Rat der
Europäischen Union

Brüssel, den 7. April 2016
(OR. en)

7644/16

JAI 257
COSI 51
FRONT 159
ASIM 49
DAPIX 49
ENFOPOL 86
SIRIS 61
DATAPROTECT 23
VISA 90
FAUXDOC 9
COPEN 96

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Eingangsdatum:	6. April 2016
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2016) 205 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit

Die Delegationen erhalten in der Anlage das Dokument COM(2016) 205 final.

Anl.: COM(2016) 205 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 6.4.2016
COM(2016) 205 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit

1. EINLEITUNG

Die Gesellschaft in Europa ist sehr mobil: Millionen EU-Bürger und Drittstaatangehörige überschreiten jeden Tag die Binnen- und Außengrenzen. Im Jahr 2015 bereisten mehr als 50 Millionen Drittstaatangehörige die EU. Dies entspricht mehr als 200 Millionen Grenzübertritten an den Außengrenzen des Schengen-Raums.

Neben diesem regulären Reiseverkehr kam es allein im Jahr 2015 aufgrund des Konflikts in Syrien und anderer Krisen zu 1,8 Millionen irregulären Grenzübertritten an den EU-Außengrenzen. Die EU-Bürger erwarten, dass die Personenkontrollen an den Außengrenzen wirksam sind und so eine effiziente Steuerung der Migration ermöglichen und zur inneren Sicherheit beitragen. Die Terroranschläge in Paris im Jahr 2015 und im März 2016 in Brüssel haben die anhaltende Bedrohung für die innere Sicherheit Europas auf bittere Weise deutlich gemacht.

Diese beiden Aspekte haben die Notwendigkeit, gemeinsam auf eine umfassende Stärkung des Grenzmanagements, der Rahmenregelungen für die Zusammenarbeit in Migrations- und Sicherheitsfragen und der einschlägigen Informationsinstrumente hinzuwirken, stärker ins Zentrum der Aufmerksamkeit rücken lassen. Grenzmanagement, Strafverfolgung und Migrationssteuerung sind dynamisch miteinander verbunden. Es ist beispielsweise bekannt, dass EU-Bürger die Außengrenzen überschritten haben, um zu terroristischen Zwecken in Konfliktgebiete zu reisen, und nach ihrer Rückkehr eine Gefahr darstellen. Auch ist belegt, dass Terroristen über die Routen der illegalen Migration in die EU gelangt sind und sich anschließend unbemerkt im Schengen-Raum aufgehalten haben.

In der Europäischen Sicherheitsagenda und in der Europäischen Migrationsagenda ist die Richtung für die Entwicklung und Umsetzung der Politik der EU zur Bewältigung der parallel bestehenden Herausforderungen im Bereich der Migrationssteuerung und im Bereich der Bekämpfung von Terrorismus und organisierter Kriminalität vorgegeben worden. Diese Mitteilung baut auf den Synergien zwischen diesen beiden Agenden auf und soll als Ausgangspunkt für eine Diskussion über die Frage dienen, wie die bestehenden und künftige Informationssysteme zu einem besseren Außengrenzen-Management und zur Stärkung der inneren Sicherheit in der EU beitragen könnten. Sie ergänzt den im Dezember 2015 vorgelegten Vorschlag zur Schaffung einer europäischen Grenz- und Küstenwache und zur Verbesserung der Krisenprävention und - intervention an den Außengrenzen.

Es gibt auf EU-Ebene mehrere Informationssysteme, über die Grenzschutz- und Polizeibeamte sachdienliche Personendaten erhalten, doch die vorhandene Datenverwaltungsarchitektur der EU ist nicht perfekt. In dieser Mitteilung werden Möglichkeiten aufgezeigt, wie die Vorteile der vorhandenen Informationssysteme optimal genutzt werden könnten und wie im Bedarfsfall neue und ergänzende Maßnahmen ausgearbeitet werden könnten, um Defizite zu beseitigen. Daneben befasst sich diese Mitteilung mit der bereits vom Europäischen Parlament und vom Rat erkannten Notwendigkeit, langfristig die Interoperabilität der Informationssysteme zu verbessern[1], und sie enthält neue Ideen, wie Informationssysteme künftig so gestaltet

[1] Schlussfolgerungen der Tagung des Europäischen Rates vom 17./18. Dezember 2015; gemeinsame Erklärung der Justiz- und Innenminister der Mitgliedstaaten sowie der Vertreter der EU-Organe zu den Terroranschlägen in Brüssel vom 22. März 2016 in Brüssel (24. März 2016); Schlussfolgerungen des Rates der EU und der im Rat vereinigten Mitgliedstaaten zur Terrorismusbekämpfung vom 20. November 2015.

werden könnten, dass Grenzschutzbeamten, Zollbehörden, Polizeibeamten und Justizbehörden jederzeit die notwendigen Informationen zur Verfügung stehen.

Künftige Initiativen sollen demnach auf der Grundlage der Grundsätze für eine bessere Rechtsetzung, einer öffentlichen Konsultation und einer Abschätzung der Auswirkungen (auch auf die Grundrechte und insbesondere das Recht auf den Schutz personenbezogener Daten) ausgearbeitet werden.

2. ANSTEHENDE HERAUSFORDERUNGEN

Da es im Schengen-Raum keine Binnengrenzen gibt, bedarf es einer starken und verlässlichen Kontrolle des über die Außengrenzen erfolgenden Personenverkehrs. Eine solche Kontrolle ist eine Grundvoraussetzung für die Gewährleistung eines hohen Maßes an innerer Sicherheit und für den freien Personenverkehr im Schengen-Raum. Das Fehlen von Binnengrenzen macht es gleichzeitig erforderlich, dass die Strafverfolgungsbehörden in den Mitgliedstaaten auf sachdienliche Personendaten zugreifen können müssen. Es gibt auf EU-Ebene mehrere Informationssysteme, über die Grenzschutz- und Polizeibeamte sachdienliche Personendaten nach Maßgabe ihres jeweiligen Verwendungszwecks erhalten.[2]

Gleichwohl weisen die Informationssysteme noch bestimmte Mängel auf, die die Arbeit dieser nationalen Behörden behindern. In der Europäischen Sicherheitsagenda wurde daher ein besserer Informationsaustausch als ein vorrangiges Ziel vorgegeben. Die Hauptmängel sind a) suboptimale Funktionen bestehender Informationssysteme, b) bestehende Lücken in der Datenverwaltungsarchitektur der EU, c) die komplexe Landschaft unterschiedlich geregelter Informationssysteme und d) die Fragmentierung der Datenverwaltungsarchitektur für die Grenzkontrolle und -sicherung.

Die in der EU vorhandenen Informationssysteme für das Grenzmanagement und die innere Sicherheit decken ein breites Spektrum von Funktionen ab. Dennoch bestehen nach wie vor **Mängel bei den Funktionen der bestehenden Systeme**. Betrachtet man die geltenden Grenzkontrollverfahren für verschiedene Kategorien von Reisenden, so wird deutlich, dass einige dieser Verfahren und die für sie verwendeten IT-Systeme mit Mängeln behaftet sind. Auch muss die Leistung der vorhandenen Instrumente für die Strafverfolgung optimiert werden. Dies erfordert eine Prüfung von Maßnahmen zur Verbesserung bestehender Informationssysteme (Abschnitt 5).

Zudem bestehen **Lücken in der Datenverwaltungsarchitektur der EU**. So gibt es nach wie vor Probleme bei den Grenzkontrollen für bestimmte Kategorien von Reisenden wie Drittstaatangehörige mit Visum für den längerfristigen Aufenthalt. Außerdem besteht bei von der Visumpflicht ausgenommenen Drittstaatangehörigen eine Informationslücke vor der Ankunft an den Grenzen. Daher sollte geprüft werden, ob es notwendig ist, gegebenenfalls zusätzliche Informationssysteme zu entwickeln, um diese Lücken zu schließen (Abschnitt 6).

Grenzschutz- und Polizeibeamte müssen sich mit einer **komplexen Landschaft unterschiedlich geregelter Informationssysteme** auf EU-Ebene auseinandersetzen. Diese Komplexität führt zu praktischen Schwierigkeiten, insbesondere wenn es zu entscheiden gilt, welche Datenbanken in einer gegeben Situation zu Rate zu ziehen sind.

[2] In Abschnitt 4 wird ein Überblick über die bestehenden Informationssysteme für das Grenzmanagement und die innere Sicherheit gegeben, Anhang 2 enthält eine ausführlichere Übersicht.

Zudem sind nicht alle Mitgliedstaaten an alle bestehenden Systeme angeschlossen.[3] Die derzeitige Komplexität des Zugriffs auf Informationssysteme auf EU-Ebene könnte verringert werden, wenn auf nationaler Ebene eine zentrale Schnittstelle für Suchanfragen geschaffen würde, die den unterschiedlichen Zwecken des Datenzugriffs Rechnung trägt (Abschnitt 7.1).

Die derzeitige Datenverwaltungsarchitektur der EU für die Grenzkontrolle und -sicherheit ist **fragmentiert**. Dies ist auf die unterschiedlichen institutionellen, rechtlichen und politischen Rahmenbedingungen zurückzuführen, unter denen die Systeme entwickelt wurden. Daten werden jeweils getrennt in unterschiedlichen Systemen gespeichert, die nur selten miteinander verbunden sind. Es bestehen Inkompatibilitäten zwischen den Datenbanken, und die zuständigen Behörden haben unterschiedliche Zugriffsmöglichkeiten. Dies kann dazu führen, dass sich insbesondere Strafverfolgungsbehörden nur ein lückenhaftes Gesamtbild machen können, weil es sehr schwierig sein kann, etwaige Verbindungen zwischen Datenfragmenten zu erkennen. Daher ist es dringend erforderlich, integrierte Lösungen für einen besseren, in völliger Übereinstimmung mit den Grundrechten erfolgenden Datenzugriff auf dem Gebiet der Grenzkontrolle und -sicherheit zu entwickeln. Zu diesem Zweck ist es notwendig, einen Prozess zur Verbesserung der Interoperabilität bestehender Informationssysteme einzuleiten (Abschnitt 7).

3. GRUNDRECHTE

Die uneingeschränkte Wahrung der Grundrechte und des Datenschutzes ist eine wesentliche Voraussetzung für die Bewältigung der oben genannten Herausforderungen.

Damit die Grundrechte eingehalten werden, gilt es gut konzipierte Technologien und Informationssysteme zu entwickeln und diese dann ordnungsgemäß einzusetzen. Technologien und Informationssysteme können den Behörden dabei helfen, die Grundrechte der Bürger zu schützen. Biometrische Technologien können die Gefahr von Verwechslungen, Diskriminierungen und Profilerstellungen aufgrund rassischer Merkmale verringern. Sie können, wenn sie mit Maßnahmen zum Schutz der Grundrechte und sonstigen Schutzmaßnahmen einhergehen, zudem dazu beitragen, gegen bestehende Gefahren für Kinder (z.B. Kindesentführungen oder Kinderhandel) vorzugehen. Auch können sie zur Senkung des Risikos beitragen, zu Unrecht festgenommen und verhaftet zu werden. Zudem können sie zur Erhöhung der Sicherheit der Bürger im Schengen-Raum beitragen, da sie bei der Bekämpfung von Terrorismus und schweren Straftaten behilflich sind.

Große Informationssysteme können allerdings auch Risiken für die Privatsphäre mit sich bringen. Diesen gilt es in angemessener Weise vorzubeugen und abzuhelfen. Die Sammlung und die Verwendung personenbezogener Daten in diesen Systemen haben Auswirkungen auf das Recht auf Privatsphäre und den Schutz personenbezogener Daten gemäß der Charta der Grundrechte der Europäischen Union. Daher müssen alle Systeme den Datenschutzvorschriften und den Anforderungen der Notwendigkeit, Verhältnismäßigkeit, Zweckbindung und Datenqualität entsprechen. Es müssen die notwendigen Sicherheitsvorkehrungen getroffen werden, um zu gewährleisten, dass die Rechte der betroffenen Personen auf den Schutz ihrer Privatsphäre und ihrer personenbezogenen Daten gewahrt bleiben. Daten sollten nur so lange gespeichert

[3] Es gelten die besonderen Bestimmungen des Protokolls Nr. 22 in Bezug auf Dänemark und der Protokolle Nr. 21 und 36 in Bezug auf das Vereinigte Königreich und Irland und der jeweiligen Beitrittsakte.

werden, wie es für die Zwecke, für die sie erhoben wurden, erforderlich ist. Darüber hinaus sollten geeignete Mechanismen vorgesehen werden, die ein sorgfältiges Risikomanagement und einen wirksamen Schutz der Rechte der betroffenen Personen gewährleisten.

Die beiden gesetzgebenden Organe haben im Dezember 2015 politische Einigung über die Datenschutzreform erzielt. Die neue Datenschutz-Grundverordnung und die Datenschutz-Richtlinie für Polizei und Justiz[4] werden, sofern sie angenommen werden, im Jahr 2018 in Kraft treten und einen einheitlichen Rahmen für die Verarbeitung personenbezogener Daten bilden.

Die Zweckbindung ist ein zentraler, in der Charta der Grundrechte der Europäischen Union verankerter Grundsatz des Datenschutzrechts. Aufgrund der unterschiedlichen institutionellen, rechtlichen und politischen Rahmenbedingungen, unter denen die Systeme auf EU-Ebene entwickelt wurden, wurde der Grundsatz der Zweckbindung durch eine unterteilte Struktur des Informationsmanagements umgesetzt.[5] Dies ist eine der Ursachen der gegenwärtigen Fragmentierung der Datenverwaltungsarchitektur der EU für die Grenzkontrolle und die innere Sicherheit. Auf der Grundlage der neuen umfassenden Rahmenregelung für den Schutz personenbezogener Daten in der EU und dank wichtiger Entwicklungen auf technologischem Gebiet und bei der IT-Sicherheit könnte der Grundsatz der Zweckbindung beim Zugang zu gespeicherten Daten und bei deren Verwendung künftig leichter und in voller Übereinstimmung mit der Charta der Grundrechte und der jüngsten Rechtsprechung des Europäischen Gerichtshofs umgesetzt werden. Bei integrierten Lösungen für die Datenverwaltung sollte durch Sicherheitsvorkehrungen wie die Aufteilung von Daten innerhalb eines Systems und durch spezifische Zugangs- und Verwendungsbestimmungen für einzelne Datenkategorien die notwendige Zweckbindung sichergestellt werden. Dies schafft Möglichkeiten für größere Interoperabilität von Informationssystemen in Verbindung mit den erforderlichen strikten Zugangs- und Verwendungsbestimmungen ohne Beeinträchtigung der bestehenden Zweckbindung.

Datenschutz durch Technik („data protection by design“) und Datenschutz durch datenschutzfreundliche Voreinstellungen („data protection by default”) sind inzwischen Grundsätze der EU-Datenschutzvorschriften. Die Kommission wird beim Entwurf neuer Instrumente, die sich auf den Einsatz von Informationstechnologien stützen, versuchen, diesem Ansatz zu folgen. Das bedeutet, dass der Schutz personenbezogener Daten in die technische Grundlage des vorgeschlagenen Instruments eingebettet und so die Datenverarbeitung auf das für den angegebenen Zweck erforderliche Mindestmaß begrenzt wird, wobei nur die Instanzen Zugriff auf die Daten haben, die die Daten benötigen.[6]

Die Anforderungen der Charta der Grundrechte und insbesondere der neuen Datenschutzreforminstrumente werden der Kommission als Richtschnur bei ihren Maßnahmen zur Beseitigung der bestehenden Lücken und Mängel in der Datenverwaltungsarchitektur der EU für die Grenzkontrolle und -sicherheit dienen. So ist sichergestellt, dass die Weiterentwicklung der Informationssysteme für diese Bereiche in Übereinstimmung mit den höchsten Datenschutzstandards erfolgen wird und künftige

---

4 Siehe http://ec.europa.eu/justice/data-protection/reform/index_de.htm.

5 KOM(2010) 385 endg.

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

Systeme im Einklang mit der Charta der Grundrechte die Grundrechte wahren und fördern werden.

4. ÜBERBLICK ÜBER DIE BESTEHENDEN INFORMATIONSSYSTEME FÜR DAS GRENZMANAGEMENT UND DIE INNERE SICHERHEIT[7]

Die in der EU vorhandenen Informationssysteme für das Grenzmanagement und die innere Sicherheit haben jeweils eigene Ziele, Zwecke, Rechtsgrundlagen[8], Nutzergruppen und institutionelle Rahmenbedingungen. Zusammengenommen bilden sie ein komplexes Muster einschlägiger Datenbanken.

Die drei wichtigsten **zentralen Informationssysteme**, die die EU entwickelt hat, sind: (i) das Schengener Informationssystem (SIS) mit einem breiten Spektrum von Personen- und Sachfahndungsausschreibungen, (ii) das Visa-Informationssystem (VIS) mit Daten über Visa für den kurzfristigen Aufenthalt und (iii) das EURODAC-System mit den Fingerabdruckdaten von Asylbewerbern und Drittstaatangehörigen, die illegal die Außengrenzen überschritten haben. Diese drei Systeme ergänzen einander, und zielen - mit Ausnahme des SIS - in erster Linie auf Drittstaatangehörige ab. Sie dienen zudem zur Unterstützung der nationalen Behörden bei der Bekämpfung von Kriminalität und Terrorismus.[9] Dies gilt insbesondere für das SIS, das derzeit am häufigsten genutzte Instrument für den Informationsaustausch. Der Informationsaustausch erfolgt bei diesen Systemen in einer gesicherten speziellen Kommunikationsinfrastruktur namens sTESTA[10].

Die Kommission schlägt vor, zusätzlich zu diesen bestehenden Systemen ein viertes zentrales Grenzmanagementsystem einzurichten: das **Einreise-/Ausreisesystem** (EES)[11], das bis 2020 umgesetzt werden und ebenfalls zur Erfassung von Drittstaatangehörigen dienen soll.

---

7 Anhang 2 enthält ein Verzeichnis der bestehenden Informationssysteme für das Grenzmanagement und die Strafverfolgung.

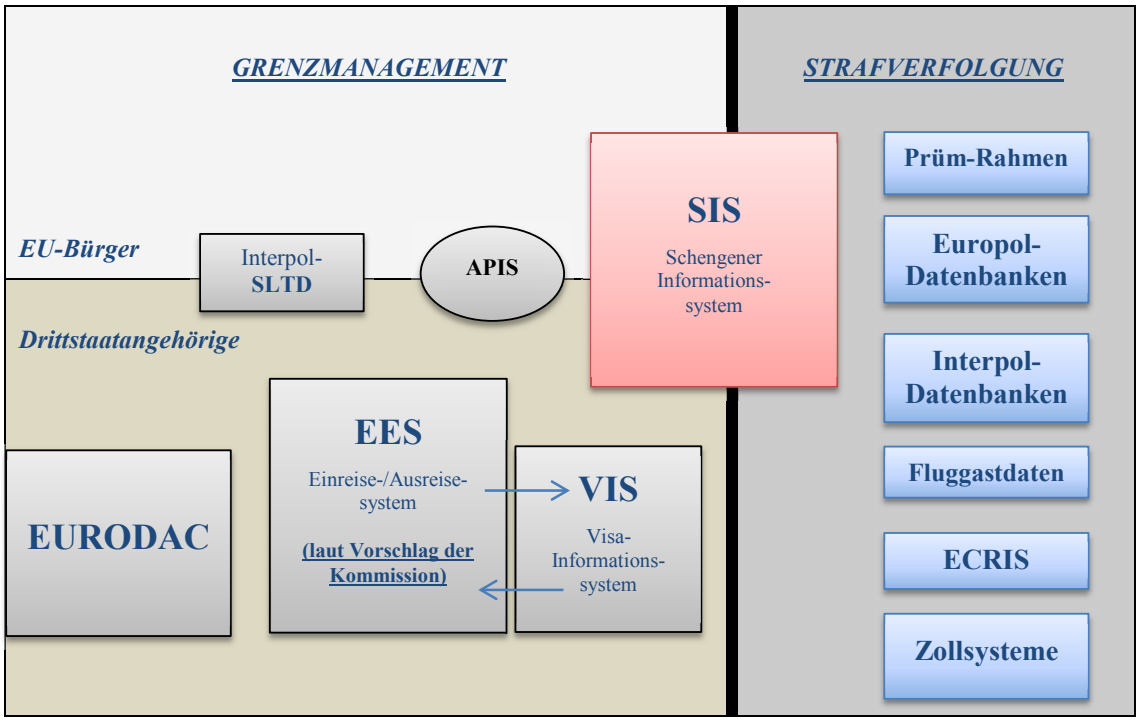
8 Es gelten die besonderen Bestimmungen des Protokolls Nr. 22 in Bezug auf Dänemark und der Protokolle Nr. 21 und 36 in Bezug auf das Vereinigte Königreich.

9 Da die Strafverfolgung ein untergeordnetes Ziel des VIS und des EURODAC-Systems ist, dürfen Strafverfolgungsbehörden unter bestimmten Bedingungen auf diese Systeme zugreifen. Dabei gilt in Bezug auf das VIS, dass die Mitgliedstaaten eine zuständige Behörde benennen müssen, die den Zugang der Strafverfolgungsbehörden kontrolliert, und dass die Polizei nachweisen muss, dass sie den Zugang für strafrechtliche Ermittlungen benötigt. In Bezug auf EURODAC gilt, dass die Ermittlungsbehörde zunächst das nationale AFIS, den Prüm-Rahmen und das VIS zu Rate zu ziehen hat, bevor sie auf EURODAC zugreifen darf.

10 Diese soll in Kürze durch das „TESTA-ng"-Netz ersetzt werden.

11 COM(2016)194 final.

Abbildung 1: *schematischer Überblick über die wichtigsten Informationssysteme für das Grenzmanagement und die Strafverfolgung*



Weitere bestehende Instrumente für das Grenzmanagement sind die Interpol-Datenbank für gestohlene und verlorene Reisedokumente (SLTD) und das Advance Passenger Information System (APIS) für die Erhebung von erweiterten Fluggastdaten vor Flügen in die EU. Diese Instrumente sind von Bedeutung für EU-Bürger und Drittstaatangehörige.

Speziell für Strafverfolgungszwecke, strafrechtliche Ermittlungen und die justizielle Zusammenarbeit hat die EU folgende **dezentrale Instrumente für den Informationsaustausch** entwickelt: (i) Prüm-Rahmen für den Austausch von DNA-, Fingerabdruck- und Fahrzeugregisterdaten und (ii) Europäisches Strafregisterinformationssystem (ECRIS) für den Austausch von Informationen aus den Strafregistern der Mitgliedstaaten. Das ECRIS ermöglicht einen über ein sicheres Netz erfolgenden Austausch von Informationen über bisherige Verurteilungen bestimmter Personen durch Strafgerichte in der Europäischen Union. Die Datenabfragen beruhen hauptsächlich auf alphanumerischen Angaben zur Identität, doch können auch biometrische Daten ausgetauscht werden.

Europol unterstützt den Austausch von Informationen zwischen nationalen Polizeibehörden und Europol als EU-Sammelstelle für kriminalpolizeiliche Informationen. Das Europol-Informationssystem (EIS) ist eine zentrale Datenbank für kriminalpolizeiliche Informationen, in der die Mitgliedstaaten Daten über schwere Straftaten und Terrorismus speichern und abfragen können. Die zuständigen Kontaktstellen bei Europol führen themenspezifische Arbeitsdateien zu Analysezwecken, die Informationen über laufende Maßnahmen in den Mitgliedstaaten enthalten. Europols Netzanwendung für sicheren Datenaustausch (SIENA) ermöglicht den Mitgliedstaaten einen raschen, sicheren und benutzerfreundlichen Austausch von Informationen untereinander, mit Europol oder mit Dritten, die ein Kooperationsabkommen mit Europol geschlossen haben. SIENA ist stark auf die Interoperabilität mit anderen Europol-Systemen ausgerichtet, damit beispielsweise auf direktem Wege Daten mit den

Kontaktstellen ausgetauscht werden können. Es ermöglicht die Eingabe von zwischen den Mitgliedstaaten ausgetauschten Informationen in die Datenbanken von Europol. Für den EU-weiten Austausch von Strafverfolgungsdaten sollte SIENA daher die erste Wahl der Mitgliedstaaten sein.

Darüber hinaus werden in den Mitgliedstaaten weitere Systeme zur Verarbeitung personenbezogener **Fluggastdaten**[12] entwickelt werden. Dabei handelt es sich um bestimmte Angaben, die Fluggäste bei der Flugbuchung und bei der Abfertigung machen müssen.

Ein wichtiger Akteur bei der behördenübergreifenden Zusammenarbeit an den Außengrenzen sind auch die **Zollbehörden**. Sie verfügen über verschiedene Systeme[13] und Datenbanken, in denen Informationen über Warenbewegungen, Wirtschaftsteilnehmer und bestehende Risiken erfasst werden, die zur Stärkung der inneren Sicherheit genutzt werden können. Diese Systeme haben ebenfalls eine eigene kontrollierte, eingeschränkte und sichere Infrastruktur („Gemeinsames Informationsnetz"), die ihre Existenzfähigkeit unter Beweis gestellt hat. Etwaige Synergien und Konvergenzen zwischen den Informationssystemen und der entsprechenden Infrastrukturen für das Grenzmanagement der EU und für Zollvorgänge sollten weiter ausgelotet werden.

5. VERBESSERUNG BESTEHENDER INFORMATIONSSYSTEME

Die in der EU vorhandenen Informationssysteme für das Grenzmanagement und die innere Sicherheit decken ein breites Spektrum von Funktionen ab. Sie weisen jedoch nach wie vor Mängel auf, die es zu beseitigen gilt, um ihre Leistung zu optimieren.

Schengener Informationssystem (SIS)

Die gegenwärtig mit Hilfe des **Schengener Informationssystems** (SIS) durchgeführten Grenzkontrollen erfolgen mittels alphanumerischer Datenabfrage (anhand des Namens und des Geburtsdatums). Fingerabdrücke dürfen nur zur Überprüfung und Bestätigung der Identität von Personen verwendet werden, die bereits anhand ihres Namens identifiziert wurden. Diese Sicherheitslücke macht es ausgeschriebenen Personen möglich, sich mit Hilfe falscher Dokumente einer genauen Identifizierung durch das SIS zu entziehen.

Dieser kritische Mängel soll gemäß dem geltenden Rechtsrahmen[14] durch die Erweiterung des SIS um eine Suchabfragefunktion für Fingerabdrücke **(automatisches Fingerabdruckidentifizierungssystem AFIS)** behoben werden. Das AFIS wird

---

[12] Siehe Abschnitt 6.2.

[13] Das Zollinformationssystem umfasst alle Systeme, die nach Maßgabe des Zollkodex der Gemeinschaft (Verordnung Nr. 2913/92), des künftigen Zollkodex der Union (Verordnung Nr. 952/2013) und der Entscheidung über ein papierloses Arbeitsumfeld für Zoll und Handel (Entscheidung 70/2008/EG) geschaffen wurden, und wurde im Rahmen des ZIS-Übereinkommens von 1995 errichtet. Es soll die Zusammenarbeit zwischen den Zollbehörden der Mitgliedstaaten erleichtern und zur Bekämpfung von Zollvergehen beitragen.

[14] Artikel 22 Buchstabe c der Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L 381 vom 28.12.2006, S. 4) und Beschluss 533/2007/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L 2015 vom 7.8.2007, S. 63).

voraussichtlich Mitte 2017 in Betrieb genommen werden können.[15] Es wird für Europol zugänglich sein und so die Europol-eigenen Systeme für strafrechtliche Ermittlungen und Terrorbekämpfungsmaßnahmen wie auch den Austausch von Fingerabdruckdaten im Prüm-Rahmen sinnvoll ergänzen. Die Kommission und die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) werden prüfen, wie groß die Möglichkeiten für eine derart breite Nutzung des künftigen AFIS sind.

Auf der Grundlage der laufenden Evaluierung und einer technischen Studie prüft die Kommission derzeit **mögliche zusätzliche Funktionen des SIS** im Hinblick auf die Vorlage von Vorschlägen zur Überarbeitung der Rechtsgrundlage des SIS. In Erwägung gezogen werden unter anderem folgende Aspekte:

- Erstellung von SIS-Ausschreibungen von irregulären Migranten, gegen die Rückführungsentscheidungen ergangen sind;
- Verwendung von Gesichtsbildern für die biometrische Identifizierung (zusätzlich zu Fingerabdrücken);
- automatische Informationsübermittlung bei einem Überprüfungstreffer;
- Speicherung der betreffenden Informationen nach einem Treffer bei Ausschreibungen zum Zwecke der verdeckten Kontrolle und der gezielten Kontrolle in der SIS-Zentraleinheit;
- Einführung einer neuen Ausschreibungskategorie „gesuchte unbekannte Person" für Personen, über die möglicherweise kriminaltechnische Daten in nationalen Datenbanken (z. B. ein an einem Tatort hinterlassener Fingerabdruck) vorliegen.[16]

Die Kommission wird weiterhin mit EU-Mitteln die Umsetzung von Projekten fördern, die eine gleichzeitige Abfrage im SIS und in den Interpol-Datenbanken für gestohlene und verlorene Reisedokumente (SLTD) bzw. gesuchte Straftäter, Fahrzeuge oder Feuerwaffen (iARMS) ermöglichen und die Informationssysteme der EU ergänzen.[17]

Interpol-Datenbank für gestohlene und verlorene Reisedokumente (SLTD)

Für ein wirksames Grenzmanagement ist es von zentraler Bedeutung, dass die Reisedokumente aller Drittstaatangehörigen und EU-Bürger mit der **SLTD-Datenbank** abgeglichen werden können. Die Strafverfolgungsbehörden sollten die SLTD-Datenbank auch für Datenabfragen im Schengen-Raum nutzen. Nach den Terroranschlägen in Paris vom 13. November 2015 hat der Rat gefordert, bis März 2016 an allen Grenzübergängen an den Außengrenzen elektronische Verbindungen zu den einschlägigen Interpol-Datenbanken herzustellen und einen automatischen Abgleich von Reisedokumenten einzuführen.[18] Alle Mitgliedstaaten sollten derartige elektronische Verbindungen

[15] Im März 2016 hat die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Verfügbarkeit und Einsatzfähigkeit der Technologie zur Identifizierung von Personen anhand der Fingerabdruckdaten des Schengener Informationssystem der zweiten Generation (SIS II) vorgelegt.

[16] Die Möglichkeit einer solchen neuen Ausschreibung wird im Hinblick auf das Ziel geprüft werden, komplementäre Lösungen zu ermitteln und Überschneidungen mit dem bestehenden Prüm-Rahmen für den Fingerabdruckabgleich mit den unterschiedlichen nationalen Datenbanken der Mitgliedstaaten zu vermeiden.

[17] Die von Interpol entwickelten Werkzeuge für die Informationssuche wie die fest installierte und vernetzte Datenbank FIND (Fixed Interpol Networked Database) und die mobile vernetzte Datenbank MIND (Mobile Interpol Networked Database) sollen die gleichzeitige Abfrage der Systeme von Interpol und des SIS erleichtern.

[18] Schlussfolgerungen des Rates der EU und der im Rat vereinigten Mitgliedstaaten zur Terrorismusbekämpfung vom 20. November 2015.

herstellen und geeignete Systeme für die automatische Aktualisierung der Daten zu gestohlenen oder verlorenen Reisedokumenten in der SLTD-Datenbank einführen.

Advance Passenger Information System (APIS)

Die Mitgliedstaaten sollten zudem nach bewährter Praxis einen automatischen Abgleich der im **Advance Passenger Information System** (APIS) gespeicherten Ausweisdaten mit dem SIS und der SLTD-Datenbank von Interpol einführen und so den Nutzen des APIS erhöhen. Die Kommission wird prüfen, inwieweit es erforderlich ist, die Rechtsgrundlage für die Verarbeitung der Ausweisdaten zu ändern, um eine breitere Nutzung des Systems zu ermöglichen, und wieweit es notwendig ist, in die Rechtsgrundlage eine Bestimmung aufzunehmen, welche die Mitgliedstaaten verpflichtet, für alle ankommenden und abgehenden Flüge Ausweisdaten anzufordern und zu verarbeiten. Dies ist besonders relevant im Kontext der Umsetzung der künftigen Richtlinie über Fluggastdatensätze, denn durch eine kombinierte Verwendung von Fluggastdaten und Ausweisdaten würde der Nutzen von Fluggastdaten für die Bekämpfung von Terrorismus und schwerer Kriminalität erhöht.[19]

Visa-Informationssystem (VIS)

Die Kommission führt zurzeit eine umfassende Evaluierung des **Visa-Informationssystems** (VIS) durch, die im Jahr 2016 abgeschlossen werden soll. Dabei wird unter anderem geprüft, wie das VIS für Kontrollen an den Außengrenzen und im Hoheitsgebiet der Mitgliedstaaten genutzt wird und wie es zur Bekämpfung von Identitäts- und Visumbetrug beiträgt. Auf der Grundlage der Ergebnisse wird die Kommission anschließend prüfen, wie sich die Funktionen des VIS verbessern lassen, beispielsweise durch

- Erhöhung der Qualität von Gesichtsbildern, um den Abgleich biometrischer Daten zu ermöglichen;
- Verwendung der biometrischen Daten von Visumantragstellern für die Suche im künftigen automatischen Fingerabdruckidentifizierungssystem, das für das SIS entwickelt werden soll;
- Senkung der Altersgrenze für die Erfassung von Fingerabdrücken von Kindern im Alter zwischen 6 und 12 Jahren bei gleichzeitiger Einführung robuster Maßnahmen zum Schutz der Grundrechte und sonstiger Schutzmaßnahmen;[20]
- Vereinfachung der Abfrage der SLTD-Datenbank von Interpol bei der Beantragung eines Visums.

Die Möglichkeiten, die der bestehende Rechtsrahmen in Bezug auf den Zugang zum VIS für **Strafverfolgungszwecke** bietet, werden von den Mitgliedstaaten bisher in unterschiedlichem Maße genutzt. In diesem Zusammenhang haben die Mitgliedstaaten praktische Probleme bei den Verfahren zum Zugang der Strafverfolgungsbehörden zum VIS gemeldet. Ebenso ist die Umsetzung des zu Strafverfolgungszwecken erfolgenden Zugangs zu EURODAC noch immer sehr begrenzt. Die Kommission wird prüfen, ob es notwendig ist, den rechtlichen Rahmen für den Zugang der Strafverfolgungsbehörden zum VIS und zu EURODAC zu überdenken.

EURODAC

Die Kommission wird, wie in ihrer Mitteilung „Reformierung des Gemeinsamen Europäischen Asylsystems und Erleichterung legaler Wege nach Europa"[21] angekündigt,

[19] Siehe Abschnitt 6.2 über die vorgeschlagene Richtlinie über Fluggastdatensätze.

[20] Soweit technisch machbar laut der einschlägigen Studie des GFS über die Fingerabdruckidentifizierung bei Kindern (EUR 26193 EN; ISBN 978-92-79-33390-3Children', 2013).

einen Vorschlag zur Reform von EURODAC unterbreiten, durch den dessen Funktionen im Zusammenhang mit der irregulärer Migration und Rückkehr bzw. Rückführung weiter ausgebaut werden sollen. Dadurch soll die derzeit noch fehlende Möglichkeit geschaffen werden, Sekundärbewegungen illegaler Migranten zwischen den Mitgliedstaaten zu überwachen. Darüber hinaus wird der Vorschlag darauf abzielen, Mittel für eine beschleunigte Identifizierung und Ausstellung neuer Ausweispapiere für Migranten bereitzustellen, um die Effizienz der Rückführungs- und Rückübernahmeverfahren zu erhöhen. In diesem Zusammenhang wird der Vorschlag auch den Austausch von EURODAC-Daten mit Drittländern unter Berücksichtigung der erforderlichen Datenschutzgarantien aufgreifen.

Europol

Die EU gewährt **Europol** Zugang zu ihren zentralen Datenbanken, doch Europol macht von dieser Möglichkeit bisher noch nicht in vollem Umfang Gebrauch. Europol darf auf die im SIS gespeicherten Daten über Festnahmen, verdeckte oder gezielte Kontrollen und beschlagnahmte Gegenstände auf direktem Wege zugreifen und diesbezügliche Suchabfragen vornehmen. Bisher hat Europol nur eine relativ begrenzte Anzahl von Suchabfragen im SIS vorgenommen. Der Zugang zum VIS zum Zwecke der Datenabfrage ist für Europol seit September 2013 rechtlich möglich. Auf EURODAC-Daten darf Europol gemäß der EURODAC-Rechtsgrundlage seit Juli 2015 zugreifen. EURODAC sollte seine laufenden Arbeiten für seine Anbindung an das VIS und EURODAC beschleunigen. Die Kommission wird generell prüfen, ob es notwendig ist, auch anderen im Bereich Inneres tätigen EU-Agenturen Zugang zu Informationssystemen zu gewähren; dies gilt insbesondere für die künftige europäische Grenz- und Küstenwache.

Prüm-Rahmen

Der **Prüm-Rahmen** wird derzeit nicht optimal genutzt. Dies ist darauf zurückzuführen, dass nicht alle Mitgliedstaaten ihren rechtlichen Pflichten in Bezug auf die Anbindung des Netzes an in ihre eigenen Systeme nachgekommen sind. Die Mitgliedstaaten haben beträchtliche finanzielle und technische Unterstützung für die Umsetzung des Prüm-Rahmens erhalten und sollten ihn nun vollständig umsetzen. Die Kommission nutzt die ihr übertragenen Befugnisse zur Gewährleistung der vollständigen Umsetzung der rechtlichen Pflichten der Mitgliedstaaten und hat im Januar 2016 einen strukturierten Dialog (EU-Pilot) mit den betroffenen Mitgliedstaaten begonnen. Falls sich die Antworten der Mitgliedstaaten als nicht zufriedenstellend erweisen, wird die Kommission nicht zögern, Vertragsverletzungsverfahren einzuleiten.

Europäisches Strafregisterinformationssystem (ECRIS)

Das Europäische Strafregisterinformationssystem **ECRIS** ermöglicht den Austausch von Informationen über Verurteilungen von Drittstaatangehörigen und Staatenlosen, doch es gibt hierfür kein effizientes Verfahren. Die Kommission hat im Januar 2016 einen Legislativvorschlag[22] angenommen, durch den dieser Mangel behoben werden soll. Darin ist vorgesehen, dass den nationalen Behörden ermöglicht wird, auf der Grundlage von Fingerabdrücken Daten über Drittstaatangehörige abzufragen, um eine sichere Identifizierung zu gewährleisten. Das Europäische Parlament und der Rat werden die betreffende Richtlinie voraussichtlich noch im Jahr 2016 erlassen.

---

[21] COM(2016)197 final.
[22] COM(2016) 7 final vom 19.1.2016.

Übergreifende Aspekte

Ein allgemeines Problem im Zusammenhang mit den Informationssystemen ist der **Grad ihrer Umsetzung** durch die Mitgliedstaaten. Die ungleiche Umsetzung des Prüm-Rahmens und die fehlenden elektronischen Anbindungen an die SLTD-Datenbank liefern hierfür ein deutliches Beispiel. Um den Grad der Umsetzung der Informationssysteme zu erhöhen, wird die Kommission die diesbezüglichen Fortschritte aller Mitgliedstaaten aufmerksam verfolgen.[23] Dabei wird sie nicht nur prüfen, ob die Mitgliedstaaten ihren rechtlichen Pflichten im Bereich der Informationssysteme nachkommen, sondern auch analysieren, wie sie die vorhandenen Instrumente nutzen und ob sie bewährte Praktiken anwenden. Bei der Überwachung und Förderung der Umsetzung wird sich die Kommission auf unterschiedliche Quellen stützen, darunter die Mitteilungen der Mitgliedstaaten und die Ortsbesichtigungen im Rahmen des Schengener Evaluierungs- und Überwachungsmechanismus.

Ein weiteres allgemeines Problem im Zusammenhang mit den Informationssystemen ist die **Qualität der eingegebenen Daten**. Wenn die Mitgliedstaaten nicht die Mindestqualitätsanforderungen einhalten, sind die Zuverlässigkeit und der Wert der gespeicherten Daten nur sehr gering, und mit zunehmender Wahrscheinlichkeit falscher oder fehlender Treffer verringert sich der Wert der betreffenden Informationssysteme. Um die Qualität der eingegebenen Daten zu verbessern, wird eu-LISA **Kapazitäten für eine zentrale Überwachung der Datenqualität** der ihrer Zuständigkeit unterliegenden Systeme entwickeln.

In den meisten Informationssystemen im Bereich der Grenzkontrolle und -sicherheit werden Identifikationsdaten aus Reise- und Identitätsdokumenten verarbeitet. Um das Grenzmanagement und die innere Sicherheit zu verbessern, muss nicht nur die Leistung der betreffenden Informationssysteme verbessert, sondern auch eine einfache und sichere Echtheitsprüfung von Reise- und Identitätsdokumenten sichergestellt werden. Zu diesem Zweck wird die Kommission Maßnahmen zur Verbesserung der Sicherheit elektronischer Dokumente und des Identitätsmanagements sowie zur Bekämpfung von Dokumentenbetrug vorschlagen. Die im Wege der eIDAS-Verordnung[24] erreichbare Interoperabilität sicherer Identifizierungen könnte ein geeignetes Mittel hierfür sein.

Maßnahmen zur Verbesserung bestehender Informationssysteme

Schengener Informationssystem (SIS)

- Entwicklung und Implementierung eines automatischen Fingerabdruckidentifizierungssystems (AFIS) für das SIS durch die Kommission und eu-LISA bis Mitte 2017
- Vorlage (spätestens Ende 2016) von Vorschlägen der Kommission zur Überarbeitung der Rechtsgrundlage des SIS im Hinblick auf die Einführung neuer Systemfunktionen
- größtmögliche Nutzung des SIS durch die Mitgliedstaaten durch Eingabe aller sachdienlichen Informationen und durch Abfrage des Systems bei Bedarf

[23] Es gelten die besonderen Bestimmungen des Protokolls Nr. 22 in Bezug auf Dänemark und der Protokolle Nr. 21 und 36 in Bezug auf das Vereinigte Königreich.

[24] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

Interpol-Datenbank für gestohlene und verlorene Reisedokumente (SLTD)

- Maßnahmen der Mitgliedstaaten für eine elektronische Anbindung an die einschlägigen Interpol-Datenbanken an allen Grenzübergängen an den Außengrenzen
- Einhaltung der den Mitgliedstaaten obliegenden Pflicht, Daten über gestohlene oder verlorene Reisedokumente gleichzeitig in das SIS und in die SLTD-Datenbank einzugeben bzw. dort abzufragen

Advance Passenger Information System (APIS)

- Maßnahmen der Mitgliedstaaten zur Sicherstellung des automatischen Abgleichs von Ausweisdaten mit dem SIS und der Interpol-Datenbank für gestohlene und verlorene Reisedokumente (SLTD) im Einklang mit den bestehenden bewährten Verfahren
- Prüfung durch die Kommission, ob die Rechtsgrundlage für die Verarbeitung von Ausweisdaten überarbeitet werden muss

Visa-Informationssystem (VIS)

- Prüfung durch die Kommission, wie das VIS weiter verbessert werden könnte, bis Ende 2016

EURODAC

- Vorlage eines Vorschlags der Kommission zur Änderung der Rechtsgrundlage von EURODAC zum weiteren Ausbau der EURODAC-Funktionen im Zusammenhang mit der irregulären Migration und der Rückkehr bzw. Rückführung

Europol

- vollständige Nutzung der Europol-eigenen Zugangsrechte für die Abfrage von SIS-, VIS- und EURODAC-Daten
- gemeinsame Maßnahmen von Kommission und Europol zur Erforschung und Förderung von Synergien zwischen dem Europol-Informationssystem (EIS) und anderen Systemen (und insbesondere dem SIS)
- gemeinsame Prüfung durch die Kommission und eu-LISA, ob das automatische Fingerabdruckidentifizierungssystem (AFIS), das für das SIS entwickelt werden soll, die Europol-eigenen Systeme für strafrechtliche Ermittlungen und Terrorbekämpfungsmaßnahmen sinnvoll ergänzen könnte

Prüm-Rahmen

- vollständige Umsetzung und Anwendung des Prüm-Rahmens durch die Mitgliedstaaten
- erforderlichenfalls Einleitung eines Vertragsverletzungsverfahrens der Kommission gegen Mitgliedstaaten, die sich noch nicht an den Prüm-Rahmen angeschlossen haben
- gemeinsame Prüfung durch die Kommission und eu-LISA, ob das automatische Fingerabdruckidentifizierungssystem (AFIS), das für das SIS entwickelt werden soll, den im Prüm-Rahmen erfolgenden Austausch von Fingerabdruckdaten sinnvoll ergänzen könnte

Europäisches Strafregisterinformationssystem (ECRIS)

- Erlass der von der Kommission vorgeschlagenen Richtlinie des Europäischen Parlaments und des Rates noch im Jahr 2016, damit die nationalen Behörden künftig auf der Grundlage von Fingerabdrücken ECRIS-Daten über Drittstaatangehörige abfragen können

Übergreifende Aspekte

- Maßnahmen der Kommission zur **Überwachung und Förderung der Umsetzung** der einschlägigen Informationssysteme
- Maßnahmen von eu-LISA zum **Aufbau von Kapazitäten für eine zentrale Überwachung der Datenqualität** der ihrer Zuständigkeit unterliegenden Informationssysteme
- Vorschläge der Kommission für Maßnahmen zur **Verbesserung der Sicherheit elektronischer Dokumente und des Identitätsmanagements** sowie zur Bekämpfung von Dokumentenbetrug
- Maßnahmen der Kommission zur Auslotung etwaiger Synergien und Konvergenzen zwischen den Informationssystemen und den entsprechenden Infrastrukturen für das Grenzmanagement der EU und für **Zollvorgänge**

6. ENTWICKLUNG ZUSÄTZLICHER INFORMATIONSSYSTEME UND LÜCKENBESEITIGUNG

Die bestehenden Informationssysteme decken ein sehr breites Spektrum von Daten ab, die für das Grenzmanagement und die Strafverfolgung benötigt werden. Dennoch gibt es noch große Lücken. Die Kommission hat, um einige dieser Lücken zu beseitigen, Legislativvorschläge zur Schaffung eines Einreise-/Ausreisesystems sowie für eine EU-weite Erfassung von Fluggastdatensätzen vorgelegt. Bei anderen erkannten Lücken gilt es sorgfältig zu prüfen, ob zusätzliche EU-Instrumente erforderlich sind.

1. Einreise-/Ausreisesystem

Die Kommission hat parallel zu dieser Mitteilung überarbeitete Legislativvorschläge für die Einführung eines Einreise-/Ausreisesystems vorgelegt. Nach der Annahme durch die beiden gesetzgebenden Organe soll eu-LISA das vorgeschlagene System in Zusammenarbeit mit den Schengen-Mitgliedstaaten entwickeln und umzusetzen.

Das Einreise-/Ausreisesystem soll zur Erfassung der Grenzübertritte (Ein- und Ausreisen) von visumpflichtigen oder visumbefreiten Drittstaatangehörigen dienen, die für einen Kurzaufenthalt von höchstens 90 Tagen in einem Zeitraum von 180 Tagen oder für Aufenthalte auf der Grundlage des neuen Rundreisevisums (bis zu einem Jahr) in den Schengen-Raum einreisen. Mit dem Einreise-/Ausreisesystem sollen folgende Ziele verfolgt werden: a) besseres Management der Außengrenzen, b) Eindämmung der irregulären Migration durch gezieltes Vorgehen gegen die Überschreitung der zulässigen Aufenthaltsdauer und c) Beitrag zur Bekämpfung von Terrorismus und schwerer Kriminalität und somit zur Sicherstellung eines hohen Maßes an innerer Sicherheit.

Im Einreise-/Ausreisesystem sollen Kenndaten von Drittstaatangehörigen (alphanumerische Daten, vier Fingerabdrücke und ein Gesichtsbild) sowie die Angaben aus ihren Reisedokumenten erfasst und mit elektronischen Aufzeichnungen über die Ein- und Ausreise verknüpft werden. Die derzeitige Praxis des Abstempelns der Reisedokumente soll eingestellt werden. Das Einreise-/Ausreisesystem soll eine effiziente Kontrolle der Einhaltung der zulässigen Aufenthaltsdauer bei Kurzaufenthalten, eine stärkere Automatisierung der Grenzkontrollen und eine bessere Aufdeckung von Dokumenten- und Identitätsbetrug ermöglichen. Durch die zentrale Erfassung sollen Personen ermittelt werden können, die die zulässige Aufenthaltsdauer überschritten haben oder sich ohne gültige Ausweispapiere im Schengen-Raum aufhalten. Durch das vorgeschlagene Einreise-/Ausreisesystem soll somit eine wichtige Lücke in der Landschaft der bestehenden Informationssysteme geschlossen werden.

2. Fluggastdaten

Fluggastdatensätze (PNR-Daten) bestehen aus Buchungsdaten mit Angaben zur Person, vollständigen Reise- und Reservierungsdetails, besonderen Bemerkungen und Informationen über den Sitzplatz, das Gepäck und das Zahlungsmittel. PNR-Daten sind nützlich und erforderlich, um Reisende mit erhöhtem Risikopotenzial vor dem Hintergrund der Bekämpfung des Terrorismus, des Drogenhandels, des Menschenhandels, der sexuellen Ausbeutung von Kindern und anderen schweren Straftaten ermitteln zu können. Die vorgeschlagene PNR-Richtlinie soll eine bessere Zusammenarbeit zwischen den nationalen Systemen ermöglichen und die zwischen den Mitgliedstaaten bestehenden Sicherheitslücken verringern. Sie zielt darauf ab, die große Lücke zu schließen, die in Bezug auf die Verfügbarkeit von Daten besteht, die für die Bekämpfung der schweren Kriminalität und des Terrorismus benötigt werden. **Die Richtlinie über Fluggastdatensätze sollte daher dringend erlassen und umgesetzt werden.**

Sie sieht vor, dass die Mitgliedstaaten PNR-Zentralstellen (PIU) einrichten, die PNR-Daten von den Fluggesellschaften erhalten. Dabei geht es nicht um die Einrichtung eines zentralen Systems oder einer zentralen Datenbank, sondern um eine gewisse Vereinheitlichung der auf nationaler Ebene bestehenden technischen Lösungen und Verfahren. Dadurch soll der Austausch von PNR-Daten zwischen den PNR-Zentralstellen gemäß der vorgeschlagenen Richtlinie vereinfacht werden. Zu diesem Zweck wird die Kommission die Mitgliedstaaten bei der Analyse verschiedener Szenarien für die Vernetzung der PNR-Zentralstellen unterstützen, damit standardisierte Lösungen und Verfahren entwickelt werden. Nach dem Erlass der Richtlinie wird die Kommission die laufenden Arbeiten an gemeinsamen Protokollen und unterstützten Datenformaten für die Übermittlung von PNR-Daten durch die Fluggesellschaften an die PNR-Zentralstellen beschleunigen. Sie wird zudem binnen drei Monaten nach dem Erlass der Richtlinie einen Vorschlag für einen einschlägigen Durchführungsrechtsakt vorlegen.

3. Informationslücke vor der Ankunft von der Visumpflicht befreiter Drittstaatangehöriger

Während bei Visuminhabern Angaben zur Person, Kontaktdaten und Hintergrundinformationen im VIS erfasst werden, stammen die über von der Visumpflicht befreiten Personen vorliegenden Informationen ausschließlich aus deren Reisedokumenten. Bei auf dem Luft- oder Seeweg eintreffenden Reisenden können diese Informationen vor der Ankunft durch Fluggastdaten ergänzt werden. Die vorgeschlagene PNR-Richtlinie sieht vor, dass die Fluggastdaten dieser Personen auch erhoben werden, wenn sie auf dem Luftweg in die EU einreisen. Über Personen, die über Landgrenzen in die EU einreisen, liegen vor der Ankunft an der Außengrenze der EU keine Informationen vor.

Zwar können Strafverfolgungsbehörden Informationen über Visuminhaber aus dem VIS abfragen, wenn dies für die Bekämpfung der schweren Kriminalität und des Terrorismus erforderlich ist, doch über von der Visumpflicht befreite Personen sind keine vergleichbaren Daten verfügbar. Dieser Mangel an Informationen ist in einer Situation, in der eine große Zahl von der Visumpflicht befreiter Reisender per Pkw, Bus oder Bahn in die EU einreisen möchte, von besonderer Bedeutung für das Management der Landgrenzen der EU. Die Bürger mehrerer Nachbarländer der EU sind bereits von der Visumpflicht befreit, und die laufenden Gespräche zwischen der EU und weiteren Nachbarländern über Visaliberalisierungen schreiten voran. Dies wird wahrscheinlich in naher Zukunft zu einer erheblichen Zunahme der Zahl der von der Visumpflicht befreiten Reisenden führen.

Die Kommission wird prüfen, ob ein neues Instrument der EU zur Bewältigung dieses Problems notwendig, machbar und angemessen ist. Eine Möglichkeit, die in Betracht gezogen werden könnte, wäre die Schaffung eines **EU-weiten Reiseinformations- und -genehmigungssystems** (ETIAS), in das von der Visumpflicht befreite Reisende sachdienliche Angaben über geplante Reisen eingeben müssten. Die automatische Verarbeitung dieser Informationen könnte den Grenzschutzbeamten bei der Bewertung von aus Drittländern stammenden Besuchern, die für einen Kurzaufenthalt einreisen möchten, behilflich sein. Länder wie die USA, Kanada und Australien haben bereits ähnliche Systeme eingeführt, die auch für EU-Bürger gelten.

Reisegenehmigungssysteme beruhen auf Online-Anträgen, in denen der Antragsteller vor Reiseantritt Angaben zu seiner Person, zu Kontaktdaten, zum Zweck der Reise, zur Reiseroute usw. macht. Wenn die Genehmigung erteilt wird, verlaufen die Grenzverfahren bei der Ankunft schneller und reibungsloser. Unabhängig von den Vorteilen, die ein System wie ETIAS für die Sicherheit und das Grenzmanagement hätte, und von seiner möglichen Bedeutung im Zusammenhang mit der Visa-Reziprozität, könnte ein solches System somit auch als Instrument für die Reiseerleichterung dienen.

4. Europäisches Polizeiregisterinformationssystem (EPRIS)

In der Europäischen Sicherheitsagenda wird betont, dass es auf dem Gebiet des Informationsaustausches weiterer Arbeiten bedarf, um künftig eine zeitnahe Verfügbarkeit polizeilicher Daten in allen Mitgliedstaaten zu gewährleisten. Die Kommission wird prüfen, inwieweit es erforderlich, technisch machbar und angemessen ist, ein Europäisches Polizeiregisterinformationssystem (EPRIS) zu schaffen, um den grenzübergreifenden Zugang zu Informationen in nationalen Datenbanken der Strafverfolgungsbehörden zu vereinfachen. Die Kommission unterstützt in diesem Zusammenhang mit EU-Mitteln ein von fünf Mitgliedstaaten durchgeführtes Pilotprojekt zur Entwicklung eines Verfahrens für die automatische grenzübergreifende Abfrage nationaler Strafregistern mit dem Abfrageergebnis „Treffer"/„kein Treffer".[25] Die Kommission wird die Ergebnisse des Projekts bei ihrer Bewertung berücksichtigen.

Maßnahmen zur Entwicklung zusätzlicher Informationssysteme und zur Beseitigung von Informationslücken

Einreise-/Ausreisesystem (EES)

- vorrangige Behandlung des einschlägigen Legislativvorschlags durch das Europäische Parlament und den Rat zwecks Erlass bis spätestens Ende 2016

Fluggastdaten (PNR)

- Erlass der Richtlinie über Fluggastdatensätze durch das Europäische Parlament und den Rat bis spätestens April 2016
- dringliche Maßnahmen der Mitgliedstaaten zur Umsetzung der Richtlinie nach deren Erlass

[25] Das Pilotprojekt für den automatischen Datenaustausch (ADEP) zielt auf die Schaffung eines technischen Systems ab, bei dem anhand eines Indexes nachgesehen werden kann, ob in einem Mitgliedstaat oder in mehreren Mitgliedstaaten Polizeiakten über eine gegebene Person oder über eine kriminalpolizeiliche Untersuchungen vorliegen. Die automatische Antwort auf eine Suchanfrage in diesem Index würde jeweils nur angeben, ob Daten verfügbar sind oder nicht („Treffer"/„kein Treffer"). Bei einem Treffer müssten in einem zweiten Schritt zusätzliche personenbezogene Daten über die üblichen Kanäle für die polizeiliche Zusammenarbeit angefordert werden.

- Unterstützung des Datenaustauschs zwischen PNR-Zentralstellen durch die Kommission in Form standardisierter Lösungen und Verfahren.
- Vorlage eines Vorschlags für einen Durchführungsbeschluss der Kommission über gemeinsame Protokolle und unterstützte Datenformate für die Übermittlung von PNR-Daten durch die Fluggesellschaften an die PNR-Zentralstellen innerhalb von drei Monaten nach dem Erlass der Richtlinie über Fluggastdatensätze

Informationslücke vor der Ankunft von der Visumpflicht befreiter Drittstaatangehöriger

- von der Kommission im Jahr 2016 durchzuführende Prüfung, inwieweit es erforderlich, technisch machbar und angemessen ist, ein neues EU-Instrument wie ein EU-weites Reiseinformations- und -genehmigungssystem zu schaffen

Europäisches Polizeiregisterinformationssystem (EPRIS)

- im Jahr 2016 von der Kommission durchzuführende Prüfung, inwieweit es erforderlich, technisch machbar und angemessen ist, ein Europäisches Polizeiregisterinformationssystem (EPRIS) zu schaffen

7. VERBESSERUNG DER INTEROPERABILITÄT VON INFORMATIONSSYSTEMEN

Unter Interoperabilität versteht man die Fähigkeit von Informationssystemen, Daten auszutauschen und die gemeinsame Nutzung von Informationen zu ermöglichen. Es gibt **vier verschiedene Aspekte der Interoperabilität**, die alle bestimmte rechtliche[26], technische und operative Fragen (u.a. im Zusammenhang mit dem Datenschutz) aufwerfen:

- eine zentrale Schnittstelle, die die gleichzeitige Abfrage mehrere Informationssysteme und die Anzeige aller Ergebnisse auf einem einzigen Bildschirm ermöglicht
- die Interoperabilität von Informationssystemen, bei denen die in einem System erfassten Daten automatisch von einem anderen System abgefragt werden
- die Einrichtung eines gemeinsamen Dienstes für den Abgleich biometrischer Daten zur Unterstützung verschiedener Informationssysteme
- ein gemeinsamer Datenspeicher für unterschiedliche Informationssysteme (Kernmodul)

Um einen Prozess zur Förderung der Interoperabilität der Informationssysteme auf EU-Ebene einzuleiten, wird die Kommission eine **Sachverständigengruppe „Informationssysteme und Interoperabilität"** einsetzen, der hochrangige Vertreter der EU-Agenturen, nationale Sachverständige und Vertreter der betroffenen institutionellen Interessenträger angehören werden. Die Sachverständigengruppe wird sich mit den rechtlichen, technischen und operativen Aspekten der verschiedenen Optionen für die Herstellung der Interoperabilität von Informationssystemen befassen und insbesondere die Notwendigkeit, die technische Durchführbarkeit und die Angemessenheit der verfügbaren Optionen und ihre Auswirkungen auf den Datenschutz prüfen. Sie soll sich in diesem Zusammenhang mit den derzeitigen Mängeln und Informationslücken befassen, die durch die Komplexität und die Fragmentierung der Informationssysteme auf europäischer Ebene bedingt sind. Die Sachverständigengruppe soll sich aus einem breiten und umfassenden Blickwinkel mit den Themen Grenzmanagement und

[26] Es gelten die besonderen Bestimmungen des Protokolls Nr. 22 in Bezug auf Dänemark und der Protokolle Nr. 21 und 36 in Bezug auf das Vereinigte Königreich.

Strafverfolgung befassen und dabei auch die Rolle, die Aufgaben und die Systeme der Zollbehörden berücksichtigen. Ihre Arbeitsmethoden sollen Synergieeffekte aus allen einschlägigen Erfahrungen ermöglichen, die in der Vergangenheit allzu oft isoliert voneinander ausgewertet wurden.

Auf diese Weise sollen ein strategisches Gesamtbild der künftigen Datenverwaltungsarchitektur der EU für die Grenzkontrolle und -sicherheit und mögliche Implementierungslösungen entworfen werden.

Dieser Konsultationsprozess wird **von folgenden Zielen geleitet** werden:

- Informationssysteme sollten einander ergänzen. Überschneidungen sollten vermieden bzw. beseitigt werden. Gegen Lücken sollte in angemessener Weise vorgegangen werden.
- Es sollte ein modularer Ansatz verfolgt werden, bei dem technologische Entwicklungen in vollem Umfang genutzt werden und nach den Grundsätzen des „eingebauten Datenschutzes“ verfahren wird.
- Von Beginn an sollte die volle Achtung aller Grundrechte von Unionsbürgern und Drittstaatangehörigen im Einklang mit der Charta der Grundrechte sichergestellt sein.
- Wo es erforderlich und machbar ist, sollten Informationssysteme miteinander verbunden und interoperabel sein. Die gleichzeitige Abfrage von Systemen sollte vereinfacht werden, damit den Grenzschutz- oder Polizeibeamten alle sachdienlichen Informationen zur Verfügung stehen, wenn und wo diese notwendig ist, damit sie ihren Aufgaben nachkommen können, ohne dass bestehende Zugangsrechte geändert werden müssen.

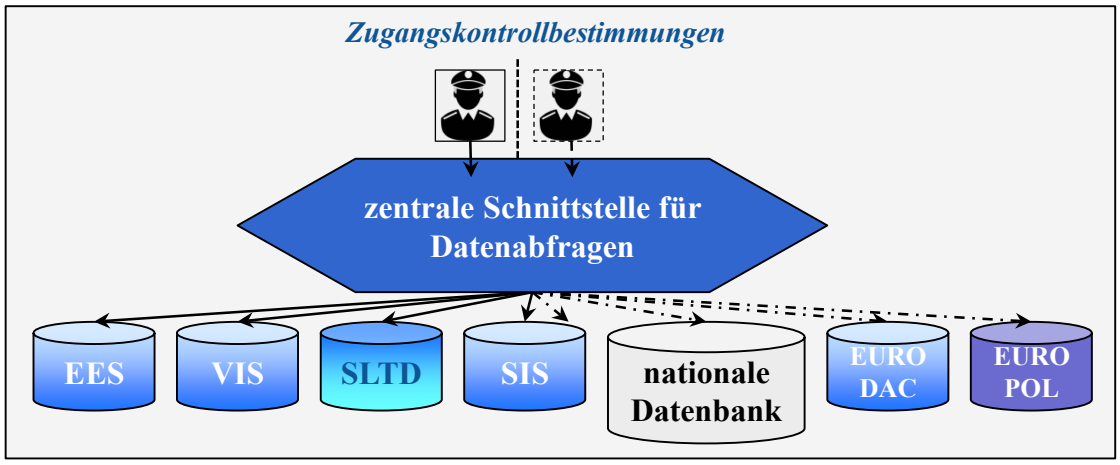
1. Zentrale Schnittstelle für Datenabfragen

Der erste Aspekt der Interoperabilität ist die **Möglichkeit, gleichzeitig mehrere Informationssysteme abzufragen und sämtliche Ergebnisse** Grenzschutz- oder Polizeibeamten unter vollständiger Wahrung ihrer Zugriffsrechte und für die jeweiligen Zwecke **auf einem einzigen Bildschirm anzeigen zu lassen**. Dafür bedarf es Plattformen mit einer gemeinsamen zentralen Schnittstelle, über die mit einer einzigen Abfrage mehrere Informationssysteme gleichzeitig abgefragt werden können. Eine solche Plattform könnte beispielsweise durch Auslesen des Chips eines Reisedokuments oder mittels biometrischer Daten mehrere verschiedene Datenbanken gleichzeitig abfragen. Die Datenabfrage über ein solche zentrale Schnittstelle sollte allen Behörden möglich sein, die in Übereinstimmung mit der bestehenden Zweckbindung und den geltenden strengen Vorschriften über die Kontrolle des Datenzugangs auf derartige Daten zugreifen und sie verwenden müssen (Grenzschutz-, Strafverfolgungs- und Asylbehörden). Sie sollte auch mit mobilen Geräten möglich sein. Durch die Schaffung einer solchen zentralen Schnittstelle würden die auf europäischer Ebene bestehenden Informationssysteme weniger komplex, denn so würde es Grenzschutz- und Polizeibeamten ermöglicht, mehrere Informationssysteme nach Maßgabe ihrer Zugangsrechte in einem Zuge und gleichzeitig abzufragen.

Mehrere Mitgliedstaaten haben bereits derartige Plattformen mit einer zentralen Schnittstelle geschaffen. Die Kommission und eu-LISA werden auf der Grundlage der dabei entstandenen bewährten Praktiken eine standardisierte Lösung für einen zentrale Schnittstelle für Datenabfragen entwickeln. Die Mitgliedstaaten sollten mit Hilfe von EU-Mitteln aus dem Fonds für die innere Sicherheit im Rahmen ihrer einschlägigen nationalen Programme die Schaffung einer solchen Funktion finanzieren. Die

Kommission wird aufmerksam verfolgen, wie die Mitgliedstaaten die Möglichkeiten einer zentralen Schnittstelle auf nationaler Ebene nutzen.

Abbildung 2: *zentrale Schnittstelle für Datenabfragen*



Datenabfragen in mehreren zentralen oder nationalen Systemen (wie auf der obigen Abbildung) sind leichter zu bewerkstelligen als Datenabfragen in dezentralen Systemen. Die Kommission und eu-LISA werden prüfen, ob über eine zentrale Schnittstelle auch gleichzeitige Datenabfragen in dezentralen Informationssystemen wie dem Prüm-Rahmen und ECRIS möglich sind. Die Kommission und eu-LISA werden diese Analyse gemeinsam mit der Sachverständigengruppe „Informationssysteme und Interoperabilität" und ohne Änderung bestehender Zugangsrechte durchführen.

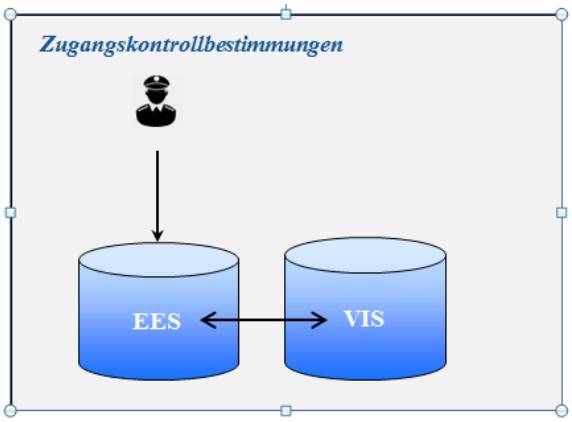
2. Vernetzung von Informationssystemen

Der zweite Aspekt der Interoperabilität ist die Vernetzung von Informationssystemen. Dabei geht es darum, dass verschiedene Systeme oder Datenbanken technisch miteinander kommunizieren können. **Daten, die in einem System erfasst sind, sollen von einem anderen System automatisch und zentral abgefragt werden können.** Dafür müssen die betreffenden Systeme technisch miteinander kompatibel und die in ihnen gespeicherten Daten (z. B. Fingerabdrücke) interoperabel sein. Durch eine solche Vernetzung lässt sich die Menge der Daten, die in Kommunikationsnetzen zirkulieren und über nationale Systeme übermittelt werden, verringern.

Dafür bedarf es allerdings angemessener Datenschutzgarantien und strenger Vorschriften über die Kontrolle des Datenzugangs. Dank der politischen Einigung, die die beiden gesetzgebenden Organe im Dezember 2015 in Sachen Datenschutzreform erzielt haben, wird ein moderner EU-weiter Datenschutzrahmen geschaffen werden, der ebensolche Garantien enthält. Es ist wichtig, dass die beiden gesetzgebenden Organe die Datenschutz-Grundverordnung und die Datenschutz-Richtlinie unverzüglich erlassen.

Der Vernetzungsaspekt ist Bestandteil des vorgeschlagenen Einreise-/Ausreisesystems (EES). Das EES und das VIS sollen direkt auf zentraler Ebene miteinander kommunizieren können. Dies ist eine wichtige Maßnahme zur Verringerung der bestehenden Fragmentierung der Datenverwaltungsarchitektur der EU für die Grenzkontrolle und die innere Sicherheit und zur Beseitigung damit verbundener Probleme. Durch den automatischen Abgleich entfällt für die Mitgliedstaaten die Notwendigkeit, bei Grenzkontrollen das VIS abzufragen. Zudem verringert sich der Wartungsaufwand, und die Systemleistung wird verbessert.

Abbildung 3: *Systemvernetzung - Beispiel: Einreise-/Ausreisesystem (EES) und Visa-Informationssystem (VIS)*



Als nächsten Schritt werden die Kommission und eu-LISA prüfen, ob die zentrale Vernetzung des künftigen Einreise-/Ausreisesystems (EES) und des Visa-Informationssystems (VIS) auf das SIS ausgeweitet und auch EURODAC mit dem SIS vernetzt werden könnte. Die Kommission und eu-LISA werden diese Analyse gemeinsam mit der Sachverständigengruppe „Informationssysteme und Interoperabilität" durchführen.

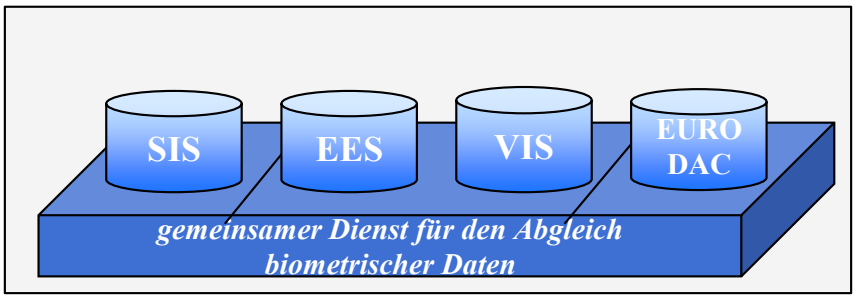
3. Gemeinsamer Dienst für den Abgleich biometrischer Daten

Der dritte Aspekt der Interoperabilität ist der Abgleich biometrischer Identifikatoren. So ist es beispielsweise wichtig, dass Fingerabdruckdaten, die in einem Konsulat eines Mitgliedstaats mit einer spezifischen Ausrüstung erhoben werden, über das VIS mit Fingerabdruckdaten abgeglichen werden können, die an einer Grenzübergangsstelle eines anderen Mitgliedstaats mit einer anderen spezifischen Ausrüstung erhoben werden. Dasselbe gilt für Fingerabdruckabfragen in anderen Systemen: Die biometrischen Proben müssen bestimmte Mindestanforderungen in Bezug auf ihre Qualität und ihr Format erfüllen, damit eine derartige Interoperabilität problemlos möglich wird.

Auf Systemebene ermöglicht die Interoperabilität biometrischer Identifikatoren die Nutzung eines gemeinsamen Dienstes für den Abgleich biometrischer Daten für mehrere Informationssysteme unter Einhaltung der Vorschriften über den Schutz personenbezogener Daten (räumliche Trennung der Daten und separate Zugangskontrollbestimmungen für die einzelnen Datenkategorien).[27] In finanzieller, wartungstechnischer und operativer Hinsicht sind solche gemeinsamen Dienste sehr vorteilhaft.

[27] Vergleichbar mit einem physischen Dateiserver, auf den eine Vielzahl von Nutzern zugreift, welche jeweils nur spezifische Zugangsrechte zu bestimmten Ordnern haben.

Abbildung 4: *gemeinsamer Dienst für den Abgleich biometrischer Daten*



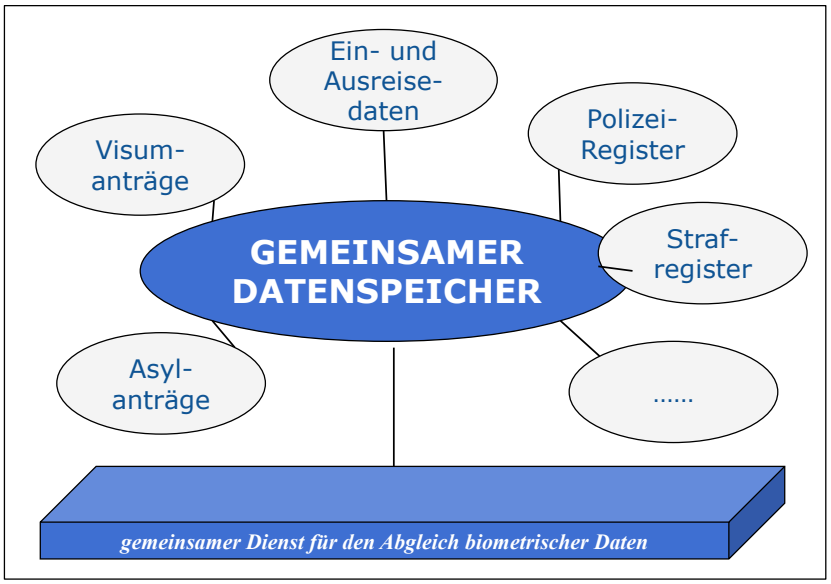
Die Kommission und eu-LISA werden prüfen, ob ein gemeinsamer Dienst für den Abgleich biometrischer Daten für alle einschlägigen Informationssysteme erforderlich und technisch machbar ist. Die Kommission und eu-LISA werden diese Analyse gemeinsam mit der Sachverständigengruppe „Informationssysteme und Interoperabilität" durchführen.

4. Gemeinsamer Datenspeicher

Das ehrgeizigste langfristige Konzept für die Gewährleistung der Interoperabilität wäre ein **gemeinsamer Datenspeicher auf EU-Ebene für verschiedene Informationssysteme**. Dieser könnte aus einem Kernmodul bestehen, das die grundlegenden Daten (alphanumerische und biometrische Daten) enthalten würde, während die anderen Datenelemente und besondere Merkmale der verschiedenen Informationssysteme (z. B. Visumdatum) in spezifischen Modulen gespeichert würden. Die Kernmodule und die spezifischen Module würden miteinander verbunden, um die jeweiligen Datensätze miteinander zu verknüpfen. Dadurch würde ein **modular aufgebautes, integriertes Identitätsmanagement für die Grenzen und die innere Sicherheit** geschaffen. Dabei müsste die Einhaltung der Datenschutzvorschriften gewährleistet werden (beispielsweise durch räumliche Trennung der Daten und separate Zugangskontrollbestimmungen für die einzelnen Datenkategorien).

Durch einen gemeinsamen Datenspeicher würde der gegenwärtigen Fragmentierung der Datenverwaltungsarchitektur der EU für die Grenzkontrolle und die innere Sicherheit ein Ende bereitet. Diese Fragmentierung läuft dem Grundsatz der Datenminimierung zuwider, da sie dazu führt, dass ein und dieselben Daten mehrfach gespeichert werden. Der gemeinsame Datenspeicher würde es im Bedarfsfall ermöglichen, bestehende Verbindungen zu ermitteln und durch die Kombination von in unterschiedlichen Informationssystemen gespeicherten Datenelementen ein Gesamtbild entstehen zu lassen. Die derzeitigen Informationslücken, die insbesondere Grenzschutz- und Polizeibeamten nur ein lückenhaftes Gesamtbild ermöglichen, würden auf diese Weise beseitigt.

Abbildung 5: *gemeinsamer Datenspeicher*



Die Option eines gemeinsamen Datenspeichers auf EU-Ebene wirft wichtige Fragen in Bezug auf die Definition des Zwecks, der Notwendigkeit, der technischen Machbarkeit und der Verhältnismäßigkeit der Datenverarbeitung auf. Der Rechtsrahmen für die Einrichtung der verschiedenen Informationssysteme müsste dafür vollständig überarbeitet werden, was nur ein langfristig zu verwirklichendes Ziel sein könnte. Die Sachverständigengruppe „Informationssysteme und Interoperabilität" wird sich mit den rechtlichen, technischen und operativen Fragen eines gemeinsamen Datenspeichers einschließlich der damit verbundenen Datenschutzaspekte befassen.

Bei allen vier oben genannten Aspekten der Interoperabilität (zentrale Schnittstelle für Datenabfragen, Systemvernetzung, gemeinsamer Dienst für den Abgleich biometrischer Daten und gemeinsamer Datenspeicher) ist es erforderlich, dass die in den verschiedenen Informationssystemen oder Modulen gespeicherten Daten miteinander kompatibel sind. Um dies zu erreichen, müssen die Arbeiten an einem **einheitlichen Nachrichtenformat** (UMF)[28] vorangetrieben werden, damit ein gemeinsamer Standard für alle einschlägigen Informationssysteme geschaffen wird.

[28] Die Kommission hat sich bereits in ihrer Mitteilung zum Europäischen Modell für den Informationsaustausch (EIXM) aus dem Jahr 2012 für die Weiterführung der Arbeiten zur Entwicklung eines einheitlichen Nachrichtenformats ausgesprochen und finanziert gegenwärtig das inzwischen dritte UMF-Pilotprojekt mit dem Ziel, einen gemeinsamen, für alle einschlägigen Datenbanken geltenden Standard für die nationale Ebene (d.h. für die Mitgliedstaaten), für die EU-Ebene (d.h. für die zentralen Systeme und die EU-Agenturen) und für die internationale Ebene (Interpol) zu schaffen.

Verbesserung der Interoperabilität von Informationssystemen

- Einsetzung einer **Sachverständigengruppe „Informationssysteme und Interoperabilität"** aus Vertretern der EU-Agenturen, nationalen Sachverständigen und Vertretern der betroffenen institutionellen Interessenträger, die die rechtlichen, technischen und operativen Aspekte der Verbesserung der Interoperabilität der Informationssysteme analysiert und insbesondere die Notwendigkeit, die technische Machbarkeit und die Verhältnismäßigkeit der verfügbaren Optionen sowie ihre Auswirkungen auf den Datenschutz prüft

Zentrale Schnittstelle für Datenabfragen

- gemeinsame Maßnahmen von Kommission und eu-LISA zur Unterstützung der Mitgliedstaaten bei der Einrichtung einer zentralen Schnittstelle für Datenabfragen in den Zentralsystemen
- gemeinsame Prüfung durch die Kommission, eu-LISA und die Sachverständigengruppe, ob über eine zentrale Schnittstelle gleichzeitige Datenabfragen in allen einschlägigen Informationssystemen möglich sind, ohne dass bestehende Zugangsrechte geändert werden müssen

Vernetzung von Informationssystemen

- gemeinsame Prüfung durch die Kommission, eu-LISA und die Sachverständigengruppe, ob die Vernetzung der zentralen Informationssysteme über die bereits vorgeschlagene Vernetzung des Einreise-/Ausreisesystems und des Visa-Informationssystem hinausgehen könnte

Gemeinsamer Dienst für den Abgleich biometrischer Daten

- gemeinsame Prüfung durch die Kommission, eu-LISA und die Sachverständigengruppe, ob ein gemeinsamer Dienst für den Abgleich biometrischer Daten für alle einschlägigen Informationssysteme erforderlich und technisch machbar ist

Gemeinsamer Datenspeicher (Kernmodul)

- gemeinsame Prüfung durch die Kommission, eu-LISA und die Sachverständigengruppe, welche rechtlichen, technischen, operativen und finanziellen Auswirkungen die langfristige Entwicklung eines gemeinsamen Datenspeichers hätte
- Mitwirkung von Kommission und eu-LISA bei den laufenden Arbeiten zur Entwicklung eines weltweit einheitlichen Nachrichtenformats für alle einschlägigen Informationssysteme

8. ZUSAMMENFASSUNG

Mit dieser Mitteilung soll eine Diskussion darüber angestoßen werden, wie Informationssysteme in der EU ausgehend von den beträchtlichen Synergien zwischen der Europäischen Sicherheitsagenda und der Europäischen Migrationsagenda das Grenzmanagement verbessern und die innere Sicherheit erhöhen können. Eine Reihe von Informationssystemen liefert den Grenzschutz- und Polizeibeamten bereits sachdienliche Informationen, doch diese Systeme sind nicht perfekt. Die EU steht vor der Herausforderung, eine solidere und intelligentere Datenverwaltungsarchitektur aufbauen zu müssen, bei der die Grundrechte und insbesondere das Recht auf den Schutz

personenbezogener Daten und der diesbezüglich geltende Grundsatz der Zweckbindung in vollem Umfang gewahrt bleiben.

Zudem müssen die vorhandenen Lücken in der Datenverwaltungsarchitektur der EU beseitigt werden. Die Kommission hat zusammen mit dieser Mitteilung einen Vorschlag für einen Rechtsakt zur Schaffung eines Einreise-/Ausreisesystems vorgelegt, der so bald wie möglich erlassen werden sollte. Auch die vorgeschlagene Richtlinie über Fluggastdatensätze sollte in den kommenden Wochen erlassen werden. Der vorgeschlagene Rechtsakt zur Schaffung einer europäischen Grenz- und Küstenwache sollte noch vor dem Sommer erlassen werden. Parallel dazu wird die Kommission weiter an der Stärkung und gegebenenfalls Verschlankung der bestehenden Systeme arbeiten und zu diesem Zweck beispielsweise ein automatisches Fingerabdruckidentifizierungssystem für das Schengener Informationssystem entwickeln.

Die Mitgliedstaaten müssen ihrer rechtlichen Pflicht nachkommen, die vorhandenen Informationssysteme in vollem Umfang zu nutzen und die erforderlichen technischen Verbindungen zu sämtlichen Informationssystemen und Datenbanken herzustellen. Bestehende Mängel - insbesondere des Prüm-Rahmens - müssen umgehend beseitigt werden. Mit dieser Mitteilung soll eine Diskussion darüber angestoßen werden, wie Systemmängel und Informationslücken beseitigt werden können, und ein entsprechender Prozess eingeleitet werden. Die Mitgliedstaaten müssen die anhaltenden Mängel bei der Dateneingabe in EU-Datenbanken und beim EU-weiten Informationsaustausch dringend abstellen.

Um die Struktur der Datenverwaltungsarchitektur der EU für die Grenzkontrolle und die innere Sicherheit zu verbessern, soll mit dieser Mitteilung ein Prozess zur Verbesserung der Interoperabilität der Informationssysteme eingeleitet werden. Die Kommission wird eine Sachverständigengruppe „Informationssysteme und Interoperabilität" einsetzen, die sich mit den rechtlichen, technischen und operativen Aspekten der verschiedenen Optionen für die Herstellung der Interoperabilität von Informationssystemen und mit etwaigen Mängeln und Lücken befassen soll. Auf der Grundlage der von der Sachverständigengruppe getroffenen Feststellungen wird die Kommission sodann dem Europäischen Parlament und dem Rat weitere konkrete Vorschläge unterbreiten, die als Grundlage für eine gemeinsame Diskussion über das weitere Vorgehen dienen können. Die Kommission wird sich ferner bemühen, die Standpunkte des Europäischen Datenschutzbeauftragten und der nationalen Datenschutzbehörden, deren Vertreter in der Artikel-29-Datenschutzgruppe zusammenkommen, einzuholen.

Ziel sollte die Entwicklung einer gemeinsamen Strategie sein, die darauf abstellt, die Datenverwaltung in der EU unter uneingeschränkter Einhaltung der Datenschutzvorschriften effizienter zu machen, die Außengrenzen der EU besser zu schützen und die innere Sicherheit in der EU zum Wohle aller EU-Bürgern zu erhöhen.

ANHANG 1: ABKÜRZUNGEN

API	erweiterte Fluggastdaten (Advance Passenger Information)
AFIS	automatisches Fingerabdruckidentifizierungssystem (Automated Fingerprint Identification System), das die Erfassung, die Speicherung, den Vergleich und die Überprüfung von Fingerabdrücken ermöglicht
CIS bzw. ZIS	Zollinformationssystem (Customs Information System)
ECRIS	Europäisches Strafregisterinformationssystem (European Criminal Records Information System)
EES	(vorgeschlagenes) Einreise-/Ausreisesystem (Entry-Exit System)
EIXM	Europäisches Informationsaustauschmodell (European Information Exchange Model)
EIS	Europol-Informationssystem (Europol Information System)
EPRIS	Europäisches Polizeiregisterinformationssystem (European Police Records Information System)
EURODAC	europäisches Dactyloskopiesystem (European Dactyloscopy System)
EUROPOL	Europäisches Polizeiamt (European Police Office)
ETIAS	(mögliches) EU-weites Reiseinformations- und -genehmigungssystem (EU Travel Information and Authorisation System)
eu-LISA	Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts
FIND	fest installierte und vernetzte Interpol-Datenbank (Fixed Interpol Networked Database)
FRONTEX	Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedstaaten der Europäischen Union (European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union)
iARMS	(Interpol-)Datenbank für gesuchte Straftäter, Fahrzeuge oder Feuerwaffen (Illicit Arms Records and tracing Management System)
Interpol	Internationale kriminalpolizeiliche Organisation (International Criminal Police Organization)
MIND	mobile vernetzte Interpol-Datenbank (Mobile Interpol Networked Database)
PIU	in jedem Mitgliedstaat einzurichtende PNR-Zentralstelle (Passenger's Information Unit), der die Fluggesellschaften die Fluggastdaten zu übermitteln haben
PNR	Fluggastdaten(sätze) (Passenger Name Records)
Prüm-Rahmen	Verfahren der polizeilichen Zusammenarbeit zum Austausch von DNA-, Fingerabdruck- und Fahrzeugregisterdaten
SafeSeaNet	europäische Plattform für den Austausch von Meeresdaten zwischen Schifffahrtsbehörden der Mitgliedstaaten
SBC	Schengener Grenzkodex (Schengen Border Code)

SIENA	Europols Netzanwendung für den sicheren Datenaustausch (Secure Information Exchange Network Application)
SIS	Schengener Informationssystem, gelegentlich auch als „Schengener Informationssystem der zweiten Generation“ (SIS II) bezeichnet
SLTD	Interpol-Datenbank für gestohlene und verlorene Reisedokumente (Stolen and Lost Travel Documents database)
sTESTA	gesicherte transeuropäische Telematikdienste für Behörden (secured Trans European Services for Telematics between Administrations), Modernisierung durch TESTA-NG (next generation) geplant
UMF	einheitliches Nachrichtenformat (Uniform Message Format), durch das Informationssysteme miteinander kompatibel gemacht werden sollen
VIS	Visa-Informationssystem (Visa Information System)
VRD	Fahrzeugregisterdaten (Vehicle Registration Data)

ANHANG 2: VERZEICHNIS DER BESTEHENDEN INFORMATIONSSYSTEME FÜR DAS GRENZMANAGEMENT UND DIE STRAFVERFOLGUNG

1. Schengener Informationssystem (SIS)

Das SIS ist die größte und meistgenutzte Plattform für den Informationsaustausch über die Einwanderung und die Strafverfolgung. Das SIS ist ein zentrales System, das von 25 Mitgliedstaaten[29] der EU und von vier assoziierten Schengen-Staaten[30] genutzt wird und derzeit 63 Millionen Ausschreibungen umfasst. Die Ausschreibungen werden von zuständigen Behörden wie Polizei-, Grenzkontroll- und Einwanderungsbehörden eingegeben und konsultiert. Das SIS enthält Datensätze über Drittstaatangehörige, denen die in Einreise in den Schengen-Raum und der Aufenthalt im Schengen-Raum untersagt ist, oder die gesucht oder vermisst werden (auch Kinder), sowie über gesuchte Gegenstände (Feuerwaffen, Kraftfahrzeuge, Ausweispapiere, industrielle Ausrüstung usw.). Im Unterschied zu anderen Instrumenten für den Informationsaustausch werden die im SIS gespeicherten Informationen durch eine Anweisung für konkrete Maßnahmen der vor Ort tätigen Beamten (beispielsweise Festnahmen oder Beschlagnahmen) ergänzt.

Die Überprüfung anhand des SIS ist obligatorisch bei der Bearbeitung von Visa für einen kurzfristigen Aufenthalt, bei Grenzkontrollen von Drittstaatangehörigen und bei nicht systematischen Kontrollen[31] von EU-Bürgern, die von ihrem Recht auf Freizügigkeit Gebrauch machen. Zudem soll jede Polizeikontrolle im Hoheitsgebiet eine automatische Überprüfung anhand des SIS einschließen.

2. Visa-Informationssystem (VIS)

Das VIS ist ein zentrales System für den Austausch von Daten über Visa für einen kurzfristigen Aufenthalt zwischen Mitgliedstaaten. Im VIS werden Daten und Entscheidungen im Zusammenhang mit Anträgen auf Ausstellung eines Visums für den kurzfristigen Aufenthalt im Schengen-Raum oder für die Durchreise durch den Schengen-Raum verarbeitet. Alle (rund 2000) konsularischen Vertretungen der Schengen-Staaten sowie alle (rund 1800) Grenzübergangsstellen an den Außengrenzen der Schengen-Staaten sind an das VIS angeschlossen.

Das VIS enthält Daten über Visumanträge und -entscheidungen sowie Angaben, ob erteilt Visa widerrufen, für nichtig erklärt oder verlängert wurden. Derzeit enthält das VIS Daten über 20 Mio. Visumanträge; in Spitzenzeiten werden über 50 000 Vorgänge über das VIS abgewickelt. Zu jedem Visumantragsteller werden ausführliche Angaben zur Person, eine digitale Fotografie und zehn Fingerabdrücke erfasst. Das VIS ist somit ein zuverlässiges Instrument für die Überprüfung der Identität von Visumantragstellern, für die Aufdeckung von Fällen von irregulärer Migration und von Sicherheitsrisiken sowie für die Vermeidung von „Visum-Shopping“.

Die Mitgliedstaaten nutzen das VIS an ihren Grenzübergangsstellen und auch im Landesinnern für die Überprüfung der Identität von Visuminhabern anhand des Abgleichs ihrer Fingerabdrücke mit den im VIS gespeicherten Fingerabdrücken. Dadurch wird sichergestellt, dass es sich bei dem Visumantragsteller um dieselbe Person wie die

[29] Alle Mitgliedstaaten außer Irland, Zypern und Kroatien.
[30] Schweiz, Liechtenstein, Norwegen und Island.
[31] Diese Bestimmung soll gemäß dem Vorschlag der Kommission zur Änderung des Schengener Grenzkodex (COM/2015/670) geändert werden.

Person, die die Grenze überquert, handelt. Anhand des Fingerabdruckabgleichs im VIS ist es zudem möglich, Personen zu identifizieren, die in den letzten fünf Jahren einen Visumantrag gestellt haben, aber keine Ausweispapiere mit sich führen.

3. EURODAC

Das europäische Dactyloskopiesystem EURODAC enthält Fingerabdrücke von Asylbewerbern und Drittstaatangehörigen, die illegal die Außengrenzen des Schengen-Raums überschreiten. Sein Hauptzweck besteht derzeit darin, nach Maßgabe der Dublin-Verordnung zu bestimmen, welcher Mitgliedstaat für die Bearbeitung eines Asylantrags zuständig ist. Wenngleich von den Grenzübergangsstellen auf EURODAC zugegriffen werden kann, ist dieses doch im Gegensatz zum SIS und VIS kein Grenzmanagementsystem.

An den Grenzübergangsstellen werden Fingerabdrücke von irregulär in die EU einreisenden Migranten genommen. Die Fingerabdrücke werden in EURODAC gespeichert, um sie zur Überprüfung der Identität der betreffenden Personen verwenden zu können, falls diese in der Folge Asyl beantragen. Die Einwanderungs- und die Polizeibehörden können zudem anhand der Fingerabdruckdaten von in einem Mitgliedstaat der EU aufgegriffenen irregulären Migranten überprüfen, über diese bereits in einem anderen Mitgliedstaat Asyl beantragt haben. Ferner können die Strafverfolgungsbehörden und Europol zu den Zwecken der Verhütung, Aufdeckung oder Untersuchung einer schweren bzw. terroristischen Straftat EURODAC-Daten abfragen.

Die Erfassung von Fingerabdrücken von Asylbewerbern und irregulären Migranten in einem zentralen System ermöglicht die Identifizierung und Überwachung der Sekundärmigration[32] in der EU bis zu dem Zeitpunkt, an dem ein Antrag auf internationalen Schutz gestellt wird oder eine Rückführungsentscheidung ergeht (was künftig mit einem entsprechenden Warnhinweis im SIS einhergehen soll). Die Identifizierung und Überwachung irregulärer Migranten ist zudem notwendig, damit die zuständigen Behörden in den Herkunftsländern neue Ausweispapiere ausstellen können und die Rückkehr somit erleichtert wird.

4. Datenbank für gestohlene und verlorene Reisedokumente (SLTD)

Die Interpol-Datenbank für gestohlene und verlorene Reisedokumente (SLTD) ist eine zentrale Datenbank für Pässe und Reisedokumente, die von den ausstellenden Behörden an Interpol als gestohlen oder verloren gemeldet wurden. Sie enthält auch Informationen über gestohlene Blankoausweisdokumente. Alle Daten von Reisedokumenten, die den Behörden der am SIS teilnehmenden Länder als verloren oder gestohlen gemeldet werden, werden sowohl in der SLTD als auch im SIS erfasst. Die SLTD enthält auch Reisedokumentendaten, die von nicht am SIS teilnehmenden Ländern (Irland, Kroatien, Zypern und Drittstaaten) eingegeben wurden.

Wie in den Schlussfolgerungen des Rates vom 9. und 20. November 2015 und im Vorschlag der Kommission vom 15. Dezember 2015 für eine Verordnung zur Änderung des Schengener Grenzkodexes[33] vorgesehen, sollen die Reisedokumentendaten aller Drittstaatangehörigen und Personen, die Freizügigkeit genießen, mit der SLTD

[32] Wie beispielsweise im Fall von Flüchtlingen, die in Griechenland ankommen, aber dort kein Asyl beantragen, sondern auf dem Landweg in andere Mitgliedstaaten weiterreisen.

[33] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 562/2006 hinsichtlich eines verstärkten Abgleichs mit einschlägigen Datenbanken an den Außengrenzen (COM(2015) 670 final).

abgeglichen werden. Alle Grenzkontrollstellen sollen an die SLTD angeschlossen werden. Zudem würden Abfragen der inländischen Strafverfolgungsstellen in der SLTD zusätzliche Sicherheit bieten.

5. Advance Passenger Information System (APIS)

Dieses System dient zur Erhebung von erweiterten Fluggastdaten (API-Daten). Dabei handelt es sich um Informationen über die Identität von Fluggästen, die bei Flügen in die EU vor dem Boarding erhoben werden und zur Identifizierung irregulärer Migranten bei der Ankunft in der EU dienen. Die Daten bestehen aus Informationen aus einem Reisedokument (vollständiger Name, Geburtsdatum und Staatsangehörigkeit des Reisenden sowie Nummer und Art des Reisedokuments) und der Angabe der Grenzübergangsstellen der Ausreise und der Einreise sowie Einzelheiten über die Beförderung. Die sich auf den Fluggast beziehenden API-Daten werden in der Regel zum Zeitpunkt der Abfertigung erhoben.

Vorabinformationen über die Beförderung auf dem Seeweg müssen gemäß dem Übereinkommen zur Erleichterung des internationalen Seeverkehrs 24 Stunden vor der planmäßigen Ankunft des Schiffs übermittelt werden. Die Richtlinie 2010/65/EU[34] sieht eine elektronische Übermittlung von Daten über eine zentrale Schnittstelle („single window“) vor, die SafeSeaNet, die elektronische Zollabfertigung (e-Customs) und andere elektronische Systeme miteinander verbindet.

Es gibt kein zentrales EU-System für die Erfassung von API-Daten.

6. Europol-Informationssystem

Das Europol-Informationssystem (EIS) ist eine zu Untersuchungszwecken dienende zentrale Datenbank mit kriminalpolizeilichen Informationen. In ihr können die Mitgliedstaaten und Europol Daten über schwere bzw. terroristische Straftaten abfragen und speichern. Bei den im EIS gespeicherten Daten handelt es sich um Informationen über Personen, Ausweisdokumente, Kraftfahrzeuge, Feuerwaffen, Telefonnummern, Emails, Fingerabdrücke, DNA und Straftaten auf dem Gebiet der Computerkriminalität, die auf unterschiedliche Weise miteinander verknüpft werden können, um einen genaueren, strukturierten Überblick über einen Fall zu ermöglichen. Das EIS dient zur Unterstützung der Zusammenarbeit bei der Strafverfolgung und ist für Grenzkontrollbehörden nicht zugänglich.

Der Informationsaustausch erfolgt über die Plattform SIENA[35]. Dabei handelt es sich um ein sicheres elektronisches Kommunikationsnetz zwischen Europol, den Verbindungsbüros, den nationalen Europol-Stellen, den benannten zuständigen Behörden (Zollbehörden, Vermögensabschöpfungsstellen usw.) und an das Netz angeschlossenen Dritten.

Im Mai 2017 wird ein neuer Rechtsrahmen für Europol in Kraft treten. Dieser Rahmen wird die operativen Möglichkeiten Europols zur Durchführung von Analysen und zur Verknüpfung verfügbarer Informationen verbessern.

---

[34] Richtlinie 2010/65/EU des Europäischen Parlaments und des Rates vom 20. Oktober 2010 über Meldeformalitäten für Schiffe beim Einlaufen in und/oder Auslaufen aus Häfen der Mitgliedstaaten und zur Aufhebung der Richtlinie 2002/6/EG.

[35] Netzanwendung für den sicheren Datenaustausch (Secure Information Exchange Network Application).

7. Prüm-Rahmen

Der Prüm-Rahmen stützt sich auf ein multilaterales Übereinkommen[36] zwischen den Mitgliedstaaten, das den Austausch von DNA-, Fingerabdruck- und Fahrzeugregisterdaten regelt. Der Grundgedanke dabei ist, dass jedes nationale System mit den nationalen Systemen der anderen Mitgliedstaaten vernetzt wird, um eine netzwerkweite Informationssuche zu ermöglichen. Wenn dabei ein Treffer in der Datenbank eines anderen Mitgliedstaats gefunden wird, werden die betreffenden Einzelheiten über bilaterale Mechanismen ausgetauscht.

8. Europäisches Strafregisterinformationssystem (ECRIS)

ECRIS ist ein elektronisches System für den Austausch von Informationen über frühere Verurteilungen einer bestimmten Person durch Strafgerichte in der EU für die Zwecke eines Strafverfahrens gegen diese Person und, sofern dies nach nationalem Recht zulässig ist, für andere Zwecke. Urteilsmitgliedstaaten müssen dem Herkunftsmitgliedstaat Informationen und aktualisierte Daten im Zusammenhang mit Verurteilungen übermitteln, die gegen einen Staatsangehörigen eines anderen Mitgliedstaats ergangen sind. Der Herkunftsmitgliedstaat muss diese Informationen speichern, damit er unabhängig davon, wo in der EU Verurteilungen ergangen sind, auf Ersuchen aktuelle Auskünfte über etwaige Vorstrafen seiner Staatsangehörigen erteilen kann.

ECRIS ermöglicht zudem den Austausch von Informationen über Verurteilungen von Drittstaatangehörigen und Staatenlosen. Die benannten Zentralbehörden in den einzelnen Mitgliedstaaten sind die Kontaktstellen im ECRIS-Netz und befassen sich mit allen Aufgaben wie der Mitteilung, Speicherung, Anforderung und Bereitstellung von Informationen aus dem Strafregister.

[36] Prümer Vertrag vom 2005, im Jahr 2008 durch den Beschluss 2008/615/JI des Rates in EU-Recht überführt.