EUROPÄISCHE KOMMISSION

Brüssel, den 20.7.2010

KOM(2010)385 endgültig

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht

1. EINLEITUNG

Die Europäische Union hat eine lange Wegstrecke zurückgelegt, seit die Staats- und Regierungschefs fünf europäischer Länder 1985 in Schengen beschlossen, die Kontrollen an ihren gemeinsamen Grenzen abzuschaffen. Ihre Vereinbarung führte zum Schengener Abkommen von 1990, das den Grundstein legte für etliche der Informationsmanagementstrategien von heute. Die Abschaffung der Kontrollen an den Binnengrenzen zog die Entwicklung einer ganzen Reihe von Maßnahmen an den Außengrenzen nach sich, vor allem in Bezug auf die Ausstellung von Visa, die Koordinierung der Asyl- und Einwanderungspolitik und die verstärkte Zusammenarbeit von Polizei-, Justiz- und Zollbehörden bei der Bekämpfung der grenzübergreifenden Kriminalität. Weder der Schengen-Raum noch der EU-Binnenmarkt könnten heute ohne grenzübergreifenden Informationsaustausch funktionieren.

Die Terroranschläge in den Vereinigten Staaten von 2001 und die Bombenattentate von Madrid und London von 2004 bzw. 2005 haben eine neue Dynamik in die Entwicklung der europäischen Informationsmanagementpolitik gebracht. 2006 verabschiedeten der Rat und das Europäische Parlament die Richtlinie über die Vorratsdatenspeicherung, um die nationalen Behörden in die Lage zu versetzen, durch die Speicherung der Telekommunikationsverkehrs- und Standortdaten die schwere Kriminalität zu bekämpfen[1]. Anschließend griff der Rat die schwedische Initiative zur Vereinfachung des grenzübergreifenden Austauschs von Informationen und Erkenntnissen für die Zwecke strafrechtlicher Ermittlungen oder polizeilicher Erkenntnisgewinnungsverfahren auf. 2008 wurde der Prüm-Beschluss angenommen, mit dem zur Bekämpfung des Terrorismus und anderer Formen der Kriminalität der Austausch von DNA-Profilen, Fingerabdrücken und Daten aus Fahrzeugregistern beschleunigt wurde. Die grenzübergreifende Zusammenarbeit zwischen den Stellen für Geldwäsche-Verdachtsanzeigen, den Vermögensabschöpfungsstellen und den Plattformen gegen Cyber-Kriminalität sowie die Nutzung von Europol und Eurojust durch die Mitgliedstaaten stellen im Schengen-Raum weitere Instrumente im Kampf gegen die schwere Kriminalität dar.

---

[1] Es gibt derzeit keine einheitliche EU-weite Definition der „schweren Kriminalität". Beispielsweise werden in dem Ratsbeschluss, mit dem Europol ermächtigt wird, das VIS abzufragen (Beschluss 2008/633/JI des Rates, ABl. L 218 vom 13.8.2008, S. 129) „schwerwiegende Straftaten" anhand einer Liste von Straftaten definiert, die im Rahmenbeschluss des Rates über den Europäischen Haftbefehl (Beschluss 2002/584/JI des Rates, ABl. L 190 vom 18.7.2002, S. 1) aufgeführt sind. Die Richtlinie über Vorratsdatenspeicherung (Richtlinie 2002/58/EG, ABl. L 105 vom 13.4.2006, S. 54) überlässt es den Mitgliedstaaten „schwere Kriminalität" zu definieren. Der Europol-Beschluss (Beschluss des Rates 2009/371/JI, ABl. L 121 vom 15.5.2009, S. 37) enthält eine andere Liste von Straftaten, die als „schwere Kriminalität" definiert werden; diese weist große Ähnlichkeit mit derjenigen aus dem Beschluss über den Europäischen Haftbefehl auf, ist aber nicht mit ihr identisch.

Unmittelbar nach den Terroranschlägen vom 11. September 2001 führte die Regierung der Vereinigten Staaten das Programm zum Aufspüren der Finanzierung des Terrorismus ein, mit dem vergleichbare Ereignisse durch die Kontrolle verdächtiger Finanztransaktionen verhindert werden sollen. Das Europäische Parlament hat kürzlich dem Abschluss eines Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (EU-USA TFTP-Abkommen) zugestimmt[2]. Darüber hinaus hat der Austausch von Fluggastdaten (Passenger Name Records - PNR) mit Drittländern die EU in ihrem Kampf gegen den Terrorismus und andere Formen schwerer Kriminalität unterstützt[3]. Nach dem Abschluss von PNR-Abkommen mit den USA, Australien und Kanada hat die Kommission kürzlich beschlossen, ihr Konzept, ein PNR-System in der EU einzuführen und diese Daten mit Drittländern auszutauschen, erneut zu überprüfen.

Die oben genannten Maßnahmen haben den freien Personenverkehr im Schengen-Raum ermöglicht, zur Verhinderung und Bekämpfung von Terroranschlägen und anderen Formen der schweren Kriminalität beigetragen und die Entwicklung der gemeinsamen Visa- und Asylpolitik gefördert.

Diese Mitteilung bietet zum ersten Mal einen vollständigen Überblick über die schon bestehenden, noch in der Umsetzung begriffenen oder in Betracht gezogenen Maßnahmen auf EU-Ebene, mit denen die Erhebung, die Speicherung und der grenzübergreifende Austausch personenbezogener Daten zu Zwecken der Strafverfolgung und Migrationssteuerung geregelt wird. Die Bürger haben das Recht zu erfahren, welche ihrer personenbezogenen Daten von wem und zu welchem Zweck verarbeitet und ausgetauscht werden. Dieses Dokument gibt klare Antworten auf diese Fragen. Herausgestellt wird der Hauptzweck der Instrumente, ihr Aufbau, die Art der darin erfassten personenbezogenen Daten, die zugriffsberechtigten Behörden sowie die für Datenschutz und Datenspeicherung geltenden Bestimmungen. Außerdem werden einige Beispiele dafür angeführt, wie diese Instrumente in der Praxis funktionieren (siehe Anhang I). Abschließend werden die Kerngrundsätze für die Gestaltung und Evaluierung von Informationsmanagementinstrumenten im Bereich Freiheit, Sicherheit und Recht herausgestellt.

Durch diesen Überblick über alle auf EU-Ebene bestehenden Maßnahmen, die das Management von personenbezogenen Informationen regeln, und durch den Vorschlag einer Reihe von Grundsätzen für die Entwicklung und Bewertung solcher Maßnahmen trägt diese Mitteilung zu einem sachkundigen Dialog mit allen Interessengruppen bei. Zugleich ist sie eine erste Reaktion auf das Anliegen der Mitgliedstaaten, ein „kohärenteres“ Konzept für den Austausch personenbezogener Informationen zum Zweck der Strafverfolgung zu entwickeln, das kürzlich in der EU-Strategie für das Informationsmanagement[4] formuliert wurde, und

---

2 Entschließung des Europäischen Parlaments vom 8.7.2010, P7_TA-PROV(2010)0279.

3 Im Gegensatz zu schwerer Kriminalität werden „terroristische Straftaten“ eindeutig im Rahmenbeschluss des Rates zur Terrorismusbekämpfung (2002/475/JI, ABl. L 164 vom 22.6.2002, S. 3, geändert durch den Rahmenbeschluss des Rates 2008/919/JI, ABl. L 330 vom 9.12.2008, S. 21) definiert.

4 Schlussfolgerungen des Rates zu einer Strategie für das Informationsmanagement im Bereich der inneren Sicherheit in der EU, Ratstagung Justiz und Inneres vom 30.11.2009 (EU-Strategie für das Informationsmanagement); „Freiheit, Sicherheit, Privatheit – Europäische Innenpolitik in einer offenen

über die Notwendigkeit der Entwicklung eines europäischen Modells für den Informationsaustausch nachzudenken, das sich auf eine Evaluierung der derzeitigen Informationsaustauschmaßnahmen stützt[5].

Die Zweckbindung ist für die meisten der in dieser Mitteilung aufgeführten Instrumente ein wichtiger Aspekt. Ein einziges, übergreifendes und vielfältig einsetzbares EU-Informationssystem würde ein Höchstmaß an Informationsaustausch ermöglichen. Allerdings würde ein solches System die Rechte des Einzelnen auf Privatsphäre und Datenschutz in grob rechtswidriger Weise einschränken und wäre äußerst schwer zu entwickeln und zu betreiben. In der Praxis hat sich die Politik im Bereich Freiheit, Sicherheit und Recht stufenweise entwickelt und einige Informationssysteme und –instrumente unterschiedlicher Größe, Reichweite und Zielrichtung hervorgebracht. Die unterteilte Struktur des Informationsmanagements, die sich in den letzten Jahrzehnten entwickelt hat, leistet mehr für die Wahrung der Rechte der Bürger auf ihre Privatsphäre als dies jede zentralisierte Alternative leisten könnte.

Nicht behandelt werden in dieser Mitteilung Maßnahmen für den Austausch nicht personenbezogener Daten zu strategischen Zwecken, beispielsweise allgemeine Risikoanalysen oder Bedrohungsbewertungen. Ebenso wenig werden die Datenschutzbestimmungen der behandelten Instrumente im Einzelnen analysiert, da die Kommission derzeit auf der Grundlage von Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union eine gesonderte Prüfung eines neuen umfassenden Rahmens für den Schutz personenbezogener Daten in der EU vornimmt. Der Rat prüft zur Zeit den Entwurf der Verhandlungsrichtlinien für ein Abkommen zwischen der EU und den USA über den Schutz personenbezogener Daten, die zum Zweck der Verhinderung, Ermittlung, Aufdeckung und Verfolgung von Straftaten einschließlich des Terrorismus im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen übermittelt und verarbeitet werden. Da sich diese Verhandlungen voraussichtlich mehr auf die Art und Weise beziehen werden, in der die Vertragsparteien bei der Übermittlung oder Verarbeitung personenbezogener Daten ein hohes Schutzniveau für die Grundrechte und Freiheiten gewährleisten können, als auf den eigentlichen Inhalt der Übermittlung oder Verarbeitung, ist diese Initiative nicht Gegenstand der vorliegenden Mitteilung[6].

2. EU-INSTRUMENTE ZUR REGELUNG DER ERHEBUNG, SPEICHERUNG ODER DES AUSTAUSCHS VON PERSONENBEZOGENEN DATEN ZU ZWECKEN DER STRAFVERFOLGUNG ODER MIGRATIONSSTEUERUNG

Dieser Abschnitt bietet einen Überblick über die Instrumente der Europäischen Union, die die Erhebung, Speicherung oder den grenzübergreifenden Austausch von personenbezogenen Daten zum Zwecke der Strafverfolgung oder Migrationssteuerung regeln. Abschnitt 2.1 stellt die schon in Kraft getretenen, in der Umsetzung begriffenen und in Betracht gezogenen Maßnahmen in den Mittelpunkt. Abschnitt 2.2 betrifft die im Aktionsplan zur Umsetzung des

---

Welt: Bericht der Informellen Hochrangigen Beratenden Gruppe zur Zukunft der europäischen Innenpolitik“, („The Future Group“), Juni 2008.

5 Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, Ratsdokument 5731/10 vom 3.3.2010, Abschnitt 4.2.2.

6 KOM(2010) 252 vom 26.5.2010.

Stockholmer Programms enthaltenen Initiativen[7]. Es werden folgende Aspekte jedes Instruments analysiert:

– Hintergrund (wurde die Maßnahme von einem Mitgliedstaat oder von der Kommission vorgeschlagen?)[8]

– Zweck, zu dem die Daten erhoben, gespeichert oder ausgetauscht werden

– Struktur (zentralisiertes Informationssystem oder dezentraler Datenaustausch)

– Art der personenbezogenen Daten

– Behörden, die Zugang zu den Daten haben

– Datenschutzbestimmungen

– Regeln für die Vorratsdatenspeicherung

– Stand der Umsetzung

– Überprüfungsmechanismus

2.1. Geltende, in der Umsetzung begriffene und in Betracht gezogene Maßnahmen

EU-Instrumente, mit denen das reibungslose Funktionieren des Schengen-Raums und der Zollunion gefördert werden soll

Das **Schengener Informationssystem** (SIS) geht auf den Wunsch einiger Mitgliedstaaten zurück, einen Raum ohne Kontrollen an den Binnengrenzen zu schaffen und zugleich den Verkehr von Personen über die Außengrenzen hinweg zu erleichtern[9]. Es besteht seit 1995 und dient dazu, die öffentliche und auch die nationale Sicherheit im Schengen-Raum aufrechtzuerhalten und den freien Personenverkehr durch die Übermittlung von Informationen über dieses System zu erleichtern. Das SIS ist ein zentralisiertes Informationssystem, das aus einem nationalen Teil in jedem beteiligten Staat sowie einer technischen Unterstützungseinheit in Frankreich besteht. Die Mitgliedstaaten können Personen ausschreiben, die verhaftet oder ausgeliefert werden sollen, Drittstaatsangehörige, denen die Einreise verweigert werden soll, vermisste Personen, Zeugen oder Personen, die vor Gericht geladen werden sollen, Personen und Fahrzeuge, die wegen der Gefahr, die sie für die

---

7 KOM(2010)171 vom 20.4.2010 (Aktionsplan zur Umsetzung des Stockholmer Programms).

8 Im Rahmen der ehemaligen dritten Säule der Europäischen Union, d.h. der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, teilten sich die Mitgliedstaaten und die Kommission das Initiativrecht. Durch den Vertrag von Amsterdam wurden die Bereiche Kontrolle der Außengrenzen, Visa, Asyl und Einwanderung in die Gemeinschaft (die erste Säule) integriert, wo die Kommission über das ausschließliche Initiativrecht verfügte. Durch den Vertrag von Lissabon wurde die Säulenstruktur der Union aufgehoben und das Initiativrecht der Kommission bestätigt. Im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (einschließlich der administrativen Zusammenarbeit) können Rechtsakte allerdings noch immer auf Initiative eines Viertels der Mitgliedstaaten vorgeschlagen werden.

9 Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen, ABl. L 239 vom 22.09.2000, S. 19.

öffentliche oder nationale Sicherheit darstellen, besonders überwacht werden, verlorene oder gestohlene Fahrzeuge, Dokumente und Schusswaffen sowie verdächtige Banknoten. In SIS eingetragen werden Namen und Aliasnamen, körperliche Merkmale, Geburtsort und -datum, Staatsangehörigkeit und ob eine Person bewaffnet oder gewalttätig ist; Polizei-, Grenzkontroll-, Zoll und Justizbehörden bei Strafverfahren haben im Rahmen ihrer jeweiligen gesetzlichen Befugnisse Zugang zu diesen Daten. Einwanderungsbehörden und konsularische Dienststellen haben Zugriff auf Daten von Drittstaatsangehörigen mit Einreiseverbot und Ausschreibungen betreffend verlorene und gestohlene Dokumente. Europol kann auf einige Kategorien von SIS-Daten zugreifen, darunter auch auf Ausschreibungen betreffend Personen, die verhaftet oder ausgeliefert werden sollen und Personen, die wegen der Gefahr, die sie für die öffentliche oder nationale Sicherheit darstellen, besonders überwacht werden. Eurojust hat Zugang zu Ausschreibungen betreffend Personen, die verhaftet oder ausgeliefert oder als Zeugen oder aus anderen Gründen vor Gericht geladen werden sollen. Die personenbezogenen Daten dürfen nur zum Zweck der spezifischen Ausschreibung benutzt werden, für die sie zur Verfügung gestellt wurden. In SIS eingegebene personenbezogene Daten werden nicht länger als für den verfolgten Zweck erforderlich und nicht über drei Jahre hinaus gespeichert. Daten über Personen, die wegen der Gefahr, die sie für die öffentliche oder nationale Sicherheit darstellen, besonders überwacht werden, müssen nach einem Jahr gelöscht werden. Die Mitgliedstaaten müssen nationale Vorschriften erlassen, die ein Datenschutzniveau garantieren, das mindestens demjenigen des Übereinkommens des Europarates über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1981 und der Empfehlung des Ministerkomitees des Europarats zur Regelung der Nutzung personenbezogener Daten durch die Polizei von 1987 entspricht[10]. Wenngleich das Schengener Abkommen keinen Überprüfungsmechanismus vorsieht, können die Vertragsparteien Änderungen vorschlagen; die Änderungen müssen einstimmig angenommen und von den Staaten ratifiziert werden. Das SIS ist in vollem Umfang in 22 Mitgliedstaaten sowie in der Schweiz, in Norwegen und Island anwendbar. Mit Ausnahme von Ausschreibungen betreffend Drittstaatsangehörige mit Einreiseverbot nehmen das Vereinigte Königreich und Irland an den Aspekten des Schengener Übereinkommens und des SIS teil, die die polizeiliche Zusammenarbeit betreffen. Zypern hat das Schengener Übereinkommen unterzeichnet, aber noch nicht umgesetzt. In Liechtenstein ist die Umsetzung für 2010 vorgesehen, in Bulgarien und Rumänien wird sie voraussichtlich 2011 erfolgen. Suchvorgänge in SIS ergeben einen „Treffer“, wenn die Angaben zu einer Person oder Sache den Angaben einer vorliegenden Ausschreibung entsprechen. Wenn sie einen Treffer erzielt haben, können die Strafverfolgungsbehörden über ihr Netz von SIRENE-Büros zusätzliche Informationen über den Gegenstand der Ausschreibung anfordern[11].

Da sich der Schengen-Raum um neue Mitgliedstaaten erweitert hat, ist der Umfang der SIS-Datenbank entsprechend gestiegen: Zwischen Januar 2008 und 2010 stieg die Gesamtzahl der SIS-Ausschreibungen von 22,9 auf 31,6 Millionen.[12] Da eine solche Zunahme des Datenvolumens und veränderte Benutzeranforderungen absehbar waren, beschlossen die Mitgliedstaaten 2001 die Entwicklung eines **Schengener Informationssystem der zweiten**

---

10 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), Europarat, 28.1.1981 (Übereinkommen 108 des Europarates); Empfehlung R (87) 15 des Ministerkomitees des Europarates zur Regelung der Benutzung personenbezogener Daten durch die Polizei, Europarat, 17.9.1987 (Empfehlung für die Polizei).

11 SIRENE steht für „Supplementary Information Request at National Entry” (Antrag auf Zusatzinformationen bei der nationalen Eingangsstelle).

12 Ratsdokument 5441/08 vom 30.1.2008; Ratsdokument 6162/10 vom 5.2.2010.

Generation (SIS II); hiermit wurde die Kommission beauftragt[13]. Das derzeit in der Entwicklung befindliche SIS II soll durch die Verbesserung der Funktionen des Systems der ersten Generation eine hohes Sicherheitsniveau im Raum der Freiheit, der Sicherheit und des Rechts gewährleisten und durch die Verwendung der über das System ausgetauschten Informationen den freien Personenverkehr erleichtern. Zusätzlich zu den vom SIS der ersten Generation erfassten Datenkategorien kann SIS II Fingerabdrücke, Fotografien, Kopien des Europäischen Haftbefehls, Vorkehrungen zur Wahrung der Interessen von Personen, deren Identität missbraucht wurde, und Verbindungen zwischen verschiedenen Ausschreibungen bearbeiten. Beispielsweise könnte SIS II eine Verbindung herstellen zwischen Ausschreibungen betreffend eine Person, die wegen Entführung gesucht wird, betreffend die entführte Person und betreffend das Fahrzeug, das für die Begehung der Straftat verwendet wurde. Die Zugangsrechte und die Regeln für die Datenspeicherung stimmen mit denen überein, die für das System der ersten Generation gelten. Die personenbezogenen Daten dürfen nur für den Zweck der spezifischen Ausschreibung benutzt werden, für den sie zur Verfügung gestellt wurden. Die in SIS gespeicherten personenbezogenen Daten müssen nach den besonderen Bestimmungen der Basisrechtsakte für dieses System bearbeitet werden (Verordnung (EG) Nr. 1987/2006 und Ratsbeschluss 2007/533/JI), in denen die Grundsätze der Richtlinie 95/46/EG erläutert werden, sowie gemäß der Verordnung (EG) Nr. 45/2001, dem Übereinkommen 108 des Europarates und der Empfehlung für die Polizei[14]. SIS II wird S-TESTA verwenden, das sichere Datenkommunikationsnetzwerk der Kommission[15]. Nach der Inbetriebnahme wird das System in allen Mitgliedstaaten, in der Schweiz, in Liechtenstein, Norwegen und Island Anwendung finden[16]. Die Kommission muss dem Europäischen Parlament und dem Rat einen halbjährlichen Fortschrittsbericht über die Entwicklung von SIS II und die Umstellung vom System der ersten Generation vorlegen[17].

Die Entwicklung von **EURODAC** geht auf die Aufhebung der Binnengrenzen zurück, die die Einführung klarer Regeln zur Bearbeitung von Asylanträgen erforderlich machte. EURODAC ist ein zentralisiertes automatisches Fingerabdruckidentifizierungssystem und enthält die Fingerabdruckdaten bestimmter Drittstaatsangehöriger. Es ist seit Januar 2003 in Betrieb und soll die Feststellung erleichtern, welcher Mitgliedstaat nach der Dublin-Verordnung für die Prüfung des einzelnen Asylantrags zuständig ist[18]. Personen im Alter von mindestens

---

13 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; Beschluss 2007/533/JI, ABl. L 205 vom 7.8.2007, S. 63.

14 Verordnung (EG) Nr. 1987/2006, ABl. L 381 vom 28.12.2006, S. 4; Beschluss 2007/533/JI, ABl. L 205 vom 7.8.2007, S. 63. Richtlinie 95/46/EG, ABl. L 281 vom 23.11.1995, S. 31. Verordnung (EG) Nr. 45/2001, ABl. L 8 vom 12.01.2001, S. 1. Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), Europarat, 18.1.1981 (Übereinkommen 108 des Europarates); Empfehlung R (87) 15 des Ministerkomitees des Europarates zur Regelung der Benutzung personenbezogener Daten durch die Polizei, Europarat, 17. September 1987 (Empfehlung für die Polizei).

15 S-TESTA (Secure Trans-European Services for Telematics between Administrations) ist ein von der Kommission finanziertes Datenkommunikationsnetz, das den sicheren und verschlüsselten Austausch von Daten zwischen den nationalen Behörden, EU-Organen, Agenturen und sonstigen Einrichtungen ermöglicht.

16 Mit Ausnahme von Ausschreibungen, die Drittstaatsangehörige mit Einreiseverbot betreffen, werden das VK und Irland am SIS II teilnehmen.

17 Verordnung (EG) Nr. 1104/2008 des Rates, ABl. L 299 vom 8.11.2008, S. 1. Beschluss 2008/839/JI des Rates, ABl. L 299 vom 8.11.2008, S. 43.

18 Verordnung (EG) Nr. 343/2003 des Rates, ABl. L 50 vom 25.2.2003, S. 1 (Dublin-Verordnung), Verordnung (EG) Nr. 2725/2000, ABl. L 316 vom 15.12.2000, S. 1 (EURODAC-Verordnung). Beide Instrumente legen das Dubliner Übereinkommen von 1990 zugrunde (ABl. C 254 vom19.8.1997. S. 1), in dem festgelegt werden sollte, welcher Mitgliedstaat für die Prüfung von Asylanträgen zuständig ist. Das System zur Bewertung von Asylanträgen ist das „Dublin-System".

14 Jahren, die in einem Mitgliedstaat Asyl beantragen, werden automatisch Fingerabdrücke abgenommen, ebenso Drittstaatsangehörigen, die beim illegalen Überschreiten einer Außengrenze aufgegriffen werden. Durch den Vergleich der Fingerabdrücke der Person mit den EURODAC-Daten versuchen die nationalen Behörden festzustellen, wo die Person möglicherweise einen Asylantrag gestellt hat, oder wo sie zuerst in die Europäische Union eingereist ist. Außerdem können die Behörden die Fingerabdrücke von Drittstaatsangehörigen, die sich illegal in ihrem Hoheitsgebiet aufhalten, mit den EURODAC-Daten vergleichen. Die Mitgliedstaaten müssen angeben, welche Behörden Zugriff auf diese Datenbank haben. Üblicherweise gehören dazu die Asyl- und Einwanderungsbehörden, der Grenzschutz und die Polizei. Die Mitgliedstaaten laden die relevanten Daten über ihre nationalen Zugangsstellen in die zentrale Datenbank hoch. Die in EURODAC gespeicherten personenbezogenen Daten dürfen ausschließlich dazu verwendet werden, die Anwendung der Dublin-Verordnung zu erleichtern; jede andere Verwendung ist strafbar. Die Fingerabdrücke von Asylbewerbern werden 10 Jahre lang gespeichert, diejenigen von illegalen Einwanderern zwei Jahre. Die Daten von Asylbewerbern werden gelöscht, sobald sie die Staatsangehörigkeit eines Mitgliedstaats erhalten, diejenigen von illegalen Einwanderern, sobald sie einen Aufenthaltstitel oder die Staatsangehörigkeit erworben oder aber das Hoheitsgebiet der Mitgliedstaaten verlassen haben. Die Richtlinie 95/46/EG ist auf die Verarbeitung personenbezogener Daten im Rahmen dieses Instruments anwendbar[19]. EURODAC läuft auf dem s-TESTA-Netz der Kommission und gilt für alle Mitgliedstaaten sowie für Norwegen, Island und die Schweiz. Ein Abkommen über die Beteiligung Liechtensteins steht kurz vor dem Abschluss. Die Kommission muss dem Europäischen Parlament und dem Rat jährlich einen Bericht über den Betrieb der Zentraleinheit von EURODAC vorlegen.

Nach den Attentaten vom 11. September 2001 beschlossen die Mitgliedstaaten, die Anwendung der gemeinsamen Visapolitik wirksamer zu gestalten, indem sie den Informationsaustausch über Visa für einen kurzfristigen Aufenthalt vereinheitlichten[20]. Die Aufhebung der Binnengrenzen hat es auch leichter gemacht, die Visasysteme der Mitgliedstaaten zu missbrauchen. Das **Visa-Informationssystem** (VIS) hat eine doppelte Funktion: Es dient der Umsetzung der gemeinsamen Visapolitik, indem es die Prüfung der Visumanträge und die Kontrollen an den Außengrenzen vereinfacht, und es dient dazu, Gefahren für die innere Sicherheit der Mitgliedstaaten vorzubeugen[21]. Das VIS wird ein zentralisiertes Informationssystem sein, das aus einem nationalen Teil in jedem beteiligten Staat sowie einer technischen Unterstützungseinheit in Frankreich besteht. Um die Zuverlässigkeit des Vergleichs der Fingerabdrücke zu gewährleisten und an den Außengrenzen die Identität von Visuminhabern zu überprüfen, nutzt das VIS ein System für den Abgleich biometrischer Daten. Es erstreckt sich auf Daten zu Visumanträgen, Fotografien, Fingerabdrücke, verbundene Beschlüsse von Visabehörden und Verbindungen zwischen miteinander verknüpften Anträgen. Die Visa-, Asyl-, Einwanderungs- und Grenzschutzbehörden werden Zugriff auf diese Datenbank haben, um die Identität von Visuminhabern und die Echtheit der Visa zu überprüfen. Die Polizei und Europol können die Daten zum Zweck der Bekämpfung des Terrorismus und anderer Formen schwerer Kriminalität einsehen[22]. Die Akten über Asylanträge werden fünf Jahre lang aufbewahrt. Die

---

19 Richtlinie 95/46/EG, ABl. L 281 vom 23.11.1995, S. 31.

20 Außerordentliche Ratstagung „Justiz und Inneres“ vom 20.9.2001.

21 Entscheidung 2004/512/EG des Rates (ABl. L 213 vom 15.6.2004, S. 5); Verordnung (EG) Nr. 767/2008, ABl. L 218 vom 13.8.2008, S. 60; Beschluss 2008/633/JI des Rates, ABl. L 218 vom 13.8.2008, S. 129. Siehe auch die Erklärung zur Terrorismusbekämpfung des Europäischen Rates vom 25.3.2004.

22 Beschluss 2008/633/JI des Rates, ABl. L 218 vom 13.8.2008, S. 129.

im VIS enthaltenen personenbezogenen Daten müssen nach Maßgabe der besonderen Bestimmungen der Basisrechtsakte für dieses System verarbeitet werden (Verordnung (EG) Nr. 767/2008 und Beschluss 2008/633/JI des Rates), die die Bestimmungen der Richtlinie 95/46/EG, der Verordnung (EG) Nr. 45/2001, des Rahmenbeschlusses 2008/977/JI des Rates, des Übereinkommens 108 des Europarates, des Zusatzprotokolls 181 und der Empfehlung für die Polizei ergänzen[23]. Das VIS wird in allen Mitgliedstaaten (mit Ausnahme des Vereinigten Königreichs und Irlands) sowie in der Schweiz, Norwegen und Island Anwendung finden. Es funktioniert auf der Grundlage des Datenkommunikationsnetzes s-TESTA der Kommission. Die Kommission nimmt drei Jahre nach der Inbetriebnahme und danach alle vier Jahre eine Bewertung des Systems vor.

Auf die Initiative Spaniens hin erließ der Rat im Jahr 2004 die Richtlinie über die Verpflichtung von Luftfahrtunternehmen, Grenzkontrollbehörden erweiterte Fluggastdaten (**Advance Passenger Information** – API) zu übermitteln[24]. Zweck dieses Instruments ist die Verbesserung der Grenzkontrollen und die Bekämpfung der illegalen Migration. Auf Anfrage müssen die Luftfahrtunternehmen diesen Behörden Namen, Geburtsdatum, Staatsangehörigkeit, Abflugort und die Grenzübergangsstelle von Fluggästen mitteilen, die aus Drittländern in die EU einreisen. Diese personenbezogenen Daten werden üblicherweise dem maschinenlesbaren Teil der Pässe der Fluggäste entnommen und den Behörden nach der Abfertigung übermittelt. Nach Ankunft des Fluges dürfen die Behörden und die Luftfahrtgesellschaften die API-Daten 24 Stunden aufbewahren. Das API-System arbeitet dezentral im Wege des Informationsaustauschs zwischen den privaten Unternehmen und den staatlichen Behörden. Im Rahmen dieses Instruments können keine Fluggastdaten zwischen Mitgliedstaaten ausgetauscht werden. Allerdings können Strafverfolgungsbehörden, sofern es sich nicht um den Grenzschutz handelt, zum Zweck der Strafverfolgung Zugang zu diesen Informationen beantragen. Die personenbezogenen Daten dürften lediglich von staatlichen Behörden zum Zweck der Grenzkontrolle und der Bekämpfung der illegalen Migration verwendet werden und sind nach Maßgabe der Richtlinie 95/46/EG zu verarbeiten[25]. Dieses Instrument ist zwar EU-weit in Kraft, wird jedoch nur von wenigen Mitgliedstaaten angewendet. Die Kommission wird die Richtlinie 2011 überarbeiten.

Ein wesentlicher Teil des Kommissionsprogramms von 1992, mit dem der Binnenmarkt errichtet wurde, betraf die Aufhebung aller Kontrollen und Formalitäten in Bezug auf die in der Gemeinschaft beförderten Waren[26]. Die Abschaffung solcher Verfahren an den Binnengrenzen brachte eine erhöhte Betrugsgefahr mit sich, der die Mitgliedstaaten begegnen mussten, indem sie zum einen ein System der gegenseitigen Amtshilfe zum Zweck der Verhinderung, Ermittlung und Verfolgung von Verstößen gegen die Zoll- und

---

[23] Verordnung (EG) Nr. 767/2008, ABl. L 218 vom 13.8.2008, S. 60; Beschluss 2008/633/JI des Rates, ABl. L 218 vom 13.8.2008, S. 129. Richtlinie 95/46/EG, ABl. L 281 vom 23.11.1995, S. 31. Verordnung (EG) Nr. 45/2001, ABl. L 8 vom 12.01.2001, S. 1. Rahmenbeschluss 2008/977/JI des Rates, ABl. L 350 vom 30.12.2008, S. 60; Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), Europarat, 18.1.1981 (Übereinkommen 108 des Europarates); Zusatzprotokoll zum Übereinkommen über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr (ETS Nr. 181), Europarat, 8.1.2001 (Zusatzprotokoll 181). Empfehlung R (87) 15 des Ministerkomitees des Europarates zur Regelung der Benutzung personenbezogener Daten durch die Polizei, Europarat, 17. September 1987 (Empfehlung für die Polizei).

[24] Richtlinie 2004/82/EG des Rates (ABl. L 261 vom 6.8.2004, S. 24).

[25] Richtlinie 95/46/EG, ABl. L 281 vom 23.11.1995, S. 31.

[26] Verordnung (EWG) 2913/92, ABl. L 302 vom 19.10.1992.

Agrarvorschriften der Gemeinschaft und zum anderen eine Zusammenarbeit der Zollbehörden einführten, die darauf abzielte, Verstöße gegen nationale Zollvorschriften insbesondere durch einen verstärkten grenzübergreifenden Informationsaustausch aufzudecken und zu verfolgen. Unbeschadet der Zuständigkeit der EU in der Zollunion[27] bezweckte das **Übereinkommen von Neapel II** über die Zusammenarbeit und gegenseitige Amtshilfe der Zollbehörden, die nationalen Zollbehörden in die Lage zu versetzen, Zuwiderhandlungen gegen die nationalen Zollbestimmungen zu verhindern und aufzudecken und sie bei der Verfolgung und Bestrafung von Verstößen gegen die Zollvorschriften der Gemeinschaft und des Mitgliedstaats zu unterstützen[28]. Im Rahmen dieses Instruments erbitten zentrale Koordinierungsstellen von ihren Partnerstellen in anderen Mitgliedstaaten schriftlich Unterstützung bei strafrechtlichen Ermittlungen betreffend Verstöße gegen die Zollvorschriften eines Mitgliedstaats oder der Gemeinschaft. Diese dürfen personenbezogene Daten ausschließlich zu den im Übereinkommen von Neapel II genannten Zwecken verarbeiten. Sie dürfen die Informationen an die nationalen Zoll-, Ermittlungs- und Justizbehörden und, soweit der die Information bereitstellende Mitgliedstaat dies zuvor genehmigt hat, an andere Behörden weiterleiten. Die Daten dürfen nur so lange aufbewahrt werden, wie es für den Zweck, zu dem sie zur Verfügung gestellt wurden, notwendig ist. Im entgegennehmenden Mitgliedstaat gilt für die personenbezogenen Daten mindestens das gleiche Schutzniveau wie im bereitstellenden Mitgliedstaat; ihre Verarbeitung muss nach Maßgabe der Richtlinie 95/46/EG und des Übereinkommens 108 des Europarats erfolgen[29]. Das Übereinkommen Neapel II wurde von sämtlichen Mitgliedstaaten ratifiziert. Falls die Mitgliedstaaten Änderungen vorschlagen, muss der geänderte Wortlaut vom Ministerrat angenommen und von den Mitgliedstaaten ratifiziert werden.

In Ergänzung zum Übereinkommen Neapel II wird mit dem ZIS-Übereinkommen das **Zollinformationssystem (ZIS)** eingeführt, mit dem durch eine rasche Informationsverbreitung die Zusammenarbeit zwischen den Zollverwaltungen der Mitgliedstaaten bei der Verhinderung, Ermittlung und Verfolgung schwerwiegender Verstöße gegen die nationalen Gesetze verbessert wird[30]. Das ZIS wird durch die Kommission verwaltet und ist ein zentralisiertes Informationssystem, auf das die Mitgliedstaaten und die Kommission, Europol und Eurojust über ihre jeweiligen Terminals zugreifen. Es enthält personenbezogene Daten im Hinblick auf Ausgangsstoffe, Beförderungsmittel, Unternehmen, Personen und Waren sowie einbehaltenes oder beschlagnahmtes Bargeld. Die personenbezogenen Daten umfassen Namen und Aliasnamen, Geburtsdatum und –ort, Staatsangehörigkeit, Geschlecht, körperliche Merkmale, Ausweisdokumente, Anschrift, Anfragen zu einer eventuellen Gewalttätigkeit in der Vergangenheit, Gründe für die Datenspeicherung im ZIS, vorgeschlagene Maßnahmen und Zulassungsdaten des

---

27 Verordnung (EG) Nr. 515/97 des Rates vom 13. März 1997 über die gegenseitige Amtshilfe zwischen Verwaltungsbehörden der Mitgliedstaaten und die Zusammenarbeit dieser Behörden mit der Kommission im Hinblick auf die ordnungsgemäße Anwendung der Zoll- und der Agrarregelung, ABl. L 82 vom 22.3.1997, S. 1, geändert durch die Verordnung (EG) Nr. 766/2008, ABl. L 218 vom 13.8.2008, S. 48.

28 Übereinkommen aufgrund von Artikel K.3 des Vertrags über die Europäische Union über gegenseitige Amtshilfe und Zusammenarbeit der Zollverwaltungen, ABl. C 24/2 vom 23.1.1998 (Übereinkommen Neapel II).

29 Richtlinie 95/46/EG, ABl. L 281 vom 23.11.1995, S. 31. Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), Europarat, 28.1.1981 (Übereinkommen 108 des Europarates).

30 Übereinkommen aufgrund von Artikel K.3 des Vertrags über die Europäische Union über den Einsatz der Informationstechnologie im Zollbereich, ABl. C 316 vom 27.11.1995, S. 34, geändert durch den Beschluss 2009/917/JI des Rates, ABl. L 323 vom 10.12.2009, S. 20.

Beförderungsmittels. Sofern Waren und Bargeld einbehalten oder beschlagnahmt werden, dürfen lediglich Angaben zur Person und die Anschrift in das ZIS eingegeben werden. Diese Informationen dürfen ausschließlich zum Zweck der Feststellung, Unterrichtung, besonderen Untersuchung oder spezifischer Kontrollen beziehungsweise der strategischen oder operativen Analyse betreffend Personen verwendet werden, die eines Verstoßes gegen die nationalen Zollvorschriften verdächtigt werden. Zugriff auf die ZIS-Daten haben die Zoll-, Steuer-, Agrar-, Gesundheits- und Polizeibehörden der Mitgliedstaaten sowie Europol und Eurojust[31]. Die Verarbeitung der personenbezogenen Daten muss in Einklang mit den besonderen Vorschriften für das ZIS und der Richtlinie 96/46/EG, der Verordnung (EG) Nr. 45/2001, dem Übereinkommen 108 des Europarates und der Empfehlung für die Polizei erfolgen[32]. Die personenbezogenen Daten dürfen nur aus Gründen des Risikomanagements und der operativen Analyse, wozu nur von den Mitgliedstaaten benannte Experten Zugang haben, vom ZIS in andere Datenverarbeitungssysteme kopiert werden. Aus dem ZIS kopierte personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies zur Erfüllung des Zwecks, zu dem sie kopiert wurden, notwendig ist, keinesfalls aber länger als 10 Jahre. Im Rahmen des ZIS wurde auch zum Zweck der Vorbeugung, Ermittlung und Verfolgung schwerwiegender Verstöße gegen nationale Gesetze das **Aktennachweissystem für Zollzwecke** (FIDE) eingeführt[33]. Wenn sie eine Ermittlungsakte anlegen, können nationale Behörden, die für Zollermittlungen zuständig sind, anhand von FIDE feststellen, ob andere Behörden bereits Ermittlungen zu einer bestimmten Person oder einem bestimmten Unternehmen durchgeführt haben. Diese Behörden können Angaben aus ihren Ermittlungsakten in FIDE eingeben: biografische Angaben zu Personen, über die ermittelt wird, Firmenname, Umsatzsteuernummer sowie Anschrift der betreffenden Unternehmen. Die Daten aus Ermittlungsakten, bei denen kein Betrug festgestellt wurde, dürfen höchstens drei Jahre gespeichert werden, solche, bei denen Zollbetrug festgestellt wurde, dürfen höchstens sechs Jahre und solche, bei denen eine Verurteilung oder Strafe ausgesprochen wurde, höchsten zehn Jahre gespeichert werden. ZIS und FIDE benutzen das Gemeinsame Kommunikationsnetz, die Gemeinsame Systemschnittstelle bzw. den sicheren Internetzugang der Kommission. Das ZIS ist in sämtlichen Mitgliedstaaten in Kraft. Die Kommission berichtet in Zusammenarbeit mit den Mitgliedstaaten dem Europäischen Parlament und dem Rat jährlich über die Funktionsweise des ZIS.

EU-Instrumente zur Verhinderung und Bekämpfung des Terrorismus und anderer Formen der schweren Kriminalität

---

31 Ab Mai 2011 werden auf der Grundlage des Beschlusses 2009/917/JI des Rates (ABl. C 323 vom 10.12.2009, S. 20) Europol und Eurojust die ZIS-Daten einsehen dürfen.

32 Übereinkommen aufgrund von Artikel K.3 des Vertrags über die Europäische Union über den Einsatz der Informationstechnologie im Zollbereich, ABl. C 316 vom 27.11.1995, S. 34, geändert durch den Beschluss 2009/917/JI des Rates, ABl. L 323 vom 10.12.2009, S. 20. Richtlinie 95/46/EG, ABl. L 281 vom 23.11.1995, S. 31. Verordnung (EG) Nr. 45/2001, ABl. L 8 vom 12.1.2001, S. 1. Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), Europarat, 28.1.1981 (Übereinkommen 108 des Europarates); Empfehlung R (87) 15 des Ministerkomitees des Europarates zur Regelung der Benutzung personenbezogener Daten durch die Polizei, Europarat, 17.9.1987 (Empfehlung für die Polizei).

33 FIDE (*Fichier d'Identification des Dossiers d'Enquêtes douanières)* beruht auf der Verordnung (EG) Nr. 766/2008 des Rates und dem gemäß Artikel 34 des Vertrags über die Europäische Union erstellten Protokoll zur Änderung des Übereinkommens über den Einsatz der Informationstechnologie im Zollbereich hinsichtlich der Einrichtung eines Aktennachweissystems für Zollzwecke, ABl. C 139 vom 13.6.2003, S. 1.

Auf die Terroranschläge in Madrid vom März 2004 hin wurden auf EU-Ebene mehrere neue Initiativen auf den Weg gebracht. Auf Wunsch des Europäischen Rates legte die Kommission 2005 den Vorschlag für ein Instrument zur Regelung des Informationsaustauschs nach dem Grundsatz der Verfügbarkeit vor[34]. Anstatt diesen Vorschlag zu unterstützen, nahm der Rat 2006 die **schwedische Initiative** an, mit der der Austausch vorliegender Informationen und Erkenntnisse zur Durchführung strafrechtlicher Ermittlungen oder polizeilicher Erkenntnisgewinnungsverfahren vereinfacht werden soll[35]. Grundlage des Instruments ist das Prinzip des „gleichberechtigten Zugangs", wonach die Bedingungen für den grenzübergreifenden Datenaustausch nicht strenger sein dürfen, als diejenigen für den inländischen Zugang. Die schwedische Initiative ist dezentral konzipiert und ermöglicht es Polizei-, Zoll- und anderen Behörden, die befugt sind, bei Straftaten zu ermitteln (mit Ausnahme der Nachrichtendienste, die üblicherweise mit Ermittlungen im Zusammenhang mit der Sicherheit des Staates betraut sind) Informationen und polizeiliche Erkenntnisse anderen EU-Ländern auszutauschen. Die Mitgliedstaaten müssen nationale Kontaktstellen benennen, die dringende Informationsanfragen bearbeiten. Mit der Maßnahme werden eindeutige Fristen für den Informationsaustausch festgelegt, und die Mitgliedstaaten müssen ein Formular ausfüllen, wenn sie Informationen anfordern. Die Mitgliedstaaten müssen die Anfragen in dringenden Fällen binnen acht Stunden, in nicht dringenden Fällen binnen einer Woche und in allen anderen Fällen binnen zwei Wochen beantworten. Die Verwendung der mit Hilfe dieses Instruments erhaltenen Informationen und Erkenntnisse unterliegt den entsprechenden nationalen Datenschutzgesetzen; die Mitgliedstaaten dürfen Informationen aus dem Inland und solche aus den anderen Mitgliedstaaten nicht unterschiedlich behandeln. Allerdings kann ein Mitgliedstaat, der Informationen weitergibt, Bedingungen für die Verwendung der Informationen oder Erkenntnisse in den anderen Mitgliedstaaten festlegen. Die personenbezogenen Daten müssen im Einklang mit den nationalen Datenschutzvorschriften, dem Übereinkommen 108 des Europarats, dem Zusatzprotokoll 181 und der Empfehlung für die Polizei verarbeitet werden[36]. Zwölf der 31 Unterzeichnerstaaten dieser Maßnahme (u.a. EU-Mitgliedstaaten, Norwegen, Island, die Schweiz und Liechtenstein) haben nationale Umsetzungsvorschriften angenommen; fünf Staaten füllen bei Informationsersuchen regelmäßig das Formular aus, aber nur zwei Staaten benutzen die Maßnahme zum häufigen Informationsaustausch[37]. Die Kommission übermittelt dem Rat ihren Bewertungsbericht vor Ende 2010.

Der **Beschluss von Prüm** baut auf einen Vertrag zwischen Deutschland, Frankreich, Spanien, den Benelux-Staaten und Österreich von 2005 auf, mit dem die Zusammenarbeit bei der Bekämpfung des Terrorismus, der grenzübergreifenden Kriminalität und der illegalen Migration verbessert werden sollte. Da mehrere Mitgliedstaaten Interesse signalisierten, diesem Vertrag beizutreten, schlug Deutschland während seiner Ratspräsidentschaft im Jahr

---

34 KOM(2005)490 vom 12.10.2005; Schlussfolgerungen des Ratsvorsitzes – Haager Programm 4./5.11.2004. Siehe auch die Erklärung zur Terrorismusbekämpfung, Europäischer Rat, 25.3.2004.

35 Rahmenbeschluss 2006/960/JI des Rates, ABl. L 386 vom 29.12.2006, S. 89.

36 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), Europarat, 28.1.1981 (Übereinkommen 108 des Europarates); Zusatzprotokoll zum Übereinkommen über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr (ETS Nr. 181), Europarat, 8.11.2001 (Zusatzprotokoll 181). Empfehlung R (87) 15 des Ministerkomitees des Europarates zur Regelung der Benutzung personenbezogener Daten durch die Polizei, Europarat, 17.9.1987 (Empfehlung für die Polizei).

37 Diese Angaben beruhen auf den Antworten auf einen Fragebogen, die der spanische Ratsvorsitz in einer Sitzung der Ad-hoc-Arbeitsgruppe des Rates zum Informationsaustausch am 22. Juni 2010 vorlegte.

2007 vor, ihn in ein EU-Instrument umzuwandeln. Im Beschluss von Prüm aus dem Jahr 2008, der bis August 2011 umgesetzt werden muss, sind Regeln für den grenzübergreifenden Austausch von DNA-Profilen, Fingerabdrücken, Daten aus Fahrzeugregistern und von Informationen über Personen, die unter Terrorverdacht stehen, festgelegt[38]. Verbessert werden soll die Verhinderung von Straftaten, insbesondere terroristischer und grenzübergreifender Straftaten, und die Aufrechterhaltung der öffentlichen Ordnung bei Großveranstaltungen. Das System funktioniert dezentral, d.h. die Datenbanken der beteiligten Staaten, in denen DNA-Profile, Fingerabdrücke und Fahrzeugzulassungen gespeichert sind, werden über nationale Kontaktpunkte zusammengeschaltet. Die Kontaktpunkte verwenden das s-TESTA-Netz der Kommission und bearbeiten die ein- und ausgehenden Anfragen zu grenzübergreifenden Vergleichen von DNA-Profilen, Fingerabdrücken und Fahrzeugregistrierungen. Ihre Befugnis, solche Daten an die einschlägigen Nutzer weiterzugeben, ist in den nationalen Gesetzen geregelt. Ab August 2011 wird der Datenabgleich vollautomatisch erfolgen. Die Mitgliedstaaten müssen sich allerdings einer rigorosen Bewertung (insbesondere in Bezug auf ihre Einhaltung der Datenschutz- und der technischen Erfordernisse) unterziehen, bevor ihnen die Genehmigung zum automatischen Datenaustausch erteilt wird. Personenbezogene Daten dürfen im Rahmen dieses Instrument nur dann ausgetauscht werden, wenn die Mitgliedstaaten ein Datenschutzniveau gewährleisten, das mindestens demjenigen des Übereinkommens 108 des Europarats, dem Zusatzprotokoll 181 und der Empfehlung für die Polizei entspricht[39]. Der Rat stellt durch einstimmigen Beschluss fest, ob diese Voraussetzung erfüllt ist. Personenbezogene Daten dürfen ausschließlich für den Zweck verwendet werden, für den sie zur Verfügung gestellt wurden, es sei denn, der bereitstellende Mitgliedstaat stimmt der Verwendung für andere Zwecke zu. Einzelpersonen können sich an ihre gemäß der Richtlinie 95/46/EG benannten nationalen Datenschutzbeauftragten wenden, um ihre Rechte in Bezug auf die Verarbeitung ihrer Daten im Rahmen dieses Instruments geltend zu machen. Der Vergleich von DNA-Profilen und Fingerabdrücken funktioniert auf der Grundlage des Ergebnisses „Treffer/kein Treffer“, d.h. anonym; die Behörden können personenbezogene Informationen nur dann anfordern, wenn ihre Suche einen Treffer ergeben hat. Solche Anträge auf Zusatzinformationen erfolgen üblicherweise im Wege der schwedischen Initiative. Der Beschluss von Prüm wird derzeit von allen EU-Mitgliedstaaten umgesetzt. Der Beitritt Norwegens und Islands steht bevor[40]. 2012 übermittelt die Kommission dem Rat ihren Bewertungsbericht.

Als Reaktion auf die Bombenattentate in London vom Juli 2005 schlugen Großbritannien, Irland, Schweden und Frankreich die Annahme eines EU-Instruments vor, mit dem die nationalen Bestimmungen über die Vorratsdatenspeicherung harmonisiert werden sollen. Die **Richtlinie über die Vorratsspeicherung von Daten** von 2006 verpflichtet die Anbieter von Telefon- und Internetdiensten zum Zwecke der Ermittlung, Feststellung und Verfolgung

---

38 Beschluss 2008/615/JI des Rates (ABl. L 210 vom 6.8.2008, S. 1); Beschluss 2008/616/JI des Rates, ABl. L 210 vom 6.8.2008, S. 12.

39 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), Europarat, 28.1.1981 (Übereinkommen 108 des Europarates); Zusatzprotokoll zum Übereinkommen über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr (ETS Nr. 181), Europarat, 8.11.2001 (Zusatzprotokoll 181). Empfehlung R (87) 15 des Ministerkomitees des Europarates zur Regelung der Benutzung personenbezogener Daten durch die Polizei, Europarat, 17.9.1987 (Empfehlung für die Polizei).

40 Bisher wurde 10 Mitgliedstaaten gestattet, mit dem automatisierten Austausch von DNA-Profilen, 5 Mitgliedstaaten, mit dem Austausch von Fingerabdrücken und 7 Mitgliedstaaten, mit dem Austausch von Fahrzeugzulassungsdaten zu beginnen. Deutschland, Österreich, Spanien und die Niederlande haben der Kommission Teilstatistiken über die Verwendung dieses Instruments übermittelt.

schwerer Straftaten die Verkehrs- und Standortdaten sowie Informationen über Teilnehmer (einschließlich deren Telefonnummer, IP-Adresse und Gerätekennung) zu speichern[41]. Die Richtlinie über die Vorratsdatenspeicherung regelt weder den Zugang noch die Verwendung von Daten, die von nationalen Behörden gespeichert werden. Nicht in den Anwendungsbereich der Richtlinie fällt ausdrücklich der Inhalt der elektronischen Kommunikation; das bedeutet, dass das Abhören im Rahmen dieses Instruments nicht möglich ist. Dieses Instrument überlässt es den Mitgliedstaaten, „schwere Straftaten" zu definieren, die nationalen Behörden zu benennen, die fallweise Zugriff auf diese Daten haben, und die Verfahren für die Gewährung des Datenzugriffs festzulegen. Die Speicherfristen liegen zwischen 6 und 24 Monaten. Im Hinblick auf den Schutz personenbezogener Daten gelten die Richtlinien 95/46/EG und 2002/58/EG[42]. Sechs Mitgliedstaaten haben diese Maßnahmen noch nicht vollständig umgesetzt, und in Deutschland und Rumänien haben die Verfassungsgerichte die nationalen Umsetzungsvorschriften für verfassungswidrig erklärt. Das deutsche Verfassungsgericht stellte fest, dass die in den deutschen Vorschriften festgelegten Regeln über den Zugang und die Verwendung der Daten nicht verfassungsgemäß sind[43]. Das rumänische Verfassungsgericht stellte fest, dass die Vorratsdatenspeicherung *per se* gegen Artikel 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention) verstößt und aus diesem Grund verfassungswidrig ist[44]. Die Kommission nimmt derzeit eines Bewertung dieses Instruments vor und wird dem Europäischen Parlament und dem Rat Ende 2010 ihren Evaluierungsbericht vorlegen.

Die derzeitige Einführung des **Europäischen Strafregisterinformationssystems** (ECRIS) geht auf eine belgische Initiative des Jahres 2004 zurück, bei der es darum ging, verurteilte Sexualstraftäter daran zu hindern, in anderen Mitgliedstaaten einer Tätigkeit nachzugehen, bei der sie Kontakte zu Kindern haben. In der Vergangenheit stützten sich die Mitgliedstaaten auf das Übereinkommen des Europarates über die Rechtshilfe in Strafsachen, wenn sie Informationen über strafrechtliche Verurteilungen austauschen wollten, doch erwies sich dieses System als ineffizient[45]. Der Rat nahm als ersten Reformschritt den Beschluss 2005/876/JI des Rates an, wonach jeder Mitgliedstaat eine Zentralbehörde benennt, die in regelmäßigen Abständen die strafrechtlichen Verurteilungen von Personen, die nicht die Staatsangehörigkeit dieses Mitgliedstaats besitzen, an den oder die Mitgliedstaat(en) übermittelt, deren Staatsangehörige(r) die betreffende Person ist[46]. Mit diesem Instrument konnten die Mitgliedstaaten auch erstmals und vorbehaltlich der nationalen Bestimmungen, Informationen über frühere Verurteilungen ihrer eigenen Staatsangehörigen in einem anderen Mitgliedstaat anfordern. Anstatt hierfür Amtshilfeverfahren anzustrengen, genügte das Ausfüllen eines Standardformulars. 2006 und 2007 legte die Kommission ein umfassendes Legislativpaket mit drei Instrumenten vor: Rahmenbeschluss des Rates 2008/675/JI, mit dem die Mitgliedstaaten verpflichtet werden, in neuen Strafverfahren die früheren Verurteilungen zu berücksichtigen, Rahmenbeschluss des Rates 2009/315/JI über die Durchführung und den Inhalt des Austauschs von Informationen aus dem Strafregister zwischen den Mitgliedstaaten und Beschluss 2009/316/JI des Rates, mit dem ECRIS als technische Grundlage für den

---

41 Richtlinie 2006/24/EG, ABl. L 105 vom 13.4.2006, S. 54.

42 Richtlinie 95/46/EG, ABl. L 281 vom 23.11.1995, S. 31. Richtlinie 2002/58/EG, ABl. L 201 vom 31.7.2002, S. 37 (Datenschutzrichtlinie für elektronische Kommunikation).

43 Urteil des deutschen Bundesverfassungsgerichts, 1 BvR 256/08, 11.3.2008.

44 Beschluss Nr. 1258 des rumänischen Verfassungsgerichts vom 8.10.2009.

45 Europäisches Übereinkommen über die Rechtshilfe in Strafsachen (ETS Nr. 30), Europarat, 20.4.1959, Siehe auch KOM(2005) 10 vom 25.1.2005.

46 Beschluss 2005/876/JI des Rates, ABl. L 322 vom 9.12.2005, S. 33.

Austausch von Strafregisterinformationen errichtet wird[47]. Die Rahmenbeschlüsse 2009/315/JI und 2009/316/JI des Rates sollen bis April 2012 umgesetzt werden und legen fest, auf welche Weise der Urteilsmitgliedstaat die Informationen über eine neue Verurteilung dem Mitgliedstaat/den Mitgliedstaaten übermitteln muss, dessen/deren Staatsangehörigkeit die verurteilte Person besitzt; ferner definieren sie die Pflichten zum Speichern dieser Informationen und legen einen Rahmen für ein computergestütztes System für den Informationsaustausch fest. ECRIS wird ein dezentrales Informationssystem sein, das die Strafregisterdatenbanken der Mitgliedstaaten über das s-TESTA-Netzwerk der Kommission miteinander verbindet. Bestimmte zentrale Behörden werden Daten über neue Verurteilungen und Strafregisterdaten austauschen. Die Daten sind verschlüsselt, entsprechend einem vorbestimmten Format strukturiert und erstrecken sich auf Angaben zur Person, Verurteilung, Strafe und den zugrundeliegenden Straftatbestand sowie zusätzliche Informationen (einschließlich Fingerabdrücke, sofern vorhanden). Ab April 2012 müssen die Auszüge aus dem Strafregister für laufende Strafverfahren bereitgestellt und den Justiz- oder zuständigen Verwaltungsbehörden zugestellt werden, beispielsweise Einrichtungen, die befugt sind, Personen mit Blick auf eine Beschäftigung für sicherheitsrelevante Tätigkeiten oder beim Erwerb von Schusswaffen zu überprüfen. Personenbezogene Daten, die für ein Strafverfahren zur Verfügung gestellt werden, dürfen nur für diesen Zweck verwendet werden. Die Verwendung für andere Zwecke setzt das Einverständnis des bereitstellenden Mitgliedstaats voraus. Die Verarbeitung personenbezogener Daten muss im Einklang stehen mit den einschlägigen Bestimmungen des Rahmenbeschlusses 2009/315/JI des Rates, in den die Regeln des Beschlusses 2005/876/JI des Rates aufgenommen wurden, sowie mit dem Rahmenbeschluss 2008/977/JI des Rates und dem Übereinkommen 108 des Europarats[48]. Für die Verarbeitung personenbezogener Daten durch die EU-Organe mithilfe von ECRIS, zum Beispiel hinsichtlich der Datensicherheit, gilt die Verordnung (EG) Nr. 45/2001[49]. Dieses Legislativpaket enthält keine Regeln über die Vorratsdatenspeicherung, da für die Speicherung von Daten betreffend strafrechtliche Verurteilungen die nationalen Gesetze gelten. Derzeit nehmen fünfzehn Mitgliedstaaten an einem Pilotprojekt teil; davon haben neun mit dem elektronischen Austausch von Informationen aus den Strafregistern begonnen. Die Kommission muss dem Europäischen Parlament und dem Rat zwei Evaluierungsberichte zur Funktionsweise dieses Legislativpakets vorlegen: Der Rahmenbeschluss 2008/675/JI muss 2011, der Rahmenbeschluss 2009/315/JI muss 2015 überprüft werden. Ab 2016 muss die Kommission darüber hinaus regelmäßige Berichte über den Betrieb von ECRIS veröffentlichen.

Aufgrund einer Initiative Finnlands nahm der Rat im Jahr 2000 ein Instrument für den Informationsaustausch zwischen den **zentralen Meldestellen zur Entgegennahme von Finanzinformationen** (Financial Intelligence Units - FIU) zum Zwecke der Bekämpfung der Geldwäsche und später des Terrorismus an[50]. FIU werden gewöhnlich innerhalb von Strafverfolgungsbehörden, Justizbehörden oder aber Verwaltungseinheiten eingerichtet, die an Finanzbehörden berichten. Sie tauschen mit ihren EU-Partnerstellen notwendige Finanz-

---

47 Rahmenbeschluss 2008/675/JI des Rates, ABl. L 220 vom 15.8.2008, S. 32; Rahmenbeschluss 2009/315/JI des Rates, ABl. L 93 vom 7.4.2009, S. 23; Beschluss 2009/316/JI des Rates, ABl. L 93 vom 7.4.2009, S. 33. Siehe auch KOM(2005) 10 vom 25.1.2005.

48 Rahmenbeschluss 2009/315/JI des Rates, ABl. L 93 vom 7.4.2009, S. 23; Beschluss 2005/876/JI des Rates (ABl. L 322 vom 9.12.2005, S. 33); Rahmenbeschluss 2008/977/JI des Rates, ABl. L 350 vom 30.12.2008, S. 60; Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), Europarat, 28.1.1981 (Übereinkommen 108 des Europarates).

49 Verordnung (EG) Nr. 45/2001, ABl. L 8 vom 12.1.2001, S. 1.

50 Beschluss 2000/642/JI des Rates, ABl. L 271 vom 24.10.2000, S. 4.

oder Strafverfolgungsdaten einschließlich der Einzelheiten von Finanztransaktionen aus; dies gilt nicht für Fälle, in denen die Weitergabe dieser Daten im Vergleich zu den Interessen natürlicher oder juristischer Personen unverhältnismäßig wäre. Die zum Zweck der Analyse oder Untersuchung der Geldwäsche oder Terrorismusfinanzierung zur Verfügung gestellten Informationen können auch für strafrechtliche Ermittlungen oder die strafrechtliche Verfolgung herangezogen werden, es sei denn, der bereitstellende Mitgliedstaat untersagt eine solche Verwendung. Die Verarbeitung der personenbezogenen Daten muss im Einklang stehen mit dem Rahmenbeschluss 2008/977/JI des Rates, dem Übereinkommen 108 des Europarats und der Empfehlung für die Polizei[51]. 2002 führten mehrere Mitgliedstaaten FIU.net ein, eine dezentrale Anwendung, mit der die Daten zwischen den FIU ausgetauscht werden können, und die sich auf das s-TESTA-Netzwerk der Kommission stützt[52]. Diese Initiative zählt 20 FIU als Mitglieder. Derzeit wird darüber diskutiert, SIENA, die sichere Anwendung von Europol, als Grundlage für das FIU.net zu verwenden[53]. Nach Prüfung der Einhaltung der FIU-Bestimmungen durch die Mitgliedstaaten ermächtigte der Rat die FIU in der dritten Richtlinie zur Bekämpfung der Geldwäsche, verdächtige Transaktionen im Zusammenhang mit Geldwäsche *und* Terrorismusfinanzierung entgegenzunehmen, zu analysieren und zu verbreiten[54]. Im Rahmen ihres Aktionsplans für Finanzdienstleistungen überprüft die Kommission seit 2009 die Umsetzung der dritten Richtlinie zur Bekämpfung der Geldwäsche[55].

2007 griff der Rat eine Initiative von Österreich, Belgien und Finnland auf und nahm ein Instrument zur Förderung der Zusammenarbeit zwischen **Vermögensabschöpfungsstellen** (Asset Recovery Offices - ARO) bei der Identifizierung und Nachverfolgung von Erträgen aus Straftaten an[56]. Ähnlich wie die FIU kooperieren die ARO dezentral, allerdings ohne Unterstützung einer Online-Plattform. Sie müssen für den Informationsaustausch die schwedische Initiative verwenden, die Einzelheiten des untersuchten Eigentums, z.B. Bankkonten, Immobilien und Fahrzeuge nennen sowie Angaben zu den gesuchten natürlichen oder juristischen Personen machen (Name, Anschrift, Geburtsdatum, Beteiligungen oder Informationen über das Unternehmen). Die Verwendung der mit Hilfe dieses Instruments ausgetauschten Informationen unterliegt den nationalen Datenschutzgesetzen; die Mitgliedstaaten dürfen Informationen aus dem Inland und solche aus den anderen Mitgliedstaaten nicht unterschiedlich behandeln. Bei der Verarbeitung der personenbezogenen Daten muss das Übereinkommen 108 des Europarats, das Zusatzprotokoll 181 und die Empfehlung für die Polizei eingehalten werden[57]. Bisher haben mehr als 20 Mitgliedstaaten

---

51 Rahmenbeschluss 2008/977/JI des Rates, ABl. L 350 vom 30.12.2008, S. 60; Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), Europarat, 28.1.1981 (Übereinkommen 108 des Europarates); Empfehlung R (87) 15 des Ministerkomitees des Europarates zur Regelung der Benutzung personenbezogener Daten durch die Polizei, Europarat, 17.9.1987 (Empfehlung für die Polizei).

52 http://www.fiu.net/

53 SIENA steht für „Secure Information Exchange Network Application".

54 Richtlinie 2005/60/EG, ABl. L 309 vom 25.11.2005, S. 15 (dritte Richtlinie zur Bekämpfung der Geldwäsche).

55 Siehe beispielsweise „Evaluation of the economic impacts of the Financial Services Action Plan – Final report" (für die Europäische Kommission, GD MARKT), CRA International, 03.2009.

56 Beschluss 2007/845/JI des Rates, ABl. L 332 vom 18.12.2007, S. 103.

57 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), Europarat, 28.1.1981 (Übereinkommen 108 des Europarates); Zusatzprotokoll zum Übereinkommen über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr (ETS Nr. 181), Europarat, 8.11.2001 (Zusatzprotokoll 181). Empfehlung R (87) 15 des Ministerkomitees des

ARO eingerichtet. Angesichts der Sensibilität der ausgetauschten Informationen wird diskutiert, beim Datenaustausch zwischen den ARO die SIENA-Anwendung von Europol einzusetzen. In einem Pilotprojekt, das im Mai 2010 eingeleitet wurde, haben zwölf ARO begonnen, für den Austausch betreffend das Aufspüren von Vermögenswerten SIENA zu verwenden. 2010 übermittelt die Kommission dem Rat ihren Bewertungsbericht.

2008 forderte die französische Ratspräsidentschaft die Mitgliedstaaten auf, nationale **Plattformen gegen Cyber-Kriminalität** einzurichten und regte Europol an, eine europäische Plattform gegen Cyber-Kriminalität zum Zwecke der Sammlung, Analyse und des Austauschs von Informationen über Internet-Straftaten einzurichten[58]. Die Bürger können ihren nationalen Plattformen Fälle von rechtswidrigem Inhalt oder Verhalten melden, die sie im Internet entdeckt haben. Die von Europol verwaltete Europäische Cybercrime-Plattform (ECCP) dient als Informationsknotenpunkt, wo Analysen durchgeführt und mit den nationalen Strafverfolgungsbehörden Informationen über Internet-Kriminalität, die unter das Mandat von Europol fällt, ausgetauscht werden[59]. Fast alle Mitgliedstaaten haben nationale Meldeplattformen eingerichtet. Europol arbeitet derzeit an der technischen Einrichtung der ECCP und wird möglicherweise bald seine SIENA-Anwendung dazu einsetzen, den Datenaustausch mit den nationalen Plattformen zu verbessern. Insoweit der Datenaustausch die Verarbeitung personenbezogener Daten durch Europol einschließt, gelten die einschlägigen Bestimmungen des Europol-Beschlusses (Beschluss 2009/371/JI des Rates), die Verordnung (EG) Nr. 45/2001, das Übereinkommen 108 des Europarats, das Zusatzprotokoll 181 und die Empfehlung für die Polizei[60]. Der Rahmenbeschluss 2008/977/JI des Rates regelt den Austausch von personenbezogenen Daten zwischen den Mitgliedstaaten und Europol[61]. Da diesbezüglich kein Rechtsinstrument geschaffen wurde, gibt es keinen förmlichen Überprüfungsmechanismus für Cybercrime-Meldeplattformen. Allerdings deckt Europol diesen wichtigen Bereich ab und wird in Zukunft in seinem dem Rat zur Genehmigung und dem Europäischen Parlament zur Kenntnisnahme vorgelegten Jahresbericht über die Tätigkeit der ECCP berichten.

Europarates zur Regelung der Benutzung personenbezogener Daten durch die Polizei, Europarat, 17. September 1987 (Empfehlung für die Polizei).

58 Schlussfolgerungen des Rates zur Errichtung von nationalen Plattformen und einer europäischen Plattform für Hinweise auf Internetstraftaten, Ratstagung Justiz und Inneres vom 24.10.2008; Schlussfolgerungen des Rates betreffend einen Aktionsplan zur Umsetzung der konzertierten Strategie für die Kriminalitätsbekämpfung, Ratstagung Allgemeine Angelegenheiten, 26.4.2010. Europol hat sein Projekt in „Europäische Cybercrime-Plattform“ (ECCP) umbenannt.

59 Ziel von Europol ist die Verhütung und Bekämpfung von organisierter Kriminalität, Terrorismus und anderen schweren Verbrechen, die zwei oder mehrere Mitgliedstaaten betreffen. Beschluss 2009/371/JI des Rates, ABl. L 121 vom 15.5.2009, S. 37.

60 Beschluss 2009/371/JI des Rates (ABl. L 121 vom 15.5.2009, S. 37); Verordnung (EG) Nr. 45/2001, ABl. L 8 vom 12.1.2001, S. 1. Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), Europarat, 28.1.1981 (Übereinkommen 108 des Europarates); Zusatzprotokoll zum Übereinkommen über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr (ETS Nr. 181), Europarat, 8.11.2001 (Zusatzprotokoll 181). Empfehlung R (87) 15 des Ministerkomitees des Europarates zur Regelung der Benutzung personenbezogener Daten durch die Polizei, Europarat, 17. September 1987 (Empfehlung für die Polizei).

61 Rahmenbeschluss 2008/977/JI des Rates, ABl. L 350 vom 30.12.2008, S. 60.

EU-Agenturen und –Einrichtungen, die den Auftrag haben, die Mitgliedstaaten bei der Verhinderung und Bekämpfung schwerer grenzübergreifender Kriminalität zu unterstützen

Das im Jahr 1995 eingerichtete **Europäische Polizeiamt** (Europol) hat 1999 seine Tätigkeit aufgenommen und wurde im Januar 2010 in eine EU-Agentur umgewandelt[62]. Ziel von Europol ist die Unterstützung der Mitgliedstaaten bei der Verhütung und Bekämpfung von organisierter Kriminalität, Terrorismus und anderen schweren Verbrechen, die zwei oder mehrere Mitgliedstaaten betreffen. Zu seinen Hauptaufgaben zählen Erhebung, Speicherung, Verarbeitung, Analyse und Austausch von Informationen und Erkenntnissen und die Unterstützung der Mitgliedstaaten bei Ermittlungen, der Bereitstellung einschlägiger Erkenntnisse und Analysen. Die Hauptverbindung zwischen Europol und den Mitgliedstaaten sind die nationalen Europol-Stellen, die Europol Verbindungsbeamte zur Verfügung stellen. Die Leiter der nationalen Europol-Stellen treffen sich regelmäßig, um Europol operativ zu unterstützen. Die Agentur wird von einem Verwaltungsrat und einem Direktor geleitet. Zu den Informationsverarbeitungssystemen von Europol zählen das Europol-Informationssystem (EIS), Arbeitsdateien und die Anwendung SIENA. Das EIS umfasst personenbezogene Daten einschließlich biometrischer Merkmale, strafrechtlicher Verurteilungen und Verbindungen zur organisierten Kriminalität betreffend Personen, die eines Verbrechens verdächtigt werden, das in den Zuständigkeitsbereich von Europol fällt. Zugang hierzu haben die nationalen Europol-Stellen, die Verbindungsbeamten, bevollmächtigte Beschäftigte von Europol und der Direktor. Die Arbeitsdateien, die der Unterstützung strafrechtlicher Ermittlungen dienen, enthalten Daten zu Personen und sonstige Informationen, die von den nationalen Europol-Stellen beigefügt werden. Zugang haben die Verbindungsbeamten, doch nur Europol-Analytiker können Daten in diese Dateien eingeben. Anhand eines Index-Systems können die nationalen Europol-Stellen und die Verbindungsbeamten prüfen, ob die Arbeitsdateien Informationen enthalten, die für ihren Mitgliedstaat von Interesse sind. Die SIENA-Anwendung von Europol wird immer häufiger von den Mitgliedstaaten genutzt, um sensible Daten zu Strafverfolgungszwecken auszutauschen. Europol kann im Rahmen der Erfüllung seiner Aufgaben Informationen und Erkenntnisse, einschließlich personenbezogener Daten, bearbeiten. Die Mitgliedstaaten dürfen die in den Europol-Dateien enthaltenen Informationen ausschließlich zum Zweck der Verhinderung und Bekämpfung grenzübergreifender schwerer Kriminalität verwenden. Werden von einem Informationen bereitstellenden Mitgliedstaaten Beschränkungen in Bezug auf die Verwendung der Daten ausgesprochen, so gelten diese Beschränkungen auch für andere Nutzer, die die Daten den Europol-Dateien entnehmen. Europol kann auch personenbezogene Daten mit Drittländern austauschen, die operative Vereinbarungen mit Europol geschlossen haben und ein angemessenes Datenschutzniveau garantieren. Daten dürfen nur so lange gespeichert werden, wie es für die Erfüllung der Aufgaben notwendig ist. Arbeitsdateien dürfen höchstens drei Jahre gespeichert werden, wobei diese Frist um weitere drei Jahre verlängert werden kann. Die Verarbeitung personenbezogener Daten durch Europol muss mit den einschlägigen Bestimmungen seines Basisrechtsakts (Beschluss 2009/371/JI des Rates), mit der Verordnung (EG) 45/2001, dem Übereinkommen 108 des Europarats, dem Zusatzprotokoll 181 und der Empfehlung für die Polizei in Einklang stehen[63]. Der Rahmenbeschluss 2008/977/JI des Rates ist auf den

---

62 Beschluss des Rates 2009/371/JI, ABl. L 121 vom 15.5.2009, S. 37. Er ersetzte das Übereinkommen aufgrund von Artikel K.3 des Vertrags über die Europäische Union über die Errichtung eines Europäischen Polizeiamts, ABl. C 316 vom 27.11.1995, S. 2.

63 Beschluss 2009/371/JI des Rates (ABl. L 121 vom 15.5.2009, S. 37); Verordnung (EG) Nr. 45/2001, ABl. L 8 vom 12.1.2001, S. 1. Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), Europarat, 28.1.1981 (Übereinkommen 108 des Europarates); Zusatzprotokoll zum Übereinkommen über den Schutz des Menschen bei der

Austausch von personenbezogenen Daten zwischen den Mitgliedstaaten und Europol anwendbar[64]. Eine gemeinsame Kontrollinstanz, bestehend aus den Mitgliedern der nationalen Kontrollinstanzen, überwacht die Verarbeitung personenbezogener Daten durch Europol sowie die Übermittlung personenbezogener Daten an andere Parteien durch Europol. Sie legt dem Europäischen Parlament und dem Rat regelmäßig einen Bericht vor. Europol legt seinen jährlichen Tätigkeitsbericht dem Rat zur Genehmigung und dem Europäischen Parlament zur Kenntnisnahme vor.

Die Terroranschläge vom 11. September 2001 haben sich nicht nur auf verschiedene oben beschriebene Instrumente ausgewirkt, sondern führten auch zur Einrichtung der **Europäischen Stelle für justizielle Zusammenarbeit** (Eurojust) im Jahr 2002[65]. Eurojust ist eine Einrichtung der EU, deren Ziel die Verbesserung der Koordinierung von Ermittlungen und Strafverfolgungen in den Mitgliedstaaten sowie der Zusammenarbeit zwischen den zuständigen nationalen Behörden ist. Es deckt dieselben Arten der Kriminalität und Straftaten ab wie Europol. Zum Zweck der Erfüllung ihrer Aufgaben haben die 27 nationalen Mitglieder von Eurojust, die zusammen das Kollegium bilden, im Rahmen des Mandats von Eurojust Zugang zu den personenbezogenen Daten von Verdächtigen und Straftätern. Dazu gehören insbesondere: Angaben zur Person, Kontaktadresse, Fahrzeugzulassungsdaten, DNA-Profile, Fotografien, Fingerabdrücke sowie Verkehrs-, Standort- und Teilnehmerdaten, die seitens der Anbieter von Telekommunikationsdiensten zur Verfügung gestellt werden. Von den Mitgliedstaaten wird erwartet, dass sie solche Informationen mit Eurojust austauschen, damit die Stelle ihre Aufgaben erfüllen kann. Alle personenbezogenen Daten zu den Fällen müssen in das System zur automatisierten Fallbearbeitung von Eurojust eingegeben werden, das sich auf das s-TESTA-Netz der Kommission stützt. Mit einem Indexsystem werden die personenbezogenen und nicht personenbezogenen Daten, die für laufende Ermittlungen relevant sind, gespeichert. Zur Erfüllung seiner Aufgaben kann Eurojust personenbezogene Daten verarbeiten, allerdings unter Einhaltung der einschlägigen Bestimmungen seines Basisrechtsakts (Beschluss 2009/426/JI des Rates), des Übereinkommens 108 des Europarats, des Zusatzprotokolls 181 und der Empfehlung für die Polizei. Der Rahmenbeschluss 2008/977/JI des Rates ist auf den Austausch von personenbezogenen Daten zwischen den Mitgliedstaaten und Eurojust anwendbar[66]. Eurojust kann Daten mit nationalen Behörden und mit Drittländern austauschen, mit denen es eine Vereinbarung geschlossen hat, sofern der Mitgliedstaat, der die Daten bereitgestellt hat, diesem Austausch zugestimmt hat und das Drittland einen angemessenen Schutz personenbezogener Daten gewährleistet. Die personenbezogenen Daten können so lange gespeichert werden, wie dies zum Erreichen der Ziele von Eurojust notwendig ist, müssen jedoch gelöscht werden, sobald der Fall abgeschlossen ist. Die Mitgliedstaaten müssen den geänderten Basisrechtsakt von Eurojust bis Juni 2011 umsetzen. Bis Juni 2014 muss die Kommission den Informationsaustausch zwischen den nationalen Mitgliedern von Eurojust überprüfen; sie kann Änderungen vorschlagen, wenn sie dies für angemessen hält. Bis Juni 2013 muss Eurojust dem Rat und der Kommission darüber berichten, welche Erfahrungen damit gemacht wurden, das System

---

automatischen Verarbeitung personenbezogener Daten betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr (ETS Nr. 181), Europarat, 8.1.2001 (Zusatzprotokoll 181). Empfehlung R (87) 15 des Ministerkomitees des Europarates zur Regelung der Benutzung personenbezogener Daten durch die Polizei, Europarat, 17. September 1987 (Empfehlung für die Polizei).

64 Rahmenbeschluss 2008/977/JI des Rates, ABl. L 350 vom 30.12.2008, S. 60.

65 Beschluss 2002/187/JI des Rates (ABl. L 63 vom 6.3.2002, S. 1), geändert durch den Beschluss 2009/426/JI des Rates (ABl. L 138 vom 4.6.2009, S. 14). Siehe auch außerordentliche Ratstagung „Justiz und Inneres“ vom 20.9.2001.

66 Rahmenbeschluss 2008/977/JI des Rates, ABl. L 350 vom 30.12.2008, S. 60.

zur automatisierten Fallbearbeitung den nationalen Behörden zugänglich zu machen. Auf dieser Grundlage können die Mitgliedstaaten die nationalen Zugangsrechte überprüfen. Eine gemeinsame Kontrollinstanz, bestehend aus von den Mitgliedstaaten benannten Richtern, überwacht die Verarbeitung personenbezogener Daten durch Eurojust und berichtet jährlich dem Rat. Der Präsident des Kollegiums legt dem Rat einen jährlichen Bericht über die Tätigkeit von Eurojust vor, den dieser an das Europäische Parlament weiterleitet.

Internationale Übereinkommen zur Verhütung und Bekämpfung des Terrorismus und anderer Formen schwerer grenzübergreifender Kriminalität

Nach den Terroranschlägen vom 11. September 2001 erließen die Vereinigten Staaten Vorschriften, denen zufolge Luftfahrtgesellschaften, die Flüge nach, von oder über das Gebiet der Vereinigten Staaten anbieten, ihren Behörden die **Fluggastdaten** (Passenger Name Records - PNR) übermitteln müssen, die sie in ihren computergestützten Buchungssystemen gespeichert haben. Kanada und Australien beschlossen gleiche Maßnahmen. Da nach den einschlägigen Vorschriften der EU eine vorherige Bewertung des von Drittländern gewährleisteten Datenschutzniveaus erforderlich ist, übernahm die Kommission diese Aufgabe und handelte die PNR-Abkommen mit diesen Ländern aus[67]. Sie unterzeichnete das Abkommen mit den Vereinigten Staaten im Juli 2007, das mit Australien im Juni 2008 und ein API/PNR-Abkommen mit Kanada im Oktober 2005[68]. Die Abkommen mit den USA und Australien sind vorläufig anwendbar, während das Abkommen mit Kanada in Kraft bleibt, obwohl im September 2009 die Angemessenheitsentscheidung der Kommission betreffend die kanadischen Datenschutznormen ausgelaufen ist[69]. Das Europäische Parlament hat den Inhalt der Abkommen kritisiert und die Kommission aufgefordert, alle drei Abkommen auf der Grundlage einer Reihe klarer Grundsätze neu zu verhandeln[70]. Die frühzeitig vor dem Abflug übersandten Fluggastdaten helfen Strafverfolgungsbehörden, die Fluggäste im Hinblick auf mögliche Verbindungen zum Terrorismus oder anderen Formen schwerer Kriminalität zu überprüfen. Zweck jedes Abkommens ist somit die Verhinderung und Bekämpfung des Terrorismus und anderer Formen des schweren internationalen Verbrechens. Im Gegenzug übermittelt das amerikanische Department of Homeland Security (DHS) den Strafverfolgungsbehörden der EU, Europol und Eurojust sogenannte „lead information“, die aus ihrer PNR-Analyse hervorgeht. Sowohl Kanada als auch die Vereinigten Staaten haben in ihren jeweiligen Abkommen versprochen, mit der EU bei der Errichtung ihres eigenen Fluggastdatensystems zusammenzuarbeiten. Die Abkommen mit den USA und Australien umfassen 19 Datenkategorien, darunter Angaben zur Person, Reservierung, Zahlungsweise sowie ergänzende Informationen; das Abkommen mit Kanada enthält 25 ähnliche Datenkategorien. Zu den ergänzenden Informationen zählen Angaben zu Flugscheinen für einfache Strecken, den Standby-Status und nicht angetretene Flüge. Außerdem gestattet das Abkommen mit den USA unter besonderen Bedingungen die Verwendung von sensiblen Informationen. Das DHS kann solche Informationen verarbeiten, wenn das Leben einer

---

67 Richtlinie 95/46/EG (Datenschutzrichtlinie), ABl. L 281 vom 23.11.1995, S. 31.

68 Das Paket für Kanada besteht aus einer Zusage Kanadas betreffend die Bearbeitung von API/PNR-Daten, der Angemessenheitsentscheidung der Kommission betreffend die kanadischen Datenschutznormen und einem internationalen Übereinkommen (siehe ABl. L 91 vom 29.3.2006, S. 49; ABl. L 82 vom 21.3.2006, S. 14). Das Abkommen mit den Vereinigten Staaten siehe ABl. L 204 vom 4.8.2007, S. 16, das Abkommen mit Australien siehe ABl. L 213 vom 8.8.2008, S. 47.

69 2009 verpflichtete sich Kanada gegenüber der Kommission, dem Ratsvorsitz und den EU-Mitgliedstaaten, seine frühere Verpflichtung aus dem Jahr 2005 betreffend die Verwendung von PNR-Daten aus der EU weiter anzuwenden. Die Angemessenheitsentscheidung der Kommission beruhte auf dieser früheren Verpflichtung.

70 Entschließung des Europäischen Parlaments vom 5.5.2010, P7_TA(2010)0144.

Person in Gefahr ist, muss die Daten jedoch binnen 30 Tagen löschen. Die PNR-Daten werden den Zentraleinheiten innerhalb des DHS, der kanadischen „Border Services Agency“ (Grenzdienstbehörde) und dem australischen Zoll übermittelt. Diese dürfen die Angaben nur an inländische Behörden weiterleiten, die für Strafverfolgung und Terrorismusbekämpfung zuständig sind. Nach dem Abkommen mit den USA geht das DHS davon aus, dass das Datenschutzniveau, das es auf die Verarbeitung der Fluggastdaten aus der EU anwenden muss, „nicht höher“ ist als dasjenige, das von europäischen Behörden in ihren inländischen PNR-Systemen angewandt wird. Wird diese Erwartung nicht erfüllt, so können die USA bestimmte Teile des Abkommens aussetzen. Nach Auffassung der Union gewährleisten Kanada und Australien ein „angemessenes“ Schutzniveau für die Fluggastdaten aus der EU, sofern sie die Bestimmungen ihres jeweiligen Abkommens einhalten. In den USA werden PNR-Daten aus der EU sieben Jahre lang in einer aktiven und weitere acht Jahre lang in einer ruhenden Datenbank gespeichert. In Australien werden die Daten dreieinhalb Jahre in einer aktiven und anschließend zwei Jahre lang in einer ruhenden Datenbank gespeichert. In beiden Ländern kann auf die ruhende Datenbank nur mit einer Sondergenehmigung zugegriffen werden. In Kanada werden die Daten dreieinhalb Jahre lang gespeichert, wobei die Informationen nach 72 Stunden anonymisiert werden. Jedes Abkommen sieht eine regelmäßige Überprüfung vor, die Abkommen mit Kanada und Australien beinhalten ferner Beendigungsklauseln. In der EU verfügt nur das Vereinigte Königreich über ein PNR-System. Frankreich, Dänemark, Belgien, Schweden und die Niederlande haben entweder bereits entsprechende Vorschriften erlassen oder sind im Begriff, die Verwendung von PNR-Daten mit Blick auf die Einführung von PNR-Systemen zu testen. Mehrere andere Mitgliedstaaten erwägen die Einführung von PNR-Systemen, und sämtliche Mitgliedstaaten verwenden im Einzelfall PNR-Daten zu Strafverfolgungszwecken.

Nach den Anschlägen vom 11. September 2001 entwickelte das amerikanische Finanzministerium sein **Programm zum Aufspüren der Finanzierung des Terrorismus** (Terrorist Finance Tracking Program – TFTP), mit dem Terroristen und ihre finanziellen Helfer ermittelt, aufgespürt und verfolgt werden sollen. Im Rahmen dieses Programm verlangte das amerikanische Finanzministerium im Wege administrativer Anordnungen von der amerikanischen Niederlassung eines belgischen Unternehmen die Übermittlung einer begrenzten Zahl von Zahlungsverkehrsdaten (FIN), die über sein Netzwerk befördert werden. Im Januar 2010 änderte das Unternehmen seine Systemarchitektur, was die Zahl der unter die US-Gerichtsbarkeit fallenden Datensätze, die diesen Anordnungen des Finanzministeriums unterliegen, um mehr als die Hälfte reduzierte. Im November 2009 unterzeichneten der Vorsitz des Rates der Europäischen Union und die Regierung der Vereinigten Staaten von Amerika ein Interimsabkommen betreffend die Verarbeitung und Übermittlung von Zahlungsverkehrsdaten zu TFTP-Zwecken von der EU an die Vereinigten Staaten; diesem stimmte das Europäische Parlament nicht zu[71]. Auf der Grundlage eines neuen Mandats handelte die Europäische Kommission einen neuen Abkommensentwurf mit den USA aus und unterbreitete dem Rat am 18. Juni 2010 den Vorschlag für einen Beschluss des Rates über den Abschluss des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (EU-USA TFTP-Abkommen)[72]. Das Europäische Parlament stimmte dem Abschluss des Abkommens am

[71] Entschließung des Europäischen Parlaments P7_TA(2010)0029 vom 11.2.2010.

[72] KOM(2010) 316 endgültig/2 vom 18.6.2010.

8. Juli 2010 zu.[73] Es wird nun erwartet, dass der Rat einen Beschluss des Rates zum Abschluss dieses Abkommens annehmen wird, demzufolge das Abkommen dann in Form eines Briefwechsels zwischen beiden Parteien in Kraft tritt. Das EU-USA TFTP-Abkommen bezweckt die Verhinderung, Ermittlung, Aufdeckung und Verfolgung des Terrorismus und der Terrorismusfinanzierung. Anbieter von Zahlungsverkehrsdiensten werden verpflichtet, dem amerikanischen Finanzministerium auf der Grundlage spezifischer geografischer Bedrohungsbewertungen und gezielter Anfragen Zahlungsverkehrsdatensätze zu übermitteln, die unter anderem den Namen, die Kontonummer, Anschrift und Identifikationsnummer des Auftraggebers oder Empfängers der Finanztransaktionen enthalten. Das amerikanische Finanzministerium darf diese Daten ausschließlich zum Zweck des TFTP-Programms und nur dann untersuchen, wenn es Grund zu der Annahme hat, dass eine Person in Verbindung mit dem Terrorismus oder der Terrorismusfinanzierung steht. Gezielte Datensuche und die Übermittlung von Zahlungsverkehrsdaten innerhalb des Einheitlichen Euro-Zahlungsverkehrsraums sind verboten. Die Vereinigten Staaten stellen den EU-Mitgliedstaaten, Europol und Eurojust „lead information" betreffend eventuelle Pläne für Terroranschläge in der EU zur Verfügung und werden die Union dabei unterstützen, ein eigenes dem TFTP entsprechendes Programm einzuführen. Sollte die EU ein solches Programm aufstellen, können beide Seiten die Vereinbarung anpassen. Bevor Daten übertragen werden, wird jedes amerikanische Informationsersuchen von Europol überprüft um sicherzustellen, dass es die Bedingungen des Abkommens erfüllt. Aus Zahlungsverkehrsdaten gewonnene Informationen dürfen nur so lange gespeichert werden, wie dies für einzelne Ermittlungen oder die Strafverfolgung notwendig ist, nicht extrahierte Daten 5 Jahre. Soweit dies für die Ermittlung, Verhinderung oder Verfolgung des Terrorismus oder der Terrorismusfinanzierung notwendig ist, kann das Finanzministerium jegliche personenbezogenen Daten, die aus den Zahlungsverkehrsdaten extrahiert wurden, an die amerikanischen Strafverfolgungsbehörden, Sicherheits- oder Terrorismusbekämpfungs-behörden, EU-Mitgliedstaaten, Europol und Eurojust weitergeben. Ferner kann es, sofern der betroffene Mitgliedstaat zustimmt, mit Drittländern „lead information" über EU-Staatsangehörige und Personen mit Wohnsitz in der EU austauschen. Die Einhaltung der strikt auf die Terrorismusbekämpfung beschränkten Zweckbindung des Abkommens sowie anderer Sicherheitsmaßnahmen wird durch unabhängige Experten, u.a. eine von der Kommission benannte Person, überwacht. Das Abkommen ist fünf Jahre gültig und kann von beiden Seiten gekündigt oder ausgesetzt werden. Eine von der Kommission geleitete Arbeitsgruppe der EU, der Vertreter von zwei Datenschutzbehörden sowie ein Jurist angehören, wird das Abkommen sechs Monate nach seinem Inkrafttreten überprüfen, wobei insbesondere die Einhaltung der Zweckbindung und der Bestimmungen über die Verhältnismäßigkeit sowie der Datenschutzvorschriften bewertet wird. Der Bericht der Kommission wird dem Europäischen Parlament und dem Rat vorgelegt.

2.2. Initiativen im Rahmen des Aktionsplans zur Umsetzung des Stockholmer Programms

Von der Kommission vorzulegende Legislativvorschläge

Im Rahmen des Stockholmer Programms forderte der Europäische Rat die Kommission auf, drei Vorschläge vorzulegen, die für diese Mitteilung von unmittelbarer Relevanz sind: ein PNR-System für die EU zur Verhinderung, Aufdeckung und Verfolgung von Terrorismus und schwerer Kriminalität, ein Ein-/Ausreisesystem und ein Registrierungsprogramm für

[73] Entschließung des Europäischen Parlaments P7_TA-PROV(2010)0279 vom 8.7.2010.

Reisende. Die letzten beiden Vorschläge sollten, so betonte der Europäische Rat, „so bald wie möglich“ vorgelegt werden. Die Kommission hat alle drei Initiativen in den Aktionsplan zur Umsetzung des Stockholmer Programms aufgenommen[74]. Sie beabsichtigt nun, dieser Aufforderung nachzukommen und künftig diese Instrumente auf der Grundlage der in Abschnitt 4 dargelegten Grundsätze der Politikgestaltung zu evaluieren.

Im November 2007 legte die Kommission einen Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von PNR-Daten zu Strafverfolgungszwecken vor[75]. Diese Initiative fand Unterstützung im Rat und wurde später geändert, um den vom Europäischen Parlament vorgeschlagenen Änderungen und den Bemerkungen des Europäischen Datenschutzbeauftragten Rechnung zu tragen. Mit dem Inkrafttreten des Vertrags von Lissabon wurde der Vorschlag hinfällig. Wie im Aktionsplan zur Umsetzung des Stockholmer Programms angegeben, bereitet die Kommission nunmehr ein **Fluggastdaten-Paket** vor, das sie Anfang 2011 vorlegen will und das Folgendes umfasst: eine Mitteilung zu einer externen Fluggastdatenstrategie der EU, in der die wichtigsten Grundsätze für die Verhandlungen über Abkommen mit Drittländern dargelegt werden, Verhandlungsleitlinien für die Neuverhandlung der PNR-Abkommen mit den USA und Australien und Verhandlungsleitlinien für ein neues Abkommen mit Kanada. Außerdem erarbeitet die Kommission derzeit einen neuen PNR-Vorschlag für die EU.

2008 legte die Kommission eine Reihe von Vorschlägen für den Ausbau des integrierten Grenzmanagements im Sinne von Reiseerleichterungen für Drittstaatsangehörige und erhöhter innerer Sicherheit vor[76]. Nachdem sie festgestellt hatte, dass die „Overstayer“ die größte Gruppe der illegalen Migranten in der EU bilden, schlug sie vor, ein **Einreise-/Ausreisesystem** für Drittstaatsangehörige einzuführen, die für kurze Aufenthalte von bis zu drei Monaten in die Union einreisen. Mit diesem System würden Zeitpunkt und Ort der Einreise sowie die zulässige Aufenthaltsdauer gespeichert und automatische Meldungen an die zuständigen Behörden gesandt, mit denen die Personen als „Overstayer“ gekennzeichnet werden. Es beruht auf einer Überprüfung der biometrischen Daten und nutzt das System für den Abgleich biometrischer Daten, das auch im Rahmen von SIS II und VIS zum Einsatz kommt. Die Kommission führt zur Zeit eine Folgenabschätzung durch und wird, wie im Aktionsplan zur Umsetzung des Stockholmer Programms angegeben, den Legislativvorschlag möglichst 2011 vorlegen.

Ein **Registrierungsprogramm für Reisende** (Registered Travellers Programme – RTP) bildet den dritten in Betracht zu ziehenden Vorschlag[77]. Dieses Programm würde es bestimmten Gruppen von Vielreisenden aus Drittländern, die zuvor ein geeignetes „Vorab-Screening“ durchlaufen haben, gestatten, mit vereinfachten Grenzkontrollen und automatischen Kontrollgates in die EU einzureisen. Das RTP würde sich auf eine Identitätsüberprüfung durch den Abgleich biometrischer Daten stützen und die schrittweise Umstellung von allgemeinen Grenzkontrollen auf solche, die das Einzelpersonenrisiko berücksichtigen, ermöglichen. Die Kommission hat eine Folgenabschätzung durchgeführt und wird entsprechend dem Aktionsplan zur Umsetzung des Stockholmer Programms den Legislativvorschlag voraussichtlich 2011 vorlegen.

---

74 Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, Ratsdokument 5731/10 vom 3.3.2010, KOM(2010)171 vom 20.4.2010 (Aktionsplan zur Umsetzung des Stockholmer Programms).

75 KOM(2007) 654 vom 6.11.2007.

76 KOM(2008) 69 vom 13.2.2008.

77 KOM(2008) 69 vom 13.2.2008.

Von der Kommission zu prüfende Initiativen

Im Rahmen des Stockholmer Programms forderte der Europäische Rat die Kommission auf, drei Vorschläge zu prüfen, die für diese Mitteilung von unmittelbarer Relevanz sind: Möglichkeiten der Verfolgung der Terrorismusfinanzierung in der EU, Möglichkeit und Nützlichkeit der Entwicklung eines Systems zur elektronischen Erteilung von Reisebewilligungen und Notwendigkeit und Zusatznutzen der Einrichtung eines Europäischen Kriminalaktennachweises. Die Kommission hat diese Initiativen ebenfalls in den Aktionsplan zur Umsetzung des Stockholmer Programms aufgenommen. Sie wird nun die Durchführbarkeit dieser Initiativen prüfen und entscheiden, ob sie und gegebenenfalls auf welche Weise sie auf der Grundlage der in Abschnitt 4 dargelegten Grundsätze der Politikgestaltung weiterverfolgt werden.

Das EU-USA TFTP-Abkommen sieht vor, dass die Europäische Kommission eine Studie über die eventuelle Einführung eines **EU-Programms zum Aufspüren der Finanzierung des Terrorismus** entsprechend dem amerikanischen TFTP durchführen wird, mit dem eine gezieltere Übermittlung von Daten aus der EU in die USA möglich wird. Im Entwurf des Beschlusses des Rates über den Abschluss dieses Abkommens wird die Kommission ferner aufgefordert, dem Europäischen Parlament und dem Rat spätestens ein Jahr nach dem Inkrafttreten des EU-USA TFTP-Abkommens einen rechtlichen und technischen Rahmen für die Extraktion der Daten auf dem Gebiet der EU vorzulegen.[78] Die Kommission ist verpflichtet, innerhalb von drei Jahren nach Inkrafttreten des Abkommens einen Fortschrittsbericht über die Entwicklung eines solchen vergleichbaren EU-Systems vorzulegen. Sollte das System fünf Jahre nach Inkrafttreten des Abkommens noch nicht eingerichtet sein, kann die EU beschließen, das Abkommen zu beenden. Gemäß dem EU-USA TFTP-Abkommen sind die USA ferner verpflichtet, mit der EU zusammenzuarbeiten und sie zu unterstützen und zu beraten, falls die EU beschließt, ein solches System einzuführen. Ohne der Entscheidung vorzugreifen, hat die Kommission damit begonnen, das Projekt im Hinblick auf Datenschutz, Ressourcen und die praktischen Auswirkungen zu prüfen. Wie im Aktionsplan zur Umsetzung des Stockholmer Programms angegeben, wird die Kommission 2011 eine Mitteilung über die Durchführbarkeit der Einführung des EU-Programms zum Aufspüren der Finanzierung des Terrorismus (EU TFTP) vorlegen.

Die Kommission schlug in ihrer Mitteilung von 2008 über das integrierte Grenzmanagement die mögliche Einführung eines **Systems zur elektronischen Erteilung von Reisebewilligungen** (ESTA) für Drittstaatsangehörige vor, die keiner Visumpflicht unterliegen[79]. Im Rahmen dieses Programms müssten die betreffenden Drittstaatsangehörigen einen elektronischen Antrag stellen, wobei sie vor Reiseantritt Angaben zur Person, Pass- und Reisedaten eingeben. Im Vergleich zum Visumverfahren böte ESTA eine schnellere und einfachere Methode der Überprüfung, ob die Person die Einreisebedingungen erfüllt. Die Kommission führt derzeit eine Studie über die Vorteile, Nachteile und praktischen Folgen der Einführung von ESTA durch. Wie im Aktionsplan zur Umsetzung des Stockholmer Programms angegeben, wird die Kommission 2011 eine Mitteilung über die Durchführbarkeit dieses Programms vorlegen.

---

78 Ratsdokument 11222/1/10 REV 1 vom 24.6.2010; Ratsdokument 11222/1/10 REV1 COR1 vom 24.6.2010.

79 KOM(2008) 69 vom 13.2.2008.

Während seines Ratsvorsitzes eröffnete Deutschland 2007 eine Diskussion über die mögliche Einführung eines **Europäischen Kriminalaktennachweises** (EPRIS)[80]. EPRIS würde die Strafverfolgungsbehörden dabei unterstützen, Informationen in der EU aufzufinden, insbesondere, was Verbindungen zwischen Personen anbelangt, die der organisierten Kriminalität verdächtigt werden. Die Kommission wird dem Rat 2010 einen Entwurf der Aufgabenbeschreibung für ihre Durchführbarkeitsstudie betreffend EPRIS unterbreiten. Wie im Aktionsplan zur Umsetzung des Stockholmer Programms angegeben, wird die Kommission möglichst 2012 eine Mitteilung über die Durchführbarkeit der Einrichtung dieses Systems vorlegen.

3. ANALYSE DER GELTENDEN, IN DER UMSETZUNG BEGRIFFENEN UND IN BETRACHT GEZOGENEN INSTRUMENTE

Der obige Überblick gibt Anlass zu folgenden Vorbemerkungen:

Dezentrale Struktur

Von den zahlreichen Instrumenten, die derzeit Anwendung finden, in der Umsetzung begriffen sind oder in Betracht gezogen werden, dienen nur sechs der Erhebung und Speicherung personenbezogener Daten auf EU-Ebene: SIS (und SIS II), VIS, EURODAC, ZIS, Europol und Eurojust. Alle anderen Instrumente regeln den dezentralen grenzübergreifenden Austausch oder die Übermittlung von personenbezogenen Informationen, die auf nationaler Ebene durch staatliche Behörden oder Privatunternehmen erhoben werden, an Drittländer. Die meisten personenbezogenen Daten werden auf nationaler Ebene erhoben und gespeichert. Die EU versucht einen Zusatznutzen zu schaffen, indem sie unter bestimmten Bedingungen den Austausch dieser Daten mit EU-Partnern und Drittländern ermöglicht. Die Kommission hat dem Europäischen Parlament und dem Rat kürzlich einen geänderten Vorschlag zur Errichtung einer Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht unterbreitet[81]. Die künftige IT-Agentur gewährleistet das Betriebsmanagement von SIS II, VIS und EURODAC sowie künftiger IT-Systeme im Bereich Freiheit, Sicherheit und Recht und stellt den laufenden Betrieb der Systeme sowie einen ununterbrochenen Informationsfluss sicher.

Zweckbindung

Die meisten der oben dargestellten Instrumente haben eine einzige Zweckbestimmung: bei EURODAC geht es um eine verbesserte Funktionsweise des Dublin-Systems; mit API sollen die Grenzkontrollen verbessert werden; die schwedische Initiative dient der Verbesserung strafrechtlicher Ermittlungen und polizeilicher Erkenntnisgewinnungsverfahren; das Übereinkommen Neapel II dient der Verhinderung, Aufdeckung, Verfolgung und Sanktionierung des Zollbetrugs; beim ZIS geht es um die Verhinderung, Ermittlung und Verfolgung schwerwiegender Verstöße gegen die nationalen Gesetze durch eine wirksamere Zusammenarbeit zwischen den nationalen Zollbehörden; ECRIS, FIU und ARO sollen den grenzübergreifenden Datenaustausch in bestimmten Bereichen rationalisieren, und der Prüm-Beschluss, die Richtlinie zur Vorratsdatenspeicherung, TFTP und PNR dienen der Bekämpfung von Terrorismus und schwerer Kriminalität. SIS, SIS II und VIS sind die wichtigsten Ausnahmen: Die ursprüngliche Zweckbestimmung des VIS war der

[80] Siehe Ratsdokument 15526/1/09 vom 2.12.2009.
[81] KOM(2010) 93 vom 19.3.2010.

grenzübergreifende Austausch von Visadaten, was später auf die Verhinderung und Bekämpfung des Terrorismus und schwerer Kriminalität ausgedehnt wurde. SIS und SIS II sollen ein hohes Sicherheitsniveau im Raum der Freiheit, der Sicherheit und des Rechts gewährleisten und den Personenverkehr anhand der über dieses System ausgetauschten Informationen erleichtern. Mit Ausnahme dieser zentralisierten Informationssysteme ist die Zweckbindung anscheinend ein Hauptmerkmal des Informationsmanagements auf EU-Ebene.

Mögliche Funktionsüberschneidungen

Dieselben personenbezogenen Daten können im Rahmen unterschiedlicher Instrumente erhoben, jedoch im Rahmen eines einzelnen Instruments jeweils nur einem beschränkten Zweck zugeführt werden (eine Ausnahme bilden das VIS, SIS und SIS II). Beispielsweise können die Angaben zu einer Person einschließlich des Namens, Geburtsdatums und –orts und der Staatsangehörigkeit mit SIS, SIS II, VIS, API, ZIS, der schwedischen Initiative, dem Prüm-Beschluss, ECRIS, FIU, ARO, Europol, Eurojust, PNR- und TFTP-Abkommen verarbeitet werden. Allerdings dürfen diese Daten im Fall von API nur zum Zweck der Grenzkontrolle verarbeitet werden, beim ZIS nur zur Verhinderung, Ermittlung und Verfolgung des Zollbetrugs, im Rahmen der schwedischen Initiative nur für strafrechtliche Ermittlungen und polizeiliche Erkenntnisgewinnungsverfahren, unter dem Prüm-Beschluss nur für die Verhinderung des Terrorismus und grenzübergreifender Kriminalität, bei ECRIS zur Überprüfung des kriminellen Hintergrunds einer Person, bei FIU zur Untersuchung der Verbindungen einer Person zum organisierten Verbrechen und zu Terrornetzwerken, bei ARO zum Aufspüren von Erträgen aus Straftaten, bei Europol und Eurojust zur Ermittlung und Unterstützung der Verfolgung schwerer grenzübergreifender Kriminalität, bei PNR zur Verhütung und Bekämpfung des Terrorismus und anderer Formen schwerer grenzüberschreitender Kriminalität und zum Aufspüren und Verfolgen von Terroristen und ihren finanziellen Helfern bei TFTP. Biometrische Daten wie Fingerabdrücke und Fotografien können im Rahmen von SIS II, VIS, EURODAC, der schwedischen Initiative, dem Prüm-Beschluss, ECRIS, Europol und Eurojust verarbeitet werden – jeweils zu dem begrenzten Zweck der Maßnahme. Der Prüm-Beschluss ist das einzige Instrument, das den grenzübergreifenden Austausch anonymer DNA-Profile ermöglicht (allerdings können diese Daten auch an Europol und Eurojust weitergeleitet werden). Im Rahmen anderer Maßnahmen werden hochspezialisierte personenbezogene Informationen entsprechend ihrer jeweiligen Zweckbestimmung verarbeitet: Bei den PNR-Systemen sind dies die Buchungsangaben der Fluggäste, bei FIDE die zur Ermittlung von Zollbetrug erforderlichen Daten, bei der Richtlinie über Vorratsdatenspeicherung die IP-Adresse und Mobiltelefon-Gerätenummer, bei ECRIS Strafregisterauszüge, bei ARO Privatvermögen und Angaben zum Unternehmen, bei Cybercrime-Plattformen Internet-Straftaten, bei Europol Verbindungen zu kriminellen Netzwerken und beim TFTP Zahlungsverkehrsdaten. Die einzige wesentliche Funktionsüberschneidung betrifft den grenzübergreifenden Austausch von Informationen und Erkenntnissen bei strafrechtlichen Ermittlungen. Aus rechtlicher Sicht würde die schwedische Initiative ausreichen, *jede* Art von Information auszutauschen, die für solche Ermittlungen relevant ist (sofern der Austausch dieser personenbezogenen Daten nach dem nationalen Recht zulässig ist). Aus dem operativen Blickwinkel könnte der Prüm-Beschluss allerdings für den Austausch von DNA-Profilen und Fingerabdruckdaten vorzuziehen sein, da sein „Treffer/kein Treffer"-System eine sofortige Antwort und der automatische Datenaustausch ein Höchstmaß an Datensicherheit gewährleistet[82]. Ebenso könnte es für FIU, ARO und

[82] Zum Prüm-Beschluss (Beschluss 2008/615/JI des Rates, ABl. L 210 vom 6.8.2008, S. 1) gibt es einen Durchführungsbeschluss (Beschluss 2008/616/JI des Rates, ABl. L 210 vom 6.8.2008, S. 12), mit dem

Cybercrime-Plattformen wirksamer sein, direkt mit ihren EU-Ansprechpartnern in Verbindung zu treten, anstatt die Formulare der schwedischen Initiative auszufüllen, um Informationen anzufordern.

Kontrollierte Zugriffsrechte

Bei Instrumenten, die zur Bekämpfung des Terrorismus und schwerer Kriminalität konzipiert wurden, sind die Zugriffsrechte gewöhnlich auf eine engere Definition von Strafverfolgungsinstanzen, d.h. auf die Polizei, den Grenzschutz und die Zollbehörden begrenzt. Die Zugriffsrechte bei Maßnahmen, die aufgrund von Schengen entstanden sind, werden normalerweise den Einwanderungsbehörden und, unter bestimmten Bedingungen, der Polizei, dem Grenzschutz und den Zollbehörden gewährt. Der Informationsfluss wird im Fall der zentralisierten SIS und VIS durch nationale Schnittstellen und bei den dezentralen Instrumenten wie dem Prüm-Beschluss, der schwedischen Initiative, dem Übereinkommen Neapel II, ECRIS, TFTP, den PNR-Abkommen, FIU, ARO und Cybercrime-Plattformen durch nationale Kontaktstellen oder zentrale Koordinierungseinheiten kontrolliert.

Variable Regeln für die Vorratsdatenspeicherung

Die Speicherfristen sind entsprechend dem Ziel der verschiedenen Instrumente sehr unterschiedlich. Das PNR-Abkommen mit den Vereinigten Staaten sieht die längste Speicherfrist vor: 15 Jahre, das API die kürzeste: 24 Stunden. Mit den PNR-Abkommen wird eine interessante Unterscheidung zwischen aktiv und passiv verwendeten Daten getroffen: Nach Ablauf einer bestimmten Frist muss die Information archiviert werden und kann nur mit einer Sondergenehmigung „entriegelt“ werden. Ein gutes Beispiel ist die Verwendung von PNR-Daten aus der EU durch Kanada: Die Information muss nach 72 Stunden anonymisiert werden, bleibt jedoch für ermächtigte Beamte dreieinhalb Jahre lang verfügbar.

Wirksames Identitätsmanagement

Einige der genannten Maßnahmen, z.B. das künftige SIS II und das VIS, sollen durch die Verwendung biometrischer Daten eine Identitätsüberprüfung ermöglichen. Es wird erwartet, dass sich die Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts durch die Einführung von SIS II erhöht, indem beispielsweise Personen, für die ein Europäischer Haftbefehl ausgestellt wurde, denen die Einreise in den Schengen-Raum verweigert wird oder die aus anderen ermittlungstechnischen Gründen (z.B. vermisste Personen oder Zeugen vor Gericht) gesucht werden, unabhängig vom Vorliegen oder von der Echtheit von Ausweispapieren identifiziert werden können. Die Einführung des VIS dürfte das Verfahren der Visumerteilung erleichtern.

Datensicherheit durch EU-Lösungen

Für den Austausch sensibler Informationen über die europäischen Grenzen hinweg ziehen die Mitgliedstaaten EU-Lösungen vor. Einige Instrumente unterschiedlicher Größe, Struktur und Zweckbestimmung beruhen auf dem von der Kommission finanzierten s-TESTA-Datenkommunikationsnetz für den Austausch sensibler Informationen. Dazu zählen das

---

dem jeweiligen Stand der Technik entsprechende Maßnahmen für den Datenschutz und die Datensicherheit sowie die Verschlüsselung und Genehmigungsverfahren für den Zugriff auf die Daten gewährleistet werden sollen und in dem spezifische Regeln für die Zulässigkeit von Suchvorgängen festlegt werden.

zentralisierte SIS II, VIS und EURODAC, ferner das dezentrale System nach dem Beschluss von Prüm, die Instrumente ECRIS und FIU sowie Europol und Eurojust. ZIS und FIDE benutzen das Gemeinsame Kommunikationsnetz, die Gemeinsame Systemschnittstelle oder den sicheren Internetzugang der Kommission. In der Zwischenzeit scheint die Datenaustauschanwendung SIENA von Europol für einige neuere Initiativen, die sich auf die sichere Datenübermittlung stützen, die Anwendung der Wahl geworden zu sein: Derzeit wird diskutiert, FIU.net, ARO und die Cybercrime-Meldeplattformen auf der Grundlage dieser Anwendung zu betreiben.

Unterschiedliche Überprüfungsmechanismen

Die vorstehend beschriebenen Instrumente sehen eine Reihe unterschiedlicher Überprüfungsmechanismen vor. Im Fall komplexer Informationssysteme wie SIS II, VIS und EURODAC muss die Kommission dem Europäischen Parlament und dem Rat jährliche oder halbjährliche Berichte über den Betrieb dieser Systeme oder den Stand ihrer Umsetzung vorlegen. Bei dezentralen Datenübermittlungsinstrumenten muss die Kommission den anderen Organen einige Jahre nach deren Inbetriebnahme einen einmaligen Evaluierungsbericht vorlegen. Die Richtlinie über Vorratsdatenspeicherung, die schwedische Initiative und die ARO-Maßnahmen müssen 2010 bewertet werden, der Prüm-Beschluss 2012 und ECRIS 2016. In den drei PNR-Abkommen sind regelmäßige und Ad-hoc-Überprüfungen vorgesehen; zwei von ihnen beinhalten Beendigungsklauseln. Europol und Eurojust legen dem Rat jährliche Berichte vor, die dieser zur Kenntnisnahme an das Europäische Parlament weiterleitet. Diese Überlegungen lassen darauf schließen, dass die derzeitige Struktur des Informationsmanagements in der EU der Annahme eines einzigen Bewertungsmechanismus für sämtliche Instrumente nicht förderlich ist. In Anbetracht dieser Unterschiede müssen bei künftigen Änderungen eines Informationsmanagementinstruments ihre mögliche Auswirkung auf alle anderen Maßnahmen berücksichtigt werden, die die Erhebung, Speicherung oder den Austausch personenbezogener Daten im Bereich Freiheit, Sicherheit und Recht regeln.

4. GRUNDSÄTZE FÜR DIE POLITIKGESTALTUNG

In Abschnitt 2 wurden verschiedene Initiativen beschrieben, die die Europäische Kommission in den letzten Jahren umgesetzt, vorgelegt oder in Erwägung gezogen hat. Allein schon die Zahl der neuen Ideen und der zunehmende Gesamtumfang der Rechtsakte im Bereich innere Sicherheit und Migrationssteuerung verlangen nach der Definition einer Reihe von Grundsätzen, die in den kommenden Jahren als Maßstab für die Einleitung und Evaluierung entsprechender Vorschläge dienen können. Diese Grundsätze basieren auf den allgemeinen Prinzipien der EU-Verträge, der Rechtsprechung des Europäischen Gerichtshofs und des Europäischen Gerichtshofs für Menschenrechte sowie den einschlägigen interinstitutionellen Vereinbarungen zwischen dem Europäischen Parlament, dem Rat und der Europäischen Kommission und ergänzen sie. Die Kommission schlägt für die Entwicklung und Umsetzung neuer Initiativen und die Evaluierung geltender Instrumente zwei Arten von Grundsätzen vor:

Materiellrechtliche Grundsätze

Schutz der Grundrechte, insbesondere des Rechts auf Privatsphäre und Datenschutz

Der Schutz der Grundrechte, wie sie in der Charta der Grundrechte der Europäischen Union niedergelegt sind, vor allem des Rechts auf Privatsphäre und des Schutzes der personenbezogenen Daten, ist für die Kommission bei der Entwicklung neuer Vorschläge, bei

denen es um die Verarbeitung personenbezogener Daten im Bereich der inneren Sicherheit oder der Migrationssteuerung geht, ein wichtiges Anliegen. Nach Artikel 7 und 8 der Charta hat jede Person „das Recht auf Achtung ihres Privat- und Familienlebens“ und „das Recht auf Schutz der sie betreffenden personenbezogenen Daten“[83]. Auch in Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der für die Tätigkeit der Mitgliedstaaten, der EU-Organe, -Agenturen und -Einrichtungen bindend ist, ist das Recht jeder Person „auf Schutz der sie betreffenden personenbezogenen Daten“ verankert[84]. Beim Entwurf neuer Instrumente, in deren Rahmen Informationstechnologie zum Einsatz kommt, wird sich die Kommission nach Möglichkeit auf das Konzept des „eingebauten Datenschutzes“ („privacy by design“) stützen. Das bedeutet, dass der Schutz personenbezogener Daten in die technische Grundlage des vorgeschlagenen Instruments eingebettet und so die Datenverarbeitung auf das für den angestrebten Zweck erforderliche Mindestmaß begrenzt wird, wobei nur die Instanzen Zugriff auf die Daten haben, die die Daten benötigen[85].

Notwendigkeit

Die Beeinträchtigung des Rechtes einer Person auf ihre Privatsphäre durch eine staatliche Behörde kann im Interesse der nationalen oder öffentlichen Sicherheit oder der Kriminalitätsvorbeugung notwendig sein[86]. Der Europäische Gerichtshof für Menschenrechte hat drei Bedingungen herausgearbeitet, unter denen solche Beeinträchtigungen gerechtfertigt sein können: Der Eingriff muss rechtmäßig sein, mit ihm muss ein legitimes Ziel verfolgt werden, und er muss in einer demokratischen Gesellschaft notwendig sein. Ein Eingriff in das Recht auf Privatsphäre gilt dann als notwendig, wenn er einem zwingenden gesellschaftlichen Erfordernis entspricht, wenn er im Vergleich zu dem verfolgten Ziel verhältnismäßig ist und wenn die staatlichen Behörde den Eingriff „ausreichend begründet“[87]. Bei allen künftigen Vorschlägen in diesem Bereich wird die Kommission die erwarteten Auswirkungen auf die Rechte des Einzelnen auf Privatsphäre und auf den Schutz der personenbezogenen Daten abschätzen und darlegen, warum die Maßnahme notwendig und die vorgeschlagene Lösung im Vergleich zum legitimen Ziel der Aufrechterhaltung der inneren Sicherheit in der Europäischen Union, zur Verhütung von Straftaten und für die Migrationssteuerung verhältnismäßig ist. Die Einhaltung der Vorschriften über den Schutz personenbezogener Daten wird in jedem Fall der Kontrolle durch eine unabhängige Instanz auf nationaler oder EU-Ebene unterliegen.

Subsidiarität

Die Kommission wird ihre neuen Vorschläge gemäß Artikel 5 des Protokolls Nr. 2 im Anhang zum Vertrag über die Europäische Union im Hinblick auf die Grundsätze der Subsidiarität und Verhältnismäßigkeit begründen. Jeder neue Legislativvorschlag wird eine Erklärung enthalten, anhand derer nach Maßgabe von Artikel 5 des Vertrags über die

---

83 Charta der Grundrechte der Europäischen Union, ABl. C 83 vom 30.3.2010, S. 389.

84 Konsolidierte Fassung des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union, ABl. C 83 vom 30.3.2010, S. 1.

85 Eine umfassende Beschreibung des „eingebauten Datenschutzes“ siehe Stellungnahme des Europäischen Datenschutzbeauftragten über die Vertrauensförderung in der Informationsgesellschaft durch die Förderung des Datenschutzes und des Rechts auf Privatsphäre vom 18.3.2010.

86 Siehe Artikel 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (ETS Nr. 5), Europarat, 4.11.1950.

87 Siehe *Marper / Vereinigtes Königreich*, Europäischer Gerichtshof für Menschenrechte, Straßburg, 4.12.2008.

Europäische Union die Einhaltung des Grundsatzes der Subsidiarität geprüft werden kann. Diese Erklärung besteht aus einer Bewertung der finanziellen, wirtschaftlichen und sozialen Auswirkungen des Vorschlags, und, im Fall einer Richtlinie, der Auswirkungen hinsichtlich der von den Mitgliedstaaten einzuführenden Vorschriften[88]. Dass ein Ziel der Union besser auf EU-Ebene erreicht werden kann, muss anhand qualitativer Indikatoren nachgewiesen werden. Bei den Legislativvorschlägen ist darauf zu achten, dass der Verwaltungsaufwand für die Union, die Regierungen der Mitgliedstaaten, die regionalen Behörden, die Wirtschaft und die Bürger so gering wie möglich gehalten wird und in einem angemessenen Verhältnis zu dem angestrebten Ziel steht. Bei Vorschlägen, die neue internationale Übereinkünfte erfordern, erstreckt sich die Erklärung auch auf die voraussichtlichen Auswirkungen des Vorschlags auf die Beziehungen mit den betreffenden Drittländern.

Sorgfältiges Risikomanagement

Im Bereich Freiheit, Sicherheit und Recht werden Informationen üblicherweise ausgetauscht, um Bedrohungen für die Sicherheit zu analysieren, die Entwicklung krimineller Aktivität zu erfassen oder Risiken in verbundenen Politikbereichen abzuschätzen[89]. Risiken stehen häufig, aber nicht ausschließlich, im Zusammenhang mit Personen, deren früheres Verhalten oder Verhaltensmuster auf ein anhaltendes Risiko in der Zukunft schließen lassen. Allerdings sollten Risiken auf Nachweisen beruhen und nicht hypothetisch sein. Die Überprüfung der Notwendigkeit und die Zweckbindung sind für jede Maßnahme des Informationsmanagements unerlässlich. Hierbei spielt die Entwicklung von Risikoprofilen, die nicht mit dem gegen die Grundrechte verstoßenden Erstellen von rassistischen oder anderweitig diskriminierenden Profilen verwechselt werden darf, eine Rolle. Diese Profile können dazu beitragen, die Ressourcen zur Erfassung von Sicherheitsrisiken und zum Schutz der Verbrechensopfer auf bestimmte Personen zu bündeln.

Prozessorientierte Grundsätze[90]

Kostenwirksamkeit

Öffentliche Dienstleistungen auf der Grundlage der Informationstechnologie sollten qualitativ besser und für den Steuerzahler von höherem Wert sein. Angesichts des derzeitigen wirtschaftlichen Umfelds müssen alle neuen Vorschläge, vor allem solche, die sich auf die Einführung oder den Ausbau von Informationssystemen beziehen, möglichst kostenwirksam sein. Daher werden schon bestehende Lösungen berücksichtigt, um Überschneidungen weitgehend auszuschließen und mögliche Synergien auszubauen. Die Kommission wird prüfen, ob die Ziele eines Vorschlags durch eine bessere Nutzung bestehender Instrumente erreicht werden können. Ferner wird sie in Betracht ziehen, bestehende Informationssysteme durch Hilfsfunktionen zu ergänzen, bevor sie neue Systeme vorschlägt.

---

88 Die Grundsätze der Folgenabschätzungen sind in den Leitlinien der Europäischen Kommission für Folgenabschätzungen niedergelegt (SEK(2009)92 vom 15.1.2009).

89 Ein praktisches Beispiel für eine erfolgreiche Gefahrenabwehr wäre z.B., wenn eine Person, die in einem Mitgliedstaat eine schwere Straftat begangen hat, daran gehindert wird, über einen anderen Mitgliedstaat erneut in den Schengen-Raum einzureisen (SIS) oder wenn eine Person daran gehindert wird, in mehreren Mitgliedstaaten Asylanträge zu stellen (EURODAC).

90 Diese Grundsätze beruhen auf den Schlussfolgerungen des Rates zu einer Strategie für das Informationsmanagement im Bereich der inneren Sicherheit in der EU, Ratstagung Justiz und Inneres vom 30.11.2009.

Politikgestaltung nach dem Bottom-up-Prinzip

Die Entwicklung neuer Initiativen muss so früh wie möglich Beiträge aller betroffenen Interessengruppen einschließlich der für die Umsetzung zuständigen nationalen Behörden, Wirtschaftsteilnehmer und der Zivilgesellschaft einbeziehen. Die Gestaltung einer Politik, die den Interessen der Endnutzer Rechnung trägt, erfordert horizontales Denken und eine umfassende Konsultation[91]. Aus diesem Grund wird die Kommission danach streben, durch Ratsstrukturen, Managementausschüsse und Ad-hoc-Gremien den ständigen Austausch mit nationalen Beamten und Fachleuten sicherzustellen.

Klare Zuständigkeiten

In Anbetracht der technischen Komplexität von Projekten zu Informationserhebung und -austausch im Bereich Freiheit, Sicherheit und Recht muss der anfänglichen Gestaltung der Governance-Strukturen besondere Aufmerksamkeit geschenkt werden. Die Erfahrung mit SIS II zeigt, dass das frühzeitige Fehlen klarer und stabiler übergreifender Ziele, Rollen und Zuständigkeiten zu erheblichen Kostenüberschreitungen und Verzögerungen bei der Umsetzung führen kann. Eine erste Bewertung der Umsetzung des Prüm-Beschlusses lässt erkennen, dass eine dezentrale Governance-Struktur vielleicht auch kein Allheilmittel ist, da die Mitgliedstaaten keinen Projektleiter haben, an den sie sich hinsichtlich finanzieller oder technischer Aspekte der Umsetzung wenden und von dem sie sich beraten lassen können. Die künftige IT-Agentur kann den Betreuern von Informationssystemen im Bereich Freiheit, Sicherheit und Recht vielleicht solche Beratung anbieten. Sie kann auch eine Plattform für die Einbeziehung einer Vielzahl von Interessengruppen in das Betriebsmanagement und die Entwicklung von IT-Systemen bieten. Als mögliche Absicherung gegen Kostenüberschreitungen und Verzögerungen, die auf geänderte Anforderungen zurückzuführen sind, wird jegliches neue Informationssystem im Bereich Freiheit, Sicherheit und Recht – vor allem, wenn es IT-Großsysteme zum Gegenstand hat – nicht entwickelt, solange die grundlegenden Rechtsinstrumente, in denen Zweck, Anwendungsbereich, Funktion und technische Einzelheiten festgelegt sind, nicht endgültig angenommen wurden.

Überprüfungs- und Beendigungsklauseln

Die Kommission wird jedes in dieser Mitteilung angeführte Instrument vor dem Hintergrund sämtlicher im Bereich des Informationsmanagements bestehenden Instrumente bewerten. Dies dürfte ein zuverlässiges Bild ergeben, wie sich die einzelnen Instrumente in den Gesamtzusammenhang der inneren Sicherheit und der Migrationssteuerung einfügen. Künftige Vorschläge werden gegebenenfalls eine jährliche Berichterstattungspflicht, regelmäßige und Ad-hoc-Überprüfungen sowie eine Beendigungsklausel beinhalten. Bestehende Instrumente bleiben nur in Kraft, wenn sie weiter dem rechtmäßigen Zweck dienen, zu dem sie geschaffen wurden. Anhang II enthält für jedes in dieser Mitteilung angeführte Instrument Überprüfungsdatum und –mechanismus.

5. AUSBLICK

Diese Mitteilung bietet zum ersten Mal einen klaren und vollständigen Überblick über die schon bestehenden, noch in der Umsetzung begriffenen oder in Betracht gezogenen

[91] Für die allgemeinen Grundsätze und Mindestnormen für öffentliche Anhörungen siehe KOM(2002)704 vom 11.12.2002.

Maßnahmen auf EU-Ebene, mit denen die Erhebung, Speicherung und der grenzübergreifende Austausch personenbezogener Daten zu Zwecken der Strafverfolgung und der Migrationssteuerung geregelt wird.

Sie bietet den Bürgern einen Überblick darüber, welche Informationen über sie erhoben, gespeichert und ausgetauscht werden, und zu welchem Zweck und durch wen dies geschieht. Sie bildet ein transparentes Referenzdokument für die Interessengruppen, die sich in die Diskussion über die künftige Richtung der EU-Politik in diesem Bereich einschalten möchten. Zugleich ist dieses Papier eine erste Antwort auf die Aufforderung des Europäischen Rates, gemäß der EU-Strategie für das Informationsmanagement[92] entsprechende Instrumente für das Informationsmanagement auf EU-Ebene zu entwickeln und über das Erfordernis eines europäischen Modells für den Informationsaustausch[93] nachzudenken.

Die Kommission beabsichtigt, dieser Mitteilung im Jahr 2012 eine Mitteilung über das europäische Modell für den Informationsaustausch folgen zu lassen[94]. Zu diesem Zweck leitete die Kommission im Januar 2010 ein „information mapping" über die Rechtsgrundlagen und den praktischen Ablauf des Austauschs von polizeilichen Erkenntnissen und Informationen zwischen den Mitgliedstaaten ein, dessen Ergebnisse die Kommission dem Rat und dem Europäischen Parlament im Jahr 2011 vorlegen möchte[95].

Ferner gibt diese Mitteilung erstmals die Sicht der Kommission im Hinblick auf die allgemeinen Grundsätze wieder, die sie bei der künftigen Entwicklung von Instrumenten für die Erhebung, Speicherung und den Austausch von Daten zugrunde legen will. Diese Grundsätze dienen zugleich der Bewertung der bestehenden Instrumente. Die Annahme eines solchen auf Grundsätze gestützten Konzepts für die Entwicklung und Bewertung der Maßnahmen wird Kohärenz und Wirksamkeit der derzeitigen und künftigen Instrumente voraussichtlich so erhöhen, dass die Grundrechte der Bürger in vollem Umfang gewahrt werden.

---

92 Schlussfolgerungen des Rates zu einer Strategie für das Informationsmanagement im Bereich der inneren Sicherheit in der EU, Ratstagung Justiz und Inneres vom 30.11.2009 (EU-Strategie für das Informationsmanagement).

93 Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, Ratsdokument 5731/10 vom 3.3.2010, Abschnitt 4.2.2.

94 Dies ist im Aktionsplan zur Umsetzung des Stockholmer Programms (KOM(2010)171 vom 20.4.2010 angegeben.

95 Dieses „information mapping“ wird in enger Zusammenarbeit mit einem entsprechenden Projektteam aus Vertretern der EU und der EFTA-Staaten, von Europol, Eurojust, Frontex und dem europäischen Datenschutzbeauftragten durchgeführt.

ANHANG I

Die folgenden Beispielfälle und Zahlen veranschaulichen die praktische Anwendung derzeit eingesetzter Informationsmanagementmaßnahmen .

Schengener Informationssystem (SIS)

Gesamtzahl der in der zentralen SIS (C.SIS)-Datenbank erfassten SIS-Ausschreibungen[96]

Ausschreibungskategorien	**2007**	**2008**	**2009**
Banknoten	177 327	168 982	134 255
Blankodokumente	390 306	360 349	341 675
Schusswaffen	314 897	332 028	348 353
Ausgestellte Dokumente	17 876 227	22 216 158	25 685 572
Fahrzeuge	3 012 856	3 618 199	3 889 098
Gesuchte Personen (Aliasnamen)	299 473	296 815	290 452
Gesuchte Personen (Hauptname)	859 300	927 318	929 546
Davon:			
Zwecks Verhaftung und Auslieferung gesuchte Personen	19 119	24 560	28 666
Drittstaatsangehörige mit Einreiseverbot	696 419	746 994	736 868
Vermisste Erwachsene	24 594	23 931	26 707
Vermisste Minderjährige	22 907	24 628	25 612
Zeugen oder vor Gericht geladene Personen	64 684	72 958	78 869
Personen, die zur Abwehr von Gefahren für die öffentliche Sicherheit unter besonderer Beobachtung stehen	31 568	34 149	32 571
Personen, die zur Abwehr von Gefahren für die nationale Sicherheit unter besonderer Beobachtung stehen	9	98	253
Insgesamt	**22 933 370**	**27 919 849**	**31 618 951**

[96] Ratsdokument 6162/10 vom 5.2.2010; Ratsdokument 5764/09 vom 28.1.2009; Ratsdokument 5441/08 vom 30.1.2008.

EURODAC – Migrationsbewegung von Asylbewerbern, die in demselben Mitgliedstaat oder in anderen Mitgliedstaaten erneut Anträge gestellt haben (2008)

Mitgliedstaaten, die zum Datenabgleich Fingerabdrücke übermitteln und für die Mitgliedstaaten (Spalten), in denen eine Person bereits zuvor Asyl beantragt hatte, "Treffer" erzielen	Mitgliedstaat, in dem der erste Asylantrag gestellt wurde[97]																													Gesamtzahl der zweiten Anträge	
	AT	BE	BG	CH	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IS	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	UK	**Inlandstreffer**	**Treffer insgesamt**
AT	1 725	74	2	0	1	87	274	5	2	31	12	25	115	212	5	0	134	3	14	0	9	52	49	1 371	1	42	111	17	260	61	**1 725**	**4 694**
BE	180	5 450	4	0	3	38	408	17	0	41	17	28	378	67	28	0	69	3	37	0	2	180	73	625	6	3	192	17	58	205	**5 450**	**8 129**
BG	5	2	116	0	1	1	5	1	0	7	0	0	0	1	0	0	1	0	2	0	0	1	3	0	0	6	8	0	0	4	**116**	**164**
CH	32	52	1	4	3	5	35	0	0	17	17	8	39	19	1	0	355	0	1	0	13	15	37	3	1	0	41	4	4	25	**4**	**732**
CY	1	0	0	0	68	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**68**	**73**
CZ	55	12	0	0	0	637	48	4	0	0	3	4	13	0	1	0	8	2	1	0	0	7	6	17	1	0	13	0	1	6	**637**	**839**
DE	260	268	12	0	4	79	1 852	42	0	174	39	56	256	106	9	2	200	5	26	2	5	174	137	149	4	43	567	30	89	128	**1 852**	**4 718**
DK	44	43	3	0	0	13	126	119	0	27	13	44	36	13	4	0	47	0	7	0	0	30	225	55	2	4	436	2	7	41	**119**	**1 341**
EE	0	0	0	0	0	0	1	1	0	0	0	8	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3	0	0	9	**0**	**23**
EL	66	88	27	0	12	9	131	10	0	766	8	8	35	3	9	0	48	0	1	0	0	33	24	3	0	13	141	0	8	316	**766**	**1 759**
ES	16	18	2	0	1	3	37	1	0	11	108	0	29	4	5	0	35	0	0	0	0	9	9	4	6	0	21	5	1	16	**108**	**341**
FI	37	44	1	0	1	10	115	25	0	48	5	229	14	30	10	1	194	0	3	0	90	49	107	44	2	4	362	3	3	81	**229**	**1512**
FR	365	339	0	0	8	97	502	29	0	92	78	31	860	161	8	0	336	11	26	1	29	106	74	1 739	8	9	286	37	75	190	**860**	**5 497**
HU	297	53	4	0	1	3	169	4	0	2	3	19	70	791	1	0	27	1	10	0	0	28	32	0	0	76	79	19	14	14	**791**	**1 717**
IE	20	21	0	0	4	2	24	1	0	9	8	0	23	4	309	0	35	0	4	0	4	16	7	0	0	0	22	2	2	187	**309**	**704**
IS	4	3	0	0	0	0	3	0	0	3	1	1	6	2	1	0	3	0	1	0	1	3	10	1	0	0	11	1	0	3	**0**	**58**
IT	390	111	5	0	6	33	349	11	0	270	47	27	192	60	23	5	3 290	0	11	0	58	78	116	9	2	6	201	59	224	680	**3 290**	**6 263**
LT	3	1	0	0	1	3	0	0	0	0	1	0	1	0	0	0	0	5	0	0	0	0	4	14	0	0	5	0	2	0	**5**	**40**
LU	7	21	4	0	0	0	12	2	0	0	0	1	9	6	0	1	8	0	2	0	1	6	4	0	0	0	10	3	1	3	**2**	**101**
LV	3	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	5	0	0	0	0	0	0	0	0	1	0	2	0	**0**	**15**
MT	1	0	0	0	0	0	0	0	0	0	0	5	1	0	0	0	6	0	0	0	16	0	1	0	0	0	1	1	0	0	**16**	**32**
NL	109	223	16	0	1	27	198	21	0	113	16	29	109	33	7	1	226	0	14	0	58	1 240	95	16	8	9	289	8	22	129	**1 240**	**3 017**
NO	84	103	6	0	2	13	256	76	0	199	55	57	78	23	8	0	524	8	13	1	83	86	276	164	1	9	826	10	21	96	**276**	**3 078**
PL	188	65	0	0	0	30	68	15	0	0	2	4	75	1	1	0	0	3	3	0	0	7	27	1 208	1	1	43	1	13	4	**1 208**	**1 760**
PT	1	10	0	0	0	0	4	1	0	0	11	0	9	0	0	0	2	0	2	0	0	2	2	0	3	0	2	0	1	2	**3**	**52**
RO	43	2	5	0	1	9	33	0	0	3	0	5	14	11	0	0	0	0	1	0	0	9	1	1	0	64	17	0	4	4	**64**	**227**
SE	243	133	30	0	4	36	516	173	0	143	29	143	145	80	16	3	276	0	16	0	130	98	430	147	5	13	1 914	11	26	122	**1 914**	**4 882**
SI	14	4	0	0	0	1	10	1	0	1	1	2	15	6	0	0	5	0	1	0	0	2	3	0	0	0	5	45	3	2	**45**	**121**
SK	105	4	0	0	0	7	33	0	1	0	0	1	2	12	0	0	3	0	0	1	0	4	4	4	0	0	9	2	195	6	**195**	**393**
UK	109	153	7	0	3	12	276	30	0	108	6	38	209	25	217	2	768	0	8	0	43	128	76	7	4	11	174	6	46	3 141	**3 141**	**5 607**
Gesamtzahl der Erstanträge	**4 407**	**7 298**	**245**	**4**	**125**	**1 155**	**5 487**	**589**	**4**	**2 067**	**480**	**773**	**2 734**	**1 670**	**663**	**15**	**6 600**	**46**	**204**	**5**	**542**	**2 363**	**1 833**	**5 581**	**55**	**313**	**5 791**	**283**	**1 082**	**5 475**	**24 433**	**57 889**

[97] KOM(2009) 494 vom 25.9.2009. „Inlandstreffer“ bedeutet, dass in einem Mitgliedstaat, in dem bereits ein Asylantrag gestellt worden war, ein neuer Asylantrag eingereicht wurde.

Advance Passenger Information (API) System

Vereinigtes Königreich: Nutzung von Fluggastdaten zur Verbesserung der Grenzkontrollen und zur Bekämpfung der illegalen Einwanderung[98]	
Zahl der Maßnahmen im Jahr 2009	
Vorfälle in der Vergangenheit (Einreiseverweigerung)	379
Verlorene, gestohlene oder annullierte Pässe (Beschlagnahme)	56

[98] Diese Informationen wurden der Kommission zum Zwecke dieser Mitteilung von der britischen Grenzbehörde (UK Border Agency) übermittelt.

Zollinformationssystem (ZIS)

Gesamtzahl der in der ZIS-Datenbank erfassten Fälle (2009) [99]	
Maßnahme	**ZIS (auf Grundlage des ZIS-Übereinkommens)**
Angelegte Fälle	2 007
Aktive Fälle	274
Abgefragte Fälle	11 920
Gelöschte Fälle	1 355

[99] Diese Informationen wurden von der Kommission zur Verfügung gestellt.

Schwedische Initiative

Anwendung der Schwedischen Initiative zur Ermittlung bei Straftaten - Beispielfälle[100]	
Tötung	2009 wurde in der Hauptstadt eines Mitgliedstaates ein Tötungsversuch unternommen. Die Polizei stellte an einem Glas, aus dem der Verdächtige getrunken hatte, Spuren sicher. Anhand der DNA aus der sichergestellten Probe erstellten die Rechtsmediziner ein DNA-Profil. Ein Abgleich mit Profilen in der nationalen DNA-Datenbank ergab jedoch keinen Treffer. Die ermittelnde Polizei beantragte daher bei ihrer Prüm-Kontaktstelle einen Abgleich der DNA mit den Daten anderer Mitgliedstaaten, die gemäß dem Prüm-Beschluss bzw. dem Prümer Vertrag zu einem solchen Datenaustausch befugt sind. Beim grenzübergreifenden Abgleich wurde ein „Treffer" erzielt. Auf Grundlage der Schwedischen Initiative fragte die ermittelnde Polizei weitere Daten über den Verdächtigen ab. Bei der zuständigen nationalen Kontaktstelle gingen binnen 36 Stunden Antworten verschiedener Mitgliedstaaten ein, anhand derer die Polizei den Verdächtigen schließlich identifizieren konnte.
Vergewaltigung	2003 wurde eine Frau von einem unbekannten Täter vergewaltigt. Die Polizei stellte beim Opfer Spuren sicher, doch wurden mit dem aus der Probe erstellten DNA-Profil in der nationalen Datenbank keine Treffer erzielt. Ein Ersuchen auf DNA-Abgleich, das von der Prüm-Kontaktstelle an andere Mitgliedstaaten, die gemäß dem Prüm-Beschluss bzw. dem Prümer Vertrag zu einem solchen Datenaustausch befugt sind, übermittelt wurde, ergab schließlich einen Treffer. Die ermittelnde Polizei fragte daraufhin auf Grundlage der Schwedischen Initiative weitere Informationen über den Verdächtigen ab. Bei der zuständigen nationalen Kontaktstelle ging binnen acht Stunden eine Antwort ein, anhand derer die Polizei schließlich den Verdächtigen identifizieren konnte.

[100] Diese Beispielfälle wurden der Kommission zum Zwecke dieser Mitteilung von den Polizeibehörden eines Mitgliedstaates zur Verfügung gestellt.

Beim grenzübergreifenden DNA-Abgleich von Deutschland erzielte Treffer, gegliedert nach Delikten (2009)[101]

Treffer gegliedert nach Delikten	**Öster-reich**	**Spanien**	**Luxem-burg**	**Niederlande**	**Slowe-nien**
Gemeingefährliche Straftaten	32	4	0	5	2
Straftaten gegen die persönliche Freiheit	9	3	5	2	0
Sexualdelikte	40	22	0	31	4
Straftaten gegen das Leben	49	24	0	15	2
Sonstige Straftaten	3 005	712	18	1 105	71

[101] Antwort der deutschen Regierung auf eine parlamentarische Anfrage von Ulla Jelpke, Inge Höger und Jan Korte (Drucksache 16/14120), Bundestag, 16. Sitzung, Drucksache 16/14150, 22.10.2009. Diese Zahlen beziehen sich auf den Zeitraum ab Beginn des Datenaustauschs zwischen Deutschland und einem Mitgliedstaat bis zum 30. September 2009.

Aufdeckung schwerer Straftaten mittels Vorratsdatenspeicherung - Beispiele aus den Mitgliedstaaten[102]	
Mord	Der Polizeibehörde eines Mitgliedstaates ist es gelungen, eine Personengruppe aufzuspüren, die aus rassistischen Motiven sechs Menschen ermordet hatte. Die Täter hatten versucht, durch Austauschen ihrer SIM-Karten zu entkommen, konnten jedoch anhand ihrer Ruflisten und Mobiltelefon-Gerätenummern identifiziert werden.
Tötung	Eine Polizeibehörde konnte zwei Tatverdächtigen die Beteiligung an einem Tötungsdelikt nachweisen, nachdem sie die Mobilfunkdaten des Opfers ausgewertet hatte. So gelang es den Ermittlern, den Weg zu rekonstruieren, den das Opfer mit den zwei Verdächtigen gemeinsam zurückgelegt hatte.
Einbruch	Den Behörden ist es gelungen, einen Täter, der 17 Einbrüche verübt hatte, anhand der Verkehrsdaten seiner anonymen Prepaid-SIM-Karte aufspüren. Nachdem die Ermittler zunächst die Freundin identifiziert hatten, konnten sie auch den Täter selbst ausfindig machen.
Betrug	Ermittler konnten eine Betrügerbande entlarven, die via Internet teure Kraftfahrzeuge „gegen Bargeld“ angeboten hatte und systematisch die Abholer der betreffenden Fahrzeuge ausraubte. Mittels IP-Adresse konnte die Polizei die Täter ermitteln und festnehmen.

[102] Diese anonymen Beispiele basieren auf den Antworten der Mitgliedstaaten auf den Fragebogen der Kommission (2009) zur Umsetzung der Richtlinie 2006/24/EG (Richtlinie über die Vorratsdatenspeicherung).

Zusammenarbeit der Finanzfahndungsstellen

Gesamtzahl der über FIU.NET gestellten Informationsanfragen der nationalen Finanzfahndungsstellen [103]		
Jahr	**Informationsanfragen**	**Aktive Nutzer**
2007	3 133	12 Mitgliedstaaten
2008	3 084	13 Mitgliedstaaten
2009	3 520	18 Mitgliedstaaten

[103] Diese Informationen wurden der Kommission zum Zwecke dieser Mitteilung vom FIU.NET-Büro zur Verfügung gestellt.

Zusammenarbeit der Vermögensabschöpfungsstellen (ARO)

Aufspüren von Erträgen aus Straftaten: von Europol bearbeitete Anfragen der Mitgliedstaaten[104]

Jahr	**2004**	**2005**	**2006**	**2007**
Anfragen	5	57	53	133
Davon:				
Fälle betreffend Betrug				29
Fälle betreffend Geldwäsche				26
Fälle betreffend Drogen				25
Fälle betreffend sonstige Straftaten				18
Fälle betreffend Drogen und Geldwäsche				19
Fälle betreffend Betrug und Geldwäsche				7
Fälle betreffend mehrere Straftaten				9

Beschlagnahme von Vermögenswerten: von Eurojust bearbeitete Fälle (2006-2007)[105]

Art der Fälle		**Einleitung durch**	
Fälle betreffend Umweltstraftaten	1	Deutschland	27 %
Fälle betreffend die Beteiligung an einer kriminellen Vereinigung	5	Niederlande	21 %
Fälle betreffend Drogenhandel	15	VK	15 %
Fälle betreffend Steuerbetrug	8	Finnland	13 %
Fälle betreffend Betrug	8	Frankreich	8 %
Fälle betreffend MwSt-Betrug	1	Spanien	6 %
Fälle betreffend Geldwäsche	9	Portugal	4 %
Fälle betreffend Bestechung	1	Schweden	2 %
Fälle betreffend Eigentumsdelikte	2	Dänemark	2 %
Fälle betreffend Waffenhandel	1	Lettland	2 %
Fälle betreffend Nachahmung und Produktpiraterie	2		
Fälle betreffend Vorauszahlungsbetrug	2		
Fälle betreffend die Fälschung offizieller Dokumente	1		
Fälle betreffend Fahrzeugkriminalität	1		
Fälle betreffend Terrorismus	1		
Fälle betreffend Fälschungen	2		
Fälle betreffend Menschenhandel	1		

[104] Bewertung der Effizienz der von den EU-Mitgliedstaaten verwendeten Methoden für die Identifizierung, das Aufspüren, das Einfrieren und die Beschlagnahme von Erträgen aus Straftaten - Abschlussbericht (für die Europäische Kommission, GD JLS), Matrix Insight, 6/2009.

[105] Ebda.

Plattformen gegen Cyber-Kriminalität

Französische Plattform gegen Cyberkriminalität (Pharos) – Beispiele für Ermittlungsfälle[106]	
Kinder-pornographie	Ein Internetnutzer meldete bei Pharos, dass er auf einen Blog mit Fotos und gezeichneten Darstellungen von sexuellem Kindesmissbrauch gestoßen war. Der Autor des Blogs, der auf einem der Fotos nackt zu sehen war, nahm über seinen Blog auch selbst Kontakt zu Kindern auf. Die Ermittler konnten als Hauptverdächtigen einen Mathematiklehrer identifizieren. Bei der Durchsuchung seiner Wohnung wurden 49 Videos mit Kinderpornographie gefunden. Ferner stellte sich heraus, dass er plante, Hausunterricht zu erteilen und dafür bereits Vorkehrungen getroffen hatte. Der Beschuldigte wurde zu einer Bewährungsstrafe verurteilt.
Sexueller Missbrauch von Kindern	Bei der französischen Polizei ging ein Hinweis auf eine Person ein, die im Internet für Sex mit Kindern Geld bot. Ein Pharos-Ermittler gab sich als Minderjähriger aus und nahm mit dem Verdächtigen Kontakt auf, der ihn für sexuelle Dienste bezahlen wollte. Anhand des Internet-Chats gelang es über Pharos, die IP-Adresse des Verdächtigen sowie den Ort ermitteln, von dem aus er agierte - eine Stadt, die aufgrund zahlreicher Kindesmissbrauchsfälle bereits bekannt war. Der Beschuldigte wurde zu einer Bewährungsstrafe verurteilt.

[106] Die Abkürzung „Pharos" steht für „plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements".

Europols Beitrag zur Bekämpfung grenzüberschreitender schwerer Kriminalität - Beispielfälle[107]	
Operation Andromeda	Im Dezember 2009 unterstützte Europol eine groß angelegte grenzüberschreitende Polizeiaktion gegen einen Drogenring mit Verbindungen in 42 Ländern. Der von Belgien und Norwegen aus gesteuerte Ring schleuste Drogen aus Peru über die Niederlande nach Belgien, Italien, ins Vereinigte Königreich sowie in andere Mitgliedstaaten. Die polizeiliche Zusammenarbeit wurde von Europol, die justizielle Zusammenarbeit von Eurojust koordiniert. Die beteiligten Behörden richteten ein mobiles Büro in Pisa ein, Europol eine Einsatzzentrale in Den Haag. Europol erfasste die Verbindungen zwischen den Verdächtigen und erstellte einen Bericht über das kriminelle Netz.
Beteiligte	Belgien, Deutschland, Italien, Litauen, die Niederlande, Norwegen, das Vereinigte Königreich und Eurojust
Ergebnisse	Die beteiligten Polizeikräfte beschlagnahmten 49 kg Kokain, 10 kg Heroin, 6000 Ecstasy-Pillen, zwei Schusswaffen, fünf gefälschte Ausweisdokumente sowie 43 000 EUR in Bar; 15 Personen wurden festgenommen.
Operation Typhon	Zwischen April 2008 und Februar 2010 unterstützte Europol die an der Operation Typhon beteiligten Polizeibehörden aus 20 Ländern durch die Erstellung einschlägiger Analysen. Bei dieser breit angelegten Aktion gegen einen Pädophilenring, der kinderpornographische Bilder über eine österreichische Website verbreitete, leistete Europol technische Unterstützung und erstellte anhand der Bilder aus Österreich kriminalpolizeiliche Analysen. Europol prüfte zunächst die Zuverlässigkeit der Daten, bereitete diese auf und führte auf dieser Grundlage seinen eigenen kriminaltechnischen Untersuchungen durch. Dank des Abgleichs der Daten mit den Informationen seiner entsprechenden Analysedatei (Analytical Work File) erstellte Europol 30 Berichte, anhand derer Untersuchungen in verschiedenen Ländern eingeleitet wurden.
Beteiligte	Belgien, Bulgarien, Dänemark, Deutschland, Frankreich, Italien, Kanada, Litauen, Luxemburg, Malta, die Niederlande, Österreich, Polen, Rumänien, die Slowakei, Slowenien, Spanien, die

[107] Diese Informationen wurden der Kommission zum Zwecke dieser Mitteilung von Europol zur Verfügung gestellt. Weitere Informationen zur Operation Andromeda sind abrufbar unter http://www.eurojust.europa.eu/.

	Schweiz, Ungarn und das Vereinigte Königreich
Ergebnisse	Den beteiligten Polizeikräften gelang es, 286 Verdächtige zu identifizieren, 118 Personen festzunehmen und fünf Missbrauchsopfer zu retten.

Eurojust: Beispiele für die Koordinierung groß angelegter grenzüberschreitender justizieller Maßnahmen gegen schwere Straftaten[108]

Menschenhandel und Terrorismus-finanzierung	Im Mai 2010 koordinierte Eurojust einen grenzüberschreitenden Einsatz, bei dem fünf Mitglieder eines organisierten kriminellen Netzes, das in Afghanistan, Pakistan, Rumänien, Albanien und Italien agierte, festgenommen wurden. Afghanische und pakistanische Staatsangehörige wurden über das Netz mit gefälschten Dokumenten ausgestattet und über den Iran, die Türkei und Griechenland nach Italien geschleust. Nach ihrer Ankunft in Italien wurden die Migranten nach Deutschland, Schweden, Belgien, Norwegen und ins Vereinigte Königreich gebracht. Die Einnahmen aus dem Menschenhandel waren für die Terrorismusfinanzierung bestimmt.
Bankkartenbetrug	Durch die Koordinierung der grenzüberschreitenden Zusammenarbeit der Polizei- und Justizbehörden haben Europol und Eurojust dazu beigetragen, einen Ring von Bankkartenbetrügern aufzudecken, der in Irland, Italien, den Niederlanden, Belgien und Rumänien agierte. Dabei ging es um den Diebstahl der Kenndaten von rund 15 000 Bankkarten, wodurch ein Schaden von 6,5 Mio. EUR verursacht worden war. Vor der Operation, die im Juli 2009 zu 24 Festnahmen führte, wurden mit Unterstützung belgischer, irischer, italienischer, niederländischer und rumänischer Richter europäische Haftbefehle ausgestellt und Abhöraktionen gegen die Verdächtigen veranlasst.
Menschen- und Drogenhandel	Nach einer von Eurojust organisierten Koordinierungssitzung im März 2009 gelang es den italienischen, niederländischen und kolumbianischen Behörden 62 des Menschen- und Drogen-handels verdächtigte Personen festzunehmen. Das Netz hatte Frauen aus Nigeria in die Niederlande geschleust und sie in Italien, Frankreich und Spanien zur Prostitution gezwungen. Mit den Einnahmen aus der Prostitution wurde in Kolumbien Kokain gekauft, das dann in der EU zum Verkauf angeboten wurde.

[108] Diese Beispiele entstammen folgender Website: http://www.eurojust.europa.eu/.

Fluggastdaten (PNR)

Aufdecken schwerer grenzübergreifender Kriminalität durch die Analyse von Fluggastdaten - Beispielfälle[109]	
Kinderhandel	Bei der Analyse von Fluggastdaten stellte sich heraus, dass drei unbegleitete Kinder von einem EU-Mitgliedstaat in einen Drittstaat reisten, jedoch keine Angaben darüber vorlagen, wer sie bei der Ankunft abholen würde. Nach Abreise der Kinder warnte die Polizei des betreffenden Mitgliedstaates die Behörden des Drittstaates vor, die den Abholer der Kinder festnahmen - einen im Mitgliedstaat registrierten Sexualstraftäter.
Menschenhandel	Bei der Analyse von Fluggastdaten wurde ein Menschenhändlerring aufgedeckt, der immer die gleiche Reiseroute nutzte. Die betreffenden Personen legten bei der Abfertigung für einen Flug innerhalb der EU gefälschte Reisedokumente vor, checkten aber gleichzeitig mit echten Reisedokumenten für einen anderen Flug in einen Drittstaat ein. Nach ihrer Ankunft in der Flughafenlounge stiegen sie schließlich in das andere Flugzeug mit dem innereuropäischen Reiseziel ein.
Kreditkartenbetrug	Mehrere Familien verwendeten bei ihrer Reise in einen Mitgliedstaat Flugtickets, die mit gestohlenen Kreditkarten gekauft worden waren. Bei den Ermittlungen stellte sich heraus, dass eine kriminelle Bande diese Kreditkarten zum Kauf der Tickets verwendet und diese wiederum über ein Callcenter verkauft hatte. Über die Fluggastdaten war es gelungen, die Reisenden mit den jeweiligen Kreditkarten und Verkäufern in Verbindung zu bringen.
Drogenhandel	Der Polizeibehörde eines Mitgliedstaates lagen Informationen vor, wonach ein Mann am Handel mit Drogen aus einem Drittstaat beteiligt war. Die Grenzschutzbeamten konnten ihm jedoch bei seiner Ankunft in der EU nie etwas nachweisen. Der Abgleich der Fluggastdaten ergab, dass er immer mit einem Komplizen reiste. Bei dessen Kontrolle konnten große Mengen Drogen sichergestellt werden.

[109] Diese Beispiele wurden zum Schutze der Informationsquellen anonymisiert.

Programm zum Aufspüren der Finanzierung des Terrorismus (TFTP)

Informationen, die dank TFTP zur Untersuchung von Terroranschlägen bereitgestellt werden konnten - Beispielfälle[110]	
Terroranschlag in Barcelona (2008)	Im Januar 2008 wurden in Barcelona im Zusammenhang mit einem vereitelten Terroranschlag auf das öffentliche Verkehrssystem der Stadt zehn Verdächtige festgenommen. Anhand der TFTP-Daten konnten Verbindungen der Verdächtigen nach Asien, Afrika und Nordamerika aufgedeckt werden.
Flüssigsprengstoff-Anschlag auf transatlantische Flüge (2006)	Zur Ermittlung und Festnahme der Urheber des gescheiterten Anschlags, bei dem im August 2006 zehn transatlantische Flüge aus dem Vereinigten Königreich in die USA und nach Kanada gesprengt werden sollten, wurden TFTP -Informationen verwendet.
Bombenanschläge in London (2005)	Die TFTP-Daten lieferten den Ermittlern neue Hinweise, bestätigten die Identität der Verdächtigen und zeigten Verbindungen zwischen den einzelnen am Anschlag beteiligten Tätern auf.
Bombenanschläge in Madrid (2004)	Nach den Anschlägen wurden mehreren EU-Mitgliedstaaten für ihre Ermittlungen TFTP-Daten zur Verfügung gestellt.

110 Zweiter Bericht über die Verarbeitung von personenbezogenen Daten aus der EU durch das Finanzministerium der Vereinigten Staaten zu Zwecken der Terrorismusbekämpfung, Richter Jean-Louis Bruguière, Januar 2010.

ANHANG II

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
Schengener Informations-system (SIS)	Initiative der Mitgliedstaaten	Aufrechterhal-tung der öffentlichen Sicherheit im Schengenraum (einschließlich der nationalen Sicherheit) sowie Erleichterung des Personen-verkehrs anhand der aus diesem System erteilten Informationen	Zentralisiert: N.SIS (nationale Elemente), die über eine Schnittstelle an das C.SIS (Zentraleinheit) angeschlossen sind	Namen und Aliasnamen, körperliche Merkmale, Geburtsort und -datum, Staatsangehörigkeit, Angaben über Bewaffnung oder Gewalttätigkeit der betreffenden Person; SIS-Ausschreibungen beziehen sich auf mehrere verschiedene Personengruppen	Polizei, Grenzpolizei, Zoll und Justizbehörden haben Zugriff auf alle Daten; die Einwanderungs-behörden und konsularischen Stellen auf die Liste der Personen mit Einreiseverbot sowie auf die Liste der abhanden gekommenen und gestohlenen Dokumente; Europol und Eurojust können bestimmte Daten abrufen.	Das Über-einkommen 108 des Europarates und die Empfehlung des Europarates R(87) 15 für die Polizei	Zur Personen-fahndung ins SIS aufgenommene personenbezogene Daten werden nicht länger als für den verfolgten Zweck erforderlich und nicht länger als drei Jahre gespeichert. Daten über Personen, die eine Gefahr für die öffentliche oder nationale Sicherheit darstellen und daher unter besonderer Beobachtung stehen, müssen nach einem Jahr gelöscht werden.	SIS ist in vollem Umfang anwendbar in 22 Mitglied-staaten sowie in der Schweiz, in Norwegen und Island. Das VK und Irland beteiligen sich am SIS, mit Ausnahme von Ausschreibungen zu Drittstaats-angehörigen mit Einreiseverbot. Bulgarien, Rumänien und Liechtenstein werden dieses Instrument voraussichtlich bald nutzen.	Die Vertragsparteien können Änderungen am Schengener Übereinkommen vorschlagen. Der geänderte Text müsste einstimmig angenommen und von den Parlamenten ratifiziert werden.

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
Schengener Informations-system II (SIS II)	Initiative der Kommission	Gewährleis-tung eines hohen Sicherheits-niveaus im Raum der Freiheit, der Sicherheit und des Rechts sowie Erleichterung des Personen-verkehrs anhand der aus diesem System erteilten Informationen	Zentralisiert: N.SIS II (nationale Elemente), die über eine Schnittstelle an das CS-SIS (Zentraleinheit) angeschlossen sind; SIS II wird auf dem sicheren s-TESTA-Netz laufen.	Für SIS geltende Datenkategorien sowie Finger-abdrücke und Fotos, Kopien des Europäischen Haftbefehls, Ausschreibungen zu missbräuchlich verwendeter Identität und Verknüpfungen zwischen Ausschreibungen. SIS II-Ausschreibungen beziehen sich auf mehrere verschiedene Personengruppen.	Polizei, Grenzpolizei, Zoll und Justizbehörden werden Zugriff auf alle Daten haben; die Einwanderungs-behörden und konsularischen Stellen auf die Liste der Personen mit Einreiseverbot sowie auf die Liste der abhanden gekommenen und gestohlenen Dokumente; Europol und Eurojust werden bestimmte Daten abrufen können.	Die besonderen Bestimmungen der grundlegenden Rechtsakte für das SIS II und die Richtlinie 95/46/EG, die Verordnung (EG) 45/2001 sowie der Rahmenbeschluss 2008/977/JI des Rates, die Verordnung (EG) 45/2011, das Übereinkommen 108 des Europarates sowie die Empfehlung des Europarates R(87) 15 für die Polizei	Zur Personen-fahndung ins SIS aufgenommene personenbezogene Daten werden nicht länger als für den verfolgten Zweck erforderlich und nicht länger als drei Jahre gespeichert. Daten über Personen, die eine Gefahr für die öffentliche oder nationale Sicherheit darstellen und daher unter besonderer Beobachtung stehen, müssen nach einem Jahr gelöscht werden.	SIS II ist in der Umsetzungsphase. Nach Inbetrieb-nahme wird das SIS II in der EU-27, in der Schweiz, in Liechtenstein, Norwegen und Island eingesetzt werden. Das VK und Irland werden sich am SIS II beteiligen, mit Ausnahme von Ausschreibungen zu Drittstaatsange-hörigen mit Einreiseverbot.	Die Kommission übermittelt dem Europäischen Parlament (EP) und dem Rat einen halbjährlichen Fortschrittsbericht, über die Entwicklung des SIS II sowie seine Migration vom SIS.

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
EURODAC	Initiative der Kommission	Unterstützung bei der Festlegung des für die Beurteilung des Asylantrags zuständigen Mitgliedstaates	Zentralisiert: Das System besteht aus nationalen Zugangsstellen, die über eine Schnittstelle an die EURODAC-Zentraleinheit angeschlossen sind. EURODAC läuft auf dem s-TESTA-Netz.	Fingerabdruckdaten, Geschlecht, Ort und Datum der Asylantragstellung, vom Herkunftsmitgliedstaat verwendete Referenznummer sowie das Datum, an dem die Fingerabdrücke genommen, übermittelt und im System erfasst wurden.	Die Mitgliedstaaten müssen angeben, welche Behörden Zugriff auf diese Daten haben. Üblicherweise gehören dazu die Asyl- und Einwanderungsbehörden, der Grenzschutz und die Polizei.	Richtlinie 95/46/EG	Fingerabdrücke der Asylbewerber 10 Jahre; Fingerabdrücke von Drittstaatsangehörigen, die beim illegalen Überschreiten einer Außengrenze aufgegriffen werden, 2 Jahre.	Die EURODAC-Verordnung ist in allen Mitgliedstaaten sowie in Norwegen, Island und in der Schweiz in Kraft. Ein Abkommen, das die Anbindung Liechtensteins ermöglichen soll, steht vor dem Abschluss.	Die Kommission übermittelt dem EP und dem Rat alljährlich einen Bericht über den Betrieb der EURODAC-Zentraleinheit.

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
Visa-Informations-system (VIS)	Initiative der Kommission	Unterstützung bei der Einführung einer gemeinsamen Visapolitik sowie bei der Abwendung von Gefahren für die innere Sicherheit	Zentralisiert: Das System besteht aus nationalen Elementen, die über eine Schnittstelle an die Zentraleinheit angeschlossen werden. VIS wird auf dem s-TESTA-Netz laufen.	Visumanträge, Fingerabdrücke, Fotos, einschlägige Visum-entscheidungen sowie Verknüpfungen zwischen den jeweiligen Anträgen	Visum-, Asyl-, Einwanderungs- und Grenz-kontrollbehörden werden Zugriff auf alle Daten haben; die Polizei und Europol können VIS zur Prävention, Aufdeckung und Untersuchung schwerer Kriminalität konsultieren.	Die besonderen Bestimmungen der Basisrechtsakte für das VIS und die Richtlinie 95/46/EG, die Verordnung (EG) 45/2001 sowie der Rahmenbeschluss 2008/977/JI des Rates, das Über-einkommen 108 des Europarates, das Zusatz-protokoll 181 des Europarates sowie die Empfehlung des Europarates R(87) 15 für die Polizei	5 Jahre	VIS ist in der Umsetzungsphase und wird in allen Mitgliedstaaten (mit Ausnahme des VK und Irlands) sowie in Norwegen, Island und in der Schweiz eingesetzt werden.	Die Kommission erstattet dem EP und dem Rat drei Jahre nach Inbetriebnahme des VIS und danach alle vier Jahre Bericht über seinen Betrieb.
Advance Passenger Information System (API)	Initiative Spaniens	Verbesserung der Grenzkon-trollen und Bekämpfung illegaler Einwanderung	Dezentralisiert	Personenbezogene Daten aus Pässen, Abreiseort und Grenzübergangsstelle für die Einreise in die EU	Grenzkontroll-behörden und - auf Anfrage – Strafverfolgungs-behörden	Richtlinie 95/46/EG	Die Daten müssen 24 Stunden nach Ankunft des Flugs in der EU gelöscht werden.	Das API-System ist in allen Mitgliedstaaten in Betrieb, wird jedoch nur von wenigen genutzt.	Die Kommission wird das API-System im Jahr 2011 bewerten.

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
Neapel-II-Übereinkommen	Initiative der Mitgliedstaaten	Unterstützung der nationalen Zollbehörden, um Verstöße gegen die nationalen Zollbestimmungen zu verhindern und aufzudecken und Unterstützung bei der Verfolgung und Bestrafung von Verstößen gegen die Zollvorschriften der Gemeinschaft und des Mitgliedstaats	Dezentralisiert, Ausführung über zentrale Koordinierungsstellen	Alle Informationen im Zusammenhang mit einer identifizierten oder identifizierbaren Person	Die zentralen Koordinierungsstellen leiten die entsprechenden Daten an die nationalen Zoll-, Ermittlungs- und Justizbehörden und, soweit der die Daten bereitstellende Mitgliedstaat dies zuvor genehmigt hat, an andere Behörden weiter.	Die Richtlinie 95/46/EG und das Übereinkommen 108 des Europarates. Im Empfängermitgliedstaat muss mindestens das gleiche Maß an Datenschutz wie im bereitstellenden Mitgliedstaat gewährleistet sein.	Die Daten dürfen nur so lange aufbewahrt werden, wie es für den Zweck, zu dem sie zur Verfügung gestellt wurden, notwendig ist.	Dieses Übereinkommen wurde von sämtlichen Mitgliedstaaten ratifiziert.	Die Vertragsparteien können Änderungen am Neapel-II-Übereinkommen vorschlagen. Der geänderte Text müsste vom Rat angenommen und von den Mitgliedstaaten ratifiziert werden.

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
Zollinformationssystem (ZIS)	Initiative der Mitgliedstaaten	Unterstützung der zuständigen Behörden bei der Verhinderung, Ermittlung und Verfolgung schwerer Verstöße gegen die nationalen Zollvorschriften	Zentralisiert, Zugriff über Terminals von allen Mitgliedstaaten und der Kommission aus; ZIS und FIDE werden auf der Grundlage von AFIS betrieben, das das Gemeinsame Kommunikationsnetz, die Gemeinsame Systemschnittstelle sowie den sicheren Webzugang der Kommission nutzt.	Namen und Aliasnamen, Geburtsdatum und -ort, Staatsangehörigkeit, Geschlecht, körperliche Merkmale, Ausweisdokumente, Anschrift, Angaben über Gewalttätigkeit in der Vergangenheit, Gründe für die Datenspeicherung im ZIS, vorgeschlagene Maßnahmen und Zulassungsdaten des Beförderungsmittels.	Die nationalen Zollbehörden, Europol und Eurojust können auf ZIS-Daten zugreifen.	Die besonderen Bestimmungen des ZIS-Übereinkommens sowie die Richtlinie 95/46/EG, die Verordnung (EG) Nr. 45/2001, das Übereinkommen 108 des Europarates und die Empfehlung des Europarates R(87) 15 für die Polizei.	Personenbezogene Daten, die vom ZIS in andere für Risikomanagement oder operative Analysen genutzte Systeme übertragen werden, dürfen nur so lange gespeichert werden, wie dies zur Erfüllung des Zwecks, zu dem sie kopiert wurden, notwendig ist, keinesfalls aber länger als 10 Jahre.	In allen Mitgliedstaaten in Kraft	Die Kommission berichtet dem EP und dem Rat gemeinsam mit den Mitgliedstaaten jährlich über den Betrieb des ZIS.

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
Schwedische Initiative	Initiative Schwedens	Vereinfachung des Informationsaustauschs zum Zwecke der Durchführung strafrechtlicher Ermittlungen oder polizeilicher Erkenntnisgewinnungsverfahren	Dezentralisiert; die Mitgliedstaaten müssen nationale Kontaktstellen bestimmen, die dringende Informationsanfragen bearbeiten.	Alle Informationen oder kriminalpolizeilichen Erkenntnisse, die den Strafverfolgungsbehörden zur Verfügung stehen.	Polizei, Zoll sowie alle anderen Behörden mit der Befugnis, bei Straftaten zu ermitteln (mit Ausnahme der Geheimdienste)	Nationale Datenschutzbestimmungen sowie das Übereinkommen 108 des Europarates, das Zusatzprotokoll 181 und die Empfehlung des Europarates R(87) 15 für die Polizei	Die über dieses Instrument bereitgestellten Informationen und Erkenntnisse dürfen nur für den eigentlichen Bestimmungszweck und unter den vom bereitstellenden Mitgliedstaat festgelegten Bedingungen genutzt werden.	12 der 31 Vertragsparteien (EU sowie EFTA-Staaten) haben nationale Rechtsvorschriften erlassen, um dieses Instrument umzusetzen. Fünf davon nutzen für Informationsanfragen das einschlägige Formular. Zwei nutzen es häufig für den Informationsaustausch.	2010 übermittelt die Kommission dem Rat ihren Bewertungsbericht.

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
Prüm-Beschluss	Initiative der Mitgliedstaaten	Bessere Verhütung von Kriminalität, insbesondere von Terrorismus, und Aufrechterhaltung der öffentlichen Ordnung	Dezentralisiert, über das s-TESTA-Netz angeschlossen. Nationale Kontaktstellen bearbeiten ausgehende und eingehende Anträge auf Datenabgleich.	Anonyme DNA-Profile und Fingerabdrücke, Daten aus Fahrzeugregistern und Informationen über Personen, die im Verdacht stehen, Verbindungen zu terroristischen Vereinigungen zu unterhalten	Kontaktstellen übermitteln Anfragen, für den Zugang in den einzelnen Mitgliedstaaten gelten die nationalen Rechtsvorschriften.	Die Sonderbestimmungen des Prüm-Beschlusses, das Übereinkommen 108 des Europarates, das Zusatzprotokoll 181 des Europarates und die Empfehlung des Europarates R(87) 15 für die Polizei; Einzelpersonen können sich an ihren nationalen Datenschutzbeauftragten wenden, um ihre Rechte bezüglich der Bearbeitung personenbezogener Daten geltend zu machen.	Die personenbezogenen Daten müssen gelöscht werden, sobald sie für den Zweck, zu dem sie übermittelt wurden, nicht mehr erforderlich sind. Für die Datenspeicherung gilt die im übermittelnden Staat zulässige Höchstdauer, die für den Empfängerstaat verpflichtend ist.	Der Prüm-Beschluss ist noch in der Umsetzungsphase. Zehn Mitgliedstaaten wurde der Austausch von DNA-Profilen gestattet, fünf der Austausch von Fingerabdruckdaten und sieben der Austausch von Daten aus Fahrzeugregistern. Die Teilnahme Norwegens und Islands steht bevor.	2012 übermittelt die Kommission dem Rat ihren Bewertungsbericht.

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
Richtlinie über die Vorratsdaten-speicherung	Initiative der Mitgliedstaaten	Verbesserung der Ermitt-lung, Auf-klärung und Verfolgung schwerer Straftaten durch die Speicherung von Tele-kommuni-kations-verkehrs- und Standortdaten	Dezentralisiert; dieses Instrument verpflichtet Anbieter von Telekommunika-tionsdiensten zur Vorratsspei-cherung von Daten	Telefonnummer, IP-Adresse und Mobiltelefon-Gerätenummern	Behörden mit Zugriffsrechten werden auf nationaler Ebene festgelegt	Richtlinie 95/46/EG und Richtlinie 2002/58/EG	Zwischen 6 und 24 Monaten	Sechs Mitglied-staaten haben diese Richtlinie bislang noch nicht umgesetzt; das deutsche und das rumänische Verfassungsgericht haben Durchführungs-bestimmungen für verfassungswidrig erklärt.	2010 übermittelt die Kommission dem EP und dem Rat ihren Bewertungsbericht.
Europäisches Strafregister-informations-system (ECRIS)	Initiative Belgiens, Vorschlag der Kommission	Verbesserung des grenzüber-schreitenden Austauschs der Straf-registerdaten von EU-Bürgern	Dezentralisiert; Anbindung über zentrale Behörden, die über das s-TESTA-Netz Strafregister-informationen austauschen.	Angaben zur Person, Verurteilungen, Strafen und Vergehen, zusätzliche Daten einschließlich Fingerabdrücke (falls verfügbar)	Justizbehörden sowie zuständige Verwaltungs-behörden	Die besonderen Bestimmungen des Beschlusses 2009/315/JI des Rates, in den die Bestimmungen des Beschlusses 2005/876/JI des Rates aufgenommen wurden, sowie der Rahmenbeschluss 2008/977/JI des Rates, das Übereinkommen 108 des Europarates und die Verordnung (EG) Nr. 45/2001.	Es gelten die nationalen Vorschriften für die Vorratsdaten-speicherung, da dieses Instrument nur den Datenaustausch regelt.	ECRIS ist in der Umsetzungsphase. Neun Mitgliedstaaten haben mit dem elektronischen Informations-austausch begonnen.	Die Kommission übermittelt dem EP und dem Rat zwei Bewertungsberichte: 2011 einen zum Rahmenbeschluss 2008/675/JI und 2015 einen zum Rahmenbeschluss 2009/315/JI. Ab 2016 veröffentlicht die Kommission regelmäßig Berichte über die Durch-führung des Beschlusses 2009/316/JI (ECRIS).

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
Zusammenarbeit der Finanzfahndungsstellen (FIU.NET)	Initiative der Niederlande	Informationsaustausch für Analysen und Ermittlungen im Bereich der Geldwäsche und Terrorismusfinanzierung	Dezentralisiert, die Finanzfahndungsstellen (FIU) tauschen über das FIU.NET, das auf dem s-TESTA-Netz läuft, Daten aus. FIU.NET könnte bald durch die Europol-Anwendung „SIENA“ unterstützt werden.	Alle für Analysen und Ermittlungen im Bereich der Geldwäsche und Terrorismusfinanzierung relevanten Daten	Finanzfahndungsstellen (der Polizei, der Justizbehörden oder der Verwaltungsbehörden, die an die Finanzbehörden berichten)	Rahmenbeschluss 2008/977/JI des Rates, Übereinkommen 108 des Europarates und die Empfehlung des Europarates R(87) 15 für die Polizei	Es gelten die nationalen Vorschriften für die Vorratsdatenspeicherung, da dieses Instrument nur den Datenaustausch regelt.	Zwanzig Mitgliedstaaten sind ans FIU.NET angeschlossen - eine Online-Anwendung für den Datenaustausch, die auf s-TESTA läuft.	Im Rahmen ihres Aktionsplans für Finanzdienstleistungen überprüft die Kommission seit 2009 die Umsetzung der Richtlinie 2005/60/EG.
Zusammenarbeit der Vermögensabschöpfungsstellen	Initiative der Mitgliedstaaten	Informationsaustausch zur Identifizierung und Nachverfolgung von Erträgen aus Straftaten	Dezentralisiert, Informationsaustausch der ARO über die Schwedische Initiative; die Zusammenarbeit dieser Stellen könnte bald durch die Europol-Anwendung „SIENA“ unterstützt werden.	Nähere Angaben zum betreffenden Eigentum (z.B. zu Bankkonten, Immobilien und Fahrzeugen) sowie zu den gesuchten Personen (u.a. Name, Adresse, Informationen zu Unternehmen und Unternehmensbeteiligungen)	Vermögensabschöpfungsstellen	Übereinkommen 108 des Europarates, Zusatzprotokoll 181 des Europarates und Empfehlung des Europarates R(87) 15 für die Polizei	Es gelten die nationalen Vorschriften für die Vorratsdatenspeicherung, da dieses Instrument nur den Datenaustausch regelt.	Mehr als zwanzig Mitgliedsstaaten haben ARO eingerichtet; zwölf nehmen an einem Pilotprojekt teil, das für den Austausch von Daten zum Aufspüren von Vermögenswerten die Europol-Anwendung „SIENA“ nutzt.	2010 übermittelt die Kommission dem Rat ihren Bewertungsbericht.

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
Nationale und EU-weite Cybercrime-Plattformen	Initiative Frankreichs	Sammlung, Austausch und Analyse von Informationen über Internet-Straftaten	Dezentralisiert, Zusammenführung nationaler Meldeplattformen und Europols EU-weiter Cybercrime-Plattform; Europols Anwendung SIENA könnte den Datenaustausch zwischen den Meldeplattformen bald unterstützen.	Unerlaubte Inhalte oder rechtswidriges Verhalten im Internet	Nationale Plattformen werden aus Hinweisen der Bürger gespeist; Europols EU-Plattform wird aus Berichten der Strafverfolgungsbehörden über schwere grenzüberschreitende Cyberkriminalität gespeist.	Die besonderen Bestimmungen des Europol-Beschlusses sowie der Rahmenbeschluss 2008/977/JI des Rates, das Übereinkommen 108 des Europarates, das Zusatzprotokoll 181 des Europarates, die Empfehlung des Europarates R(87) 15 für die Polizei und die Verordnung (EG) Nr. 45/2001.	Es gelten die nationalen Vorschriften zur Vorratsspeicherung von Daten, da dieses Instrument nur den Informationsaustausch regelt.	Fast alle Mitgliedstaaten haben nationale Meldeplattformen eingerichtet; Europol arbeitet an seiner EU-weiten Cybercrime-Plattform.	Europol, das den Bereich Cyberkriminalität abdeckt, wird künftig in seinem Jahresbericht, den es dem Rat zur Genehmigung und dem EP zur Information vorlegt, über die Maßnahmen der EU-Cybercrime-Plattform berichten.

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
Europol	Initiative der Mitgliedstaaten	Unterstützung der Mitglied-staaten bei der Verhütung und Bekämpfung von organisierter Kriminalität, Terrorismus und anderer Formen schwerer Kriminalität, die zwei oder mehrere Mitglied-staaten betreffen.	Europol ist eine EU-Agentur mit Sitz in Den Haag. Europol entwickelt „SIENA“, seine eigene sichere Anwendung für den Informations-austausch.	Das Europol-Informationssystem (EIS) umfasst personenbezogene Daten (einschließlich biometrischer Merkmale, Verurteilungen und Verbindungen zur organisierten Kriminalität) betreffend Personen, die eines Verbrechens verdächtigt werden, das in den Zuständigkeits-bereich von Europol fällt. Die Arbeitsdateien zu Analysezwecken enthalten einschlägige personenbezogene Daten.	Zugriff auf das EIS haben die nationalen Europol-Stellen, Verbindungs-beamte, Europol-Mitarbeiter und der Direktor. Verbindungs-beamte haben Zugriff auf die Arbeitsdateien zu Analysezwecken. Der Austausch von personen-bezogenen Daten ist mit Dritt-staaten möglich, die ein ein-schlägiges Abkommen mit Europol ge-schlossen haben.	Die besonderen Bestimmungen des Europol-Be-schlusses sowie der Rahmen-beschluss 2008/977/JI des Rates, das Über-einkommen 108 des Europarates, das Zusatz-protokoll 181 des Europarates, die Empfehlung des Europarates R(87) 15 für die Polizei und die Verordnung (EG) Nr. 45/2001.	Arbeitsdateien zu Analysezwecken dürfen höchstens drei Jahre gespeichert werden, wobei diese Frist um weitere drei Jahre verlängert werden kann.	Europol wird von allen Mitglied-staaten sowie den Drittländern, die mit Europol ein operatives Abkommen geschlossen haben, aktiv genutzt. Die neue Europol-Rechtsgrundlage wurde von allen Mitgliedstaaten umgesetzt.	Eine gemeinsame Kontrollinstanz überwacht die Ver-arbeitung personen-bezogener Daten durch Europol sowie die Übermittlung solcher Daten an Dritte. Sie erstattet dem EP und dem Rat in regelmäßigen Abständen Bericht. Darüber hinaus erstellt Europol einen Jahresbericht über seine Tätigkeit und legt diesen dem Rat zur Genehmigung und dem EP zur Information vor.

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
Eurojust	Initiative der Mitgliedstaaten	Verbesserung der Koordination von Ermittlungen und Strafverfolgungen in den Mitgliedstaaten sowie Ausbau der Zusammenarbeit zwischen den einschlägigen Behörden	Eurojust ist eine EU-Einrichtung mit Sitz in Den Haag, die für den Datenaustausch s-TESTA nutzt.	Personenbezogene Daten von Verdächtigen und Straftätern im Falle schwerer Verbrechen, die zwei oder mehrere Mitgliedstaaten betreffen (einschließlich Angaben zur Person, Adresse, DNA-Profile, Fingerabdrücke, Fotos, Telekommunikations verkehrs- und Standortdaten).	Zugriff haben die 27 Europol-Mitgliedstaaten. Sie können - sofern die ursprüngliche Informationsquelle zustimmt - die Daten nationalen Behörden und Drittstaaten zur Verfügung stellen.	Die besonderen Bestimmungen des Eurojust-Beschlusses sowie der Rahmenbeschluss 2008/977/JI des Rates, das Übereinkommen 108 des Europarates, das Zusatzprotokoll 181 des Europarates und die Empfehlung des Europarates R(87) 15 für die Polizei.	Die Informationen müssen gelöscht werden, sobald der Zweck, zu dem sie bereitgestellt wurden, erfüllt bzw. der Fall abgeschlossen ist.	Die geänderte Rechtsgrundlage von Eurojust wird derzeit von den Mitgliedstaaten umgesetzt.	Bis Juni 2014 überprüft die Kommission den Datenaustausch zwischen Eurojust und den Mitgliedstaaten. Bis Juni 2013 erstattet Eurojust dem Rat und der Kommission darüber Bericht, inwieweit den Mitgliedstaaten auf das Fallverwaltungssystem (Case Management System) Zugriff gewährt wurde. Eine gemeinsame Kontrollinstanz überwacht die Verarbeitung personenbezogener Daten durch Eurojust und erstattet dem Rat jährlich darüber Bericht. Der Präsident des Eurojust-Kollegiums legt dem Rat einen Jahresbericht über die Tätigkeiten von Eurojust vor, der vom Rat wiederum an das EP weitergeleitet wird.

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
Fluggastdaten (PNR)-Abkommen mit den USA und Australien, API/PNR-Abkommen mit Kanada	Initiative der Kommission	Verhütung und Bekämpfung des Terrorismus und anderer Formen schwerer grenzüber-schreitender Kriminalität	Internationale Übereinkünfte	Die Abkommen mit den USA und Australien umfassen 19 Kategorien von Fluggastdaten, einschließlich Angaben zur Person, Reservierung, Bezahlung sowie ergänzende Informationen; das Abkommen mit Kanada enthält 25 ähnliche Datenkategorien.	Zugriff haben das US-Ministerium für Heimatschutz, die kanadische Grenzdienstbe-hörde CBSA sowie der austra-lische Zoll, die die Daten den nationalen für Strafverfolgung und Terrorismus-bekämpfung zu-ständigen Stellen zur Verfügung stellen können.	Die Datenschutz-bestimmungen sind in den einschlägigen internationalen Abkommen festgelegt.	USA: sieben Jahre aktive, acht Jahre passive Nutzung; Australien : 3,5 Jahre aktive, zwei Jahre passive Nutzung; Kanada: 72 Stunden aktive, 3,5 Jahre passive Nutzung.	Die Abkommen mit den USA und mit Australien sind vorläufig anwend-bar; das Ab-kommen mit Kanada ist bereits in Kraft. Die Kommission wird diese Abkommen neu verhandeln. Sechs EU-Mitglied-staaten haben Rechtsvorschriften erlassen, die die Nutzung von Fluggastdaten zu Strafverfolgungs-zwecken ermöglichen.	Jedes Abkommen sieht eine periodische Überprüfung vor, die Abkommen mit Kanada und Australien beinhalten ferner Beendigungs-klauseln.

Tabellarische Übersicht über geltende, in der Umsetzung begriffene und in Betracht gezogene Instrumente

Instrument	Hintergrund	Zweck(e)	Aufbau	Art der personenbezogenen Daten	Datenzugriff	Datenschutz	Datenspeicherung	Stand der Umsetzung	Überprüfung
EU-USA TFTP-Abkommen	Initiative der Kommission	Verhinderung, Aufdeckung, Ermittlung und Verfolgung des Terrorismus und der Terrorismusfinanzierung	Internationales Abkommen	Zahlungsverkehrsdaten, die u.a. Folgendes enthalten: Namen, Kontonummer, Adresse und Kennnummer des Auftraggebers und der Empfänger von Finanztransaktionen	Das US-Finanzministerium kann aus Zahlungsverkehrs daten gewonnene personenbezogene Daten mit den für die Strafverfolgung, die öffentliche Sicherheit bzw. für die Terrorbekämpfung zuständigen US-Behörden, den Mitgliedstaaten, Europol oder Eurojust austauschen. Eine Weiterleitung an Drittstaaten bedarf der Zustimmung der Mitgliedstaaten.	Das Abkommen umfasst strikte Bestimmungen, was die Zweckbindung und die Verhältnismäßigkeit anbelangt.	Aus Zahlungsverkehrsdaten gewonnene personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies für einzelne Ermittlungen oder die Strafverfolgung notwendig ist, nicht extrahierte Daten dürfen nur 5 Jahre gespeichert werden.	Das EP hat dem Abschluss des EU-USA TFTP-Abkommens am 8.Juli 2010 zugestimmt. Es wird nun erwartet, dass der Rat einen Beschluss des Rates zum Abschluss dieses Abkommens annehmen wird, demzufolge das Abkommen dann in Form eines Briefwechsels zwischen beiden Parteien in Kraft tritt.	Die Kommission überprüft das Abkommen sechs Monate nach seinem Inkrafttreten. Sie übermittelt dem EP und dem Rat ihren Evaluierungsbericht.