS. 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.

Das EIS, das den Austausch hoch sensibler Informationen ermöglicht, verfügt über ein solides Sicherheitssystem. 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 Sicherheit der Informationen sowie ihre sichere und angemessene Verarbeitung entsprechend den Wünschen des Eigentümers der Informationen und gemäß dem nationalen Recht der Mitgliedstaaten 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 verwendet wird. SIENA ist ein Mitteilungssystem, das ein Fallbearbeitungssystems mit speziellen Arten von Mitteilungen zur Unterstützung des sicheren Austauschs personenbezogener operativer Daten – einschließlich des Datenaustauschs gemäß dem "schwedischen Rahmenbeschluss" – einschließt.

Bei Konzeption und Funktionsweise von SIENA wurde größter Wert auf Sicherheit, Datenschutz und Vertraulichkeit gelegt. Es wurden alle erforderlichen Maßnahmen getroffen, um den sicheren Austausch von Informationen des Geheimhaltungsgrads "EU RESTRICTED" zu ermöglichen. Beim Datenaustausch über SIENA gibt es klare Verantwortlichkeiten für die Datenverarbeitung. Für jede abgehende SIENA-Meldung müssen der Vertraulichkeitsgrad, die Bearbeitungscodes und die Zuverlässigkeit der Quellen und der Informationen angegeben werden.

Die SIENA-Nutzerschnittstelle ist mehrsprachig und ermöglicht damit den SIENA-Operatoren, in ihrer bzw. ihren eigenen Landessprache(n) zu arbeiten. Ferner können die SIENA-Operatoren Abfragen durchführen und statistische Berichte über die über SIENA ausgetauschten Daten erstellen.

SIENA unterstützt den bilateralen Datenaustausch und ermöglicht es den Mitgliedstaaten, auch Daten außerhalb des Europol-Mandats auszutauschen. Erfolgt der Datenaustausch jedoch 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 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.

Seit Mai 2014 unterstützt SIENA den strukturierten Datenaustausch auf der Grundlage des UMF-Formats (Universal Message Format). Der Austausch aller UMF-Komponenten wird von SIENA unterstützt, aber derzeit sind nur die Daten zur UMF-Komponente PERSON in der SIENA-Mitteilung selbst sichtbar – alle anderen UMF-Komponenten sind in der bzw. den Anlage(n) sichtbar.

Die Interoperabilität von SIENA zu den übrigen Europol-Systemen wie dem Europol-Informationssystem (EIS), dem Europol-Analysesystem (EAS) und dem Vereinheitlichten Suchsystem (Unified Search System/USE) wird angestrebt.

Immer mehr Mitgliedstaaten zeigen Interesse an einer Anbindung ihres nationalen Fallbearbeitungssystems (Case Management System/CMS) an SIENA. Die vereinfachte SIENA-Webservice-Implementierung ermöglicht es den Mitgliedstaaten, alle ein- und ausgehenden SIENA-Meldungen automatisch in ihrem nationalen Fallbearbeitungssystem zu registrieren. Die erweiterte SIENA-Webservice-Implementierung ermöglicht es ferner den SIENA-Operatoren, SIENA-Nachrichten direkt über ihr nationales Fallbearbeitungssystem auszutauschen.

Ende 2014 verzeichnete SIENA 4 663 Nutzer aus den Mitgliedstaaten (ENU, LB und einzelstaatlich benannte zuständige Behörden (DCA)), von operativen Dritten (NCP, LB und DCA), strategischen Dritten (NCP und LB) und Europol. Mehr als 500 benannte zuständige Behörden sind an SIENA angeschlossen. Aus den SIENA-Statistiken für 2014 geht hervor, dass Monat für Monat etwa 50 500 SIENA-Meldungen ausgetauscht werden.

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 internationalen 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[25].

2.4.4 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 erleichtern, bei denen Feuerwaffen eine Rolle gespielt haben.

---

[25] Gemeinsamer Standpunkt 2005/69/JI des Rates zum Austausch bestimmter Daten mit Interpol (ABl. L 27 vom 27.1.2005, S. 61).

2.5. ECRIS[26]

Mit dem IT-basierten Europäischen Strafregisterinformationssystem (ECRIS)[27] werden die elektronischen Mittel für den Austausch von Informationen über Verurteilungen zwischen den Mitgliedstaaten in einem standardisierten Formatbereitgestellt. 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.

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.

---

[26] 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).

[27] Beschluss 2009/316/JI des Rates zur Einrichtung des Europäischen Strafregisterinformationssystems (ECRIS) gemäß Artikel 11 des Rahmenbeschlusses 2009/315/JI (ABl. L 93 vom 7.4.2009, S. 33).

2.6. Visa-Informationssystem (VIS)[28]

Das Visa-Informationssystem (VIS) ist hauptsächlich ein Einwanderungskontrollsystem. Es ist ein Werkzeug, das die Zusammenarbeit auf der Ebene der Grenzkontrollen durch die elektronische Verifizierung und den elektronischen Austausch von Visa-Daten zwischen den Mitgliedstaaten an den EU-Außengrenzen erleichtert. Als solches zielt es auf ausländische Staatsangehörige ab.
Die benannten Behörden der Mitgliedstaaten (d.h. konsularische Vertretungen, Grenzkontrollstellen, Polizei- und Einwanderungsbehörden)[29] und Europol[30] – im Rahmen seiner Aufgaben – sind befugt zur Abfrage des VIS[31] 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.

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.

---

28 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).

29 Erklärungen betreffend die benannten Behörden der Mitgliedstaaten und die benannte(n) zentrale(n) Zugangsstelle(n), die für Datenabfragen Zugang zum Visa-Informationssystem hat/haben im Sinne von Artikel 3 Absatz 2 und Artikel 3 Absatz 3 des Beschlusses 2008/633/JI des Rates (ABl. C 236 vom 14.8.2013, S. 1).

30 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); Beschluss 2013/392 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 (ABl. L 198 vom 23.7.2013, S. 45).

31 Am 16. April 2015 hat der Europäische Gerichtshof den 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, 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.

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 dem 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. VIS und SIS II teilen sich die gleiche technische Plattform, so dass der Zugang zu den Daten für die Beamten der beiden Systeme auf Gegenseitigkeit beruht, d.h. die VIS-Beamten können auf SIS-II-Daten zugreifen und umgekehrt.

2.7. Eurodac[32] [33]

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.

---

32 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).

33 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).

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, die ein dediziertes verschlüsseltes virtuelles Netz für Eurodac-Daten zur Verfügung stellt ("Kommunikationsinfrastruktur").

Jeder Mitgliedstaat hat eine einzige nationale Zugangsstelle.

Die mit der Verordnung (EU) Nr. 1077/2011[34] errichte Agentur ("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.

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.

---

[34] 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).

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:

– den nationalen Fingerabdruck-Datenbanken,

– den automatisierten Fingerabdruck-Identifizierungssystemen (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

– dem 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, das heißt, 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 sonstiger schwerer Straftaten einer Personenkategorie zugeordnet werden kann, die von dieser Verordnung erfasst wird.

2.8. ZIS – Zollinformationssystem[35]

Das Zollinformationssystem ergänzt das Neapel-II-Übereinkommen[36]. 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[37] 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.

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.

---

35 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).

36 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.

37 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 (13394/11 ENFOCUSTOM 85).

2.9. Gefälschte und echte Dokumente online – FADO[38]

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.

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.

---

[38] 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).

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[39] 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.

[39] http://www.prado.consilium.europa.eu/

2.11. 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** **(LSTD)**	Gemeinsamer Standpunkt 2005/69/JI des Rates zum Austausch bestimmter Daten mit Interpol ABl. L 27 vom 27.1.2005, S. 61	• Internationale und organisierte Kriminalität • Innere Sicherheit	• Unionsbürger • Drittstaatsangehörige	

ECRIS	Beschluss 2009/316/JI des Rates zur Einrichtung des Europäischen Strafregisterinformationssystems (ECRIS) gemäß Artikel 11 des Rahmenbeschlusses 2009/315/JI ABl. L 93 vom 7.4.2009, S. 33	Strafverfahren	• Unionsbürger • Drittstaatsangehörige	
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	• Schwerkriminalität • Innere Sicherheit • Terrorismusbekämpfung	• Drittstaatsangehörige	• SIS II • Europol • Interpol

	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			

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

ZIS	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
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. "Schwedischer Rahmenbeschluss"[40]

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[41] – 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[42], 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;
- 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.

---

40 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.).

41 Siehe Abbildung 1.

42 Siehe 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.

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[43] 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.
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 um 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;

[43] Siehe Abbildung 2.

- 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):	
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

3.2. 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) ergänzt, mit dem durch die vollständige 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.

Rechtsvorschriften

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)

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[44]. Am 9. April 2013 wurde das Schengener Informationssystem der zweiten Generation ("SIS II") in 24 EU-Mitgliedstaaten sowie in vier mit der Schengen-Zusammenarbeit assoziierten Nicht-EU-Staaten (Norwegen, Island, Schweiz und Liechtenstein) in Betrieb genommen.

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, so dass sie geeignete Maßnahmen für die Zwecke der Bekämpfung der Kriminalität und der irregulären Einwanderung ergreifen können.

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

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.

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 diejenigen 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.

3.3. Europol

Rechtsvorschriften

Beschluss 2009/371/JI des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol) (ABl. L 121 vom 15.5.2009, S. 37)[45]

[45] Über den Entwurf einer Verordnung über Europol wird derzeit verhandelt.

Kernbestimmungen

Europol hat zum Ziel, die Tätigkeit der für Prävention und Bekämpfung von Straftaten 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 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 EU ist mit Aufgaben in Bezug auf die Weitergabe relevanter Informationen und Erkenntnisse betraut. Jede nationale Einheit entsendet mindestens einen Verbindungsbeamten, der das nationale Verbindungsbüro bei Europol bildet und die Interessen der nationalen Einheit 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 Einheiten betraut. Dieser bilaterale Austausch kann sich auch auf Straftaten erstrecken, die über das Europol-Mandat hinausgehen.

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 Einheit, die Verbindungsbeamten und ordnungsgemäß ermächtigtes Personal von Europol haben das Recht, Daten in die Systeme einzugeben und von dort abzurufen.

3.4. Interpol

Rechtsvorschriften

Interpol-**Statuten**[46]

Vorschriften für die Verarbeitung von Informationen[47]

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

[46] http://www.interpol.int/en/About-INTERPOL/Legal-materials/The-Constitution

[47] http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts

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 weit gehende 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 grundegenden 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.

3.5. Verbindungsbeamte

Rechtsvorschriften

Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 19. Juni 1990 (SDÜ)[48], 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[49]

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[50]

[48] Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 19. Juni 1990 (SDÜ) (ABl. L 239 vom 22.9.2000, S. 19).
[49] Beschluss 2003/170/JI des Rates vom 27. Februar 2003 (Abl. L 67 vom 12.3.2003, S. 27).
[50] Beschluss 2006/560/JI des Rates vom 24. Juli 2006 (Abl. L 219 vom 10.8.2006, S. 31).

Beschluss 2009/371/JI des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol) (ABl. L 121 vom 15.5.2009, S. 37).

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;

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[51] 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[52].

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.

---

[51] 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 (ABl. C 322 vom 29.12.2006, S. 1).

[52] ABl. C 314 vom 22.12.2007, S. 4

Entsprechend dem derzeit geltenden Europol-Beschluss 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 nehmen Aufgaben in Bezug auf die Weitergabe relevanter Informationen und Erkenntnisse wahr. Jede nationale Einheit entsendet mindestens einen Verbindungsbeamten, der das nationale Verbindungsbüro bei Europol bildet und die Interessen der nationalen Einheit 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 Einheiten 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.

3.6. "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 (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)

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[53].

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).

3.7. 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)

[53] 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.

ABl. L 198 vom 23.7.2013, S. 45

Kernbestimmungen

Das VIS ist ein System, das den zuständigen nationalen Behörden ermöglicht, Visa-Daten 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.

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.

3.8. 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 der 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) neu gefasst (ABl. L 180 vom 29.6.2013, S. 1).

Kernbestimmungen

In der Verordnung (EU) Nr. 603/2016 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[54] und sonstiger schwerwiegender Straftaten[55] niedergelegt.

3.9. 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.

---

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

55 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).

3.9.1 Zollinformationssystem – ZIS[56]

Das Zollinformationssystem ergänzt das Neapel-II-Übereinkommen[57]. 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[58] 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.

---

56 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).

57 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.

58 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 (13394/11 ENFOCUSTOM 85).

3.10. Nationale Vermögensabschöpfungsstellen (ARO) und CARIN

Rechtsvorschriften

Beschluss 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.

Kernbestimmungen

Seit der Annahme des Beschlusses 2007/845/JI[59] 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[60] 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.

---

[59] Beschluss 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).

[60] 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 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.

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.

3.11. Zentrale Meldestellen für Geldwäsche-Verdachtsanzeigen (FIU)

Rechtsvorschriften

Beschluss 2000/642/JI des Rates vom 17. Oktober 2000 über Vereinbarungen für eine Zusammenarbeit zwischen den zentralen Meldestellen der Mitgliedstaaten beim Austausch von Informationen

ABl. L 271 vom 24.1.2000, S. 4

Kernbestimmungen

In einem Ersuchen muss angegeben werden, wie die erbetenen Informationen verwendet werden sollen, und – und dies ist ein wesentlicher Bestandteil des Beschlusses – die antwortende zentrale Meldestelle muss alle einschlägigen Informationen einschließlich der Finanzinformationen und der strafrechtlich relevanten Daten bereitstellen. Eine zentrale Meldestelle kann die Weitergabe von Informationen ablehnen, wenn damit laufende strafrechtliche Ermittlungen behindert würden oder es eindeutig in einem Missverhältnis zu den legitimen Interessen der betroffenen Person stehen oder nicht mit den Grundprinzipien des nationalen Rechts im Einklang stehen würde.

Die zentralen Meldestellen ergreifen alle erforderlichen Maßnahmen, einschließlich Sicherheitsvorkehrungen, um zu gewährleisten, dass die übermittelten Informationen anderen Behörden, Dienststellen oder Abteilungen nicht zugänglich sind. Die Mitgliedstaaten sorgen für angemessene und gesicherte Meldewege zwischen den zentralen Meldestellen und treffen hierfür entsprechende Vereinbarungen.

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, 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.

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

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.

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 vorgehen, 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.)

3.13. 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.

Der Beschluss 2009/316/JI des Rates vom 6. April 2009 zur Einrichtung des Europäischen Strafregisterinformationssystems (ECRIS) gemäß Artikel 11 des Rahmenbeschlusses 2009/315/JI beruht auf den mit dem Rahmenbeschluss 2009/315/JI festgelegten Grundsätzen und ergänzt diese Grundsätze in technischer Hinsicht.

Kernbestimmungen

Der Rahmenbeschluss 2009/315/JI des Rates verpflichtet einen verurteilenden Mitgliedstaat, alle in sein Strafregister eingetragenen Verurteilungen sowie alle etwa daran vorgenommenen Anpassungen und Streichungen so rasch wie möglich dem bzw. den Mitgliedstaat(en) der Staatsangehörigkeit der betreffenden Person mitzuteilen. Der Mitgliedstaat der Staatsangehörigkeit ist verpflichtet, die Informationen für die Zwecke der Weiterübermittlung zu speichern, und jede Anpassung oder Löschung im verurteilenden Mitgliedstaat zieht eine identische Anpassung oder Löschung im Strafregister des Mitgliedstaats der Staatsangehörigkeit der betreffenden Person nach sich. Wenn Informationen über Verurteilungen für die Zwecke von Strafverfahren beim Mitgliedstaat der Staatsangehörigkeit der betreffenden Person angefordert werden, so ist der ersuchte Mitgliedstaat verpflichtet, die im Strafregister gespeicherten Informationen über Verurteilungen zu übermitteln. Werden Informationen für andere Zwecke als Strafverfahren erbeten, so antwortet der ersuchte Mitgliedstaat im Einklang mit dem innerstaatlichen Recht.

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.

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[61]

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.

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

3.14. 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.

TEIL III – NATIONALE MERKBLÄTTER

VON HIER AB WURDE DER TEXT BIS ZUM ENDE DES DOKUMENTS (Seite 391) GELÖSCHT