144274/EU XXV. GP
Eingelangt am 23/05/17

Rat der
Europäischen Union

Brüssel, den 17. Mai 2017
(OR. en)

9348/17

COSI 103
CT 45
FRONT 231
DAPIX 193
ENFOPOL 243
ENFOCUSTOM 129
GENVAL 57
AVIATION 69
COPEN 158
SIRIS 89
ASIM 51
VISA 186
CYBER 78
JAI 507

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Eingangsdatum:	16. Mai 2017
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2017) 261 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN EUROPÄISCHEN RAT UND DEN RAT Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Siebter Fortschrittsbericht

Die Delegationen erhalten in der Anlage das Dokument COM(2017) 261 final.

Anl.: COM(2017) 261 final

www.parlament.gv.at

EUROPÄISCHE
KOMMISSION

Brüssel, den 16.5.2017
COM(2017) 261 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN EUROPÄISCHEN RAT UND DEN RAT

Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Siebter Fortschrittsbericht

www.parlament.gv.at

I. EINLEITUNG

Dies ist der siebte Monatsbericht über die Fortschritte auf dem Weg zu einer wirksamen und echten Sicherheitsunion. Er beleuchtet die Entwicklungen in zwei der wichtigsten Bereiche: „Bekämpfung des Terrorismus und der organisierten Kriminalität sowie der Instrumente zu ihrer Unterstützung“ und „Stärkung unserer Abwehrbereitschaft und Widerstandsfähigkeit gegen diese Bedrohungen“. In diesem Bericht geht es schwerpunktmäßig um die Arbeiten an der Interoperabilität der Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung mit dem Ziel, unter uneingeschränkter Einhaltung der Datenschutzvorschriften für eine wirksamere und effizientere Datenverwaltung in der EU zu sorgen, damit ein besserer Schutz der Außengrenzen gewährleistet und die innere Sicherheit im Interesse aller Bürger erhöht wird. Der Bericht liefert zudem einen Überblick über den aktuellen Stand der Fortschritte, die bei den wichtigsten legislativen und nichtlegislativen Dossiers erzielt wurden.

Die jüngste weltweite Cyberattacke, bei der mit Ransomware Tausende von Computersystemen lahmgelegt wurden, hat erneut deutlich gemacht, dass die Widerstandsfähigkeit der EU gegenüber Cyberangriffen und die Sicherheitsmaßnahmen angesichts der rasch zunehmenden organisierten Cyberkriminalität dringend verstärkt werden müssen, wie dies bereits im letzten Fortschrittsbericht zur Sicherheitsunion[1] angemerkt und in der von Europol erstellten Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität[2] herausgestellt wurde. Die Kommission beschleunigt ihre Arbeiten im Bereich der Cybersicherheit. Wie in ihrer Halbzeitbewertung zum digitalen Binnenmarkt[3] angekündigt, überprüft sie dazu insbesondere die Cybersicherheitsstrategie der EU aus dem Jahr 2013[4], um zeitnah und wirksam auf diese Bedrohungen reagieren zu können.

In Präsident Junckers Rede zur Lage der Union vom September 2016[5] und den Schlussfolgerungen des Europäischen Rates vom Dezember 2016[6] wurde betont, dass die derzeitigen Mängel bei der Datenverarbeitung beseitigt und die Interoperabilität der bestehenden Informationssysteme verbessert werden müssen. Die jüngsten Terrorangriffe haben diese Problematik noch stärker ins Blickfeld gerückt und verdeutlicht, dass dringend für die Interoperabilität der Informationssysteme gesorgt werden muss und die derzeitigen Informationslücken, aufgrund deren es möglich ist, dass Terrorverdächtige in verschiedenen, nicht miteinander verbundenen Datenbanken unter unterschiedlichen Aliasnamen erfasst werden, geschlossen werden müssen. In diesem Bericht wird das Konzept der Kommission erläutert, **mit dem bis zum Jahr 2020 die Interoperabilität der Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung erreicht werden soll,** damit sichergestellt wird, dass Grenzschutz- und Strafverfolgungsbeamte, darunter Zollbeamte sowie Mitarbeiter von Einwanderungs- und Justizbehörden, über die erforderlichen Informationen verfügen. Dabei handelt es sich um eine Folgemaßnahme zu der

---

1 COM(2016) 213 final vom 12.4.2017.

2 https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

3 COM(2017) 228 final vom 10.5.2017. Siehe auch den Vierten Fortschrittsbericht zur Sicherheitsunion (COM(2017) 41 final vom 25.1.2017).

4 JOIN(2013) 1 final vom 7.2.2013.

5 Lage der Union 2016 (14.9.2016), https://ec.europa.eu/commission/state-union-2016_de.

6 Schlussfolgerungen des Europäischen Rates vom 15.12.2016, http://www.consilium.europa.eu/de/meetings/european-council/2016/12/20161215-euco-conclusions-final_pdf/.

www.parlament.gv.at

im April 2016 von der Kommission vorgelegten Mitteilung „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“[7] und zu den Arbeiten der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität, die die Kommission im Nachgang zu der genannten Mitteilung eingesetzt hat.

II. SOLIDERE UND INTELLIGENTERE INFORMATIONSSYSTEME

1. Die Kommissionsmitteilung vom April 2016 und die bisherigen Maßnahmen

In der Mitteilung „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“ vom April 2016 wurden einige strukturelle Mängel der Informationssysteme ermittelt:

- suboptimale Funktionen in einigen der bestehenden Informationssysteme,
- Informationslücken in der Datenverwaltungsarchitektur der EU,
- die komplexe Landschaft unterschiedlich geregelter Informationssysteme und
- die Fragmentierung der Datenverwaltungsarchitektur für das Grenzmanagement und die Sicherheit, in der Daten jeweils getrennt in nicht miteinander verbundenen Systemen gespeichert werden, wodurch Informationslücken entstehen.

Um diese Mängel zu beseitigen, **schlug die Kommission Maßnahmen in drei Bereichen vor** und betonte, dass die Vorgaben der Charta der Grundrechte und insbesondere der umfassende Rahmen für den Schutz personenbezogener Daten in der EU der Kommission als Richtschnur bei ihrer Arbeit dienen werden.

Erstens zeigte die Kommission Möglichkeiten auf, **um die Vorteile der vorhandenen Informationssysteme optimal auszuschöpfen, und wies nachdrücklich darauf hin, dass die Mitgliedstaaten diese Systeme in vollem Umfang nutzen müssen**. Danach legte die Kommission im Dezember 2016 Legislativvorschläge zur Stärkung des Schengener Informationssystems (SIS)[8] vor, bei dem es sich um das erfolgreichste Instrument für die Zusammenarbeit von Grenzschutzbeamten, Zollbehörden, Polizeibeamten und Justizbehörden handelt. Damit die Rückkehr bzw. Rückführung von Migranten erleichtert und besser gegen irreguläre Migration vorgegangen werden kann, unterbreitete die Kommission außerdem im Mai 2016 einen Legislativvorschlag zur Stärkung der Datenbank Eurodac[9], die Informationen zu Asyl und irregulärer Migration enthält. Im Januar 2016 legte die Kommission einen Legislativvorschlag vor, um das Europäische Strafregisterinformationssystem (ECRIS)[10] zu erweitern und so den Austausch von Strafregistereinträgen von Drittstaatsangehörigen in der EU zu erleichtern. Wie angekündigt[11] wird die Kommission im Juni 2017 unter Berücksichtigung der Ergebnisse der Beratungen mit den beiden gesetzgebenden Organen über den Vorschlag vom Januar 2016 einen ergänzenden Vorschlag zur Einrichtung eines zentralen Systems[12] unterbreiten, damit

---

7 COM(2016) 205 final vom 6.4.2016.

8 COM(2016) 881 final vom 21.12.2016, COM(2016) 882 final vom 21.12.2016, COM(2016) 883 final vom 21.12.2016.

9 COM(2016) 272 final vom 4.5.2016.

10 COM(2016) 7 final vom 19.1.2016.

11 Siehe „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Fünfter Fortschrittsbericht“ (COM(2017) 203 final vom 2.3.2017).

12 Wenn die Mitgliedstaaten Informationen zur Verurteilung eines Drittstaatsangehörigen abfragen, wird das zentrale System sie an die Mitgliedstaaten weiterleiten, in denen die Strafregisterangaben zu finden sind.

www.parlament.gv.at

verurteilte Drittstaatsangehörige identifiziert werden können und in Erfahrung gebracht werden kann, welche Mitgliedstaaten Informationen über die betreffenden Personen besitzen.

Im Juni 2017 wird die Kommission zudem einen Legislativvorschlag zur Überarbeitung des rechtlichen Mandats von eu-LISA[13] vorlegen, in dessen Rahmen die Agentur auch mit dem Ausbau der Interoperabilität der zentralen EU-Informationssysteme für Sicherheit, Grenzmanagement und Migrationssteuerung beauftragt werden soll.

Zweitens wurden in der Mitteilung Möglichkeiten aufgezeigt, **um neue und ergänzende Maßnahmen auszuarbeiten, mit denen die Defizite in der Datenverwaltungsarchitektur der EU beseitigt werden können**. Insbesondere ermittelte die Kommission erhebliche Informationslücken in Bezug auf Drittstaatsangehörige, die den Schengen-Raum besuchen, insbesondere in Bezug auf von der Visumpflicht befreite Drittstaatsangehörige, die über Landgrenzen in die EU einreisen. Derzeit werden Außengrenzübertritte von Drittstaatsangehörigen nicht erfasst, und es liegen keine Informationen über von der Visumpflicht befreite Drittstaatsangehörige vor deren Ankunft an den Landaußengrenzen der EU vor. Als Follow-up unterbreitete die Kommission Legislativvorschläge zur Einführung von zwei neuen Informationssystemen, mit denen diese erheblichen Lücken geschlossen werden sollen. Im April 2016 schlug die Kommission ein Einreise-/Ausreisesystem der EU vor, das durch qualitativ bessere und effizientere Kontrollen zur Modernisierung des Außengrenzenmanagements beitragen soll.[14] Im November 2016 legte sie einen Vorschlag über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) vor, um Informationen über alle Personen, die ohne Visum in die Europäische Union reisen, zu erfassen, damit vorab Kontrollen zur Verhinderung irregulärer Migration und Sicherheitskontrollen erfolgen können.[15]

Der dritte Aspekt, der in der Mitteilung herausgestellt wurde, ist **die Notwendigkeit, die Interoperabilität der Informationssysteme zu verbessern**. Wie in der Mitteilung erläutert, wird auf der Grundlage der umfassenden Rahmenregelung für den Schutz personenbezogener Daten in der EU und dank wichtiger Entwicklungen auf technologischem Gebiet und bei der IT-Sicherheit die Interoperabilität der Informationssysteme in Verbindung mit den erforderlichen strikten Zugangs- und Verwendungsbestimmungen ohne Beeinträchtigung der bestehenden Zweckbindung erreicht werden können. Zur Herstellung der Interoperabilität werden in der Mitteilung **vier Optionen** aufgezeigt:

- eine **zentrale Schnittstelle für Datenabfragen**, die die gleichzeitige Abfrage mehrerer Informationssysteme und die Anzeige der Ergebnisse aller abgefragten Systeme auf einem einzigen Bildschirm ermöglicht,
- die **Vernetzung der Informationssysteme**, wobei 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 und
- ein **gemeinsamer Speicher für Identitätsdaten** mit alphanumerischen Daten für verschiedene Informationssysteme (einschließlich gebräuchlicher biografischer Attribute wie Name und Geburtsdatum).

---

[13] Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts.

[14] COM(2016) 194 final vom 6.4.2016.

[15] COM(2016) 731 final vom 16.11.2016.

Die Kommission hat eine Diskussion darüber angestoßen, wie durch die Informationssysteme in der Europäischen Union das Grenzmanagement verbessert und die innere Sicherheit erhöht werden kann. Um die entsprechenden Arbeiten voranzubringen, hat sie eine hochrangige Expertengruppe für Informationssysteme und Interoperabilität eingesetzt (siehe Abschnitt II.3).

2. Fortschritte bei den Prioritäten in Bezug auf die Informationssysteme

Um ihre Aufgaben erfüllen zu können, müssen Grenzschutz- und Strafverfolgungsbeamte sowie Mitarbeiter von Einwanderungs- und Justizbehörden Zugang zu genauen und vollständigen Daten haben. **Daher ist es unerlässlich, dass das Europäische Parlament und der Rat die vorrangigen Vorschläge zu den Informationssystemen**, die in Bezug auf den ersten Aspekt der Mitteilung vom April 2016 vorgelegt wurden, **voranbringen**. Wie oben dargelegt, wird dies entscheidend dazu beitragen, dass die vorhandenen Informationssysteme wirksamer für das Grenzmanagement und die Sicherheit eingesetzt werden können, und große Informationslücken schließen, indem neue Systeme, die für die Absicherung der Außengrenze erforderlich sind, eingeführt werden.

Am weitesten fortgeschritten ist der Vorschlag zum **Einreise-/Ausreisesystem der EU**. Er befindet sich in der Trilog-Phase und könnte durchaus – wie vom Europäischen Rat angestrebt – im Juni 2017 verabschiedet werden. Die technischen Beratungen über das **Europäische Reiseinformations- und -genehmigungssystem** (ETIAS) kommen weiter voran, aber die beiden gesetzgebenden Organe müssen noch ihre Verhandlungspositionen festlegen. Die Annahme des Mandats des Rates ist für Juni 2017 geplant, während der Ausschuss des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres (LIBE) sein Verhandlungsmandat im September 2017 annehmen will. In der Gemeinsamen Erklärung zu den gesetzgeberischen Prioritäten der EU für 2017[16] wurde diesem Dossier Vorrang eingeräumt, damit das Gesetzgebungsverfahren vor Ende 2017 abgeschlossen werden kann. Die Kommission wird die gesetzgebenden Organe weiterhin dabei unterstützen, dieses Ziel zu erreichen. Die beiden Organe sind auch mit den Kommissionsvorschlägen zur Stärkung des **Schengener Informationssystems** (SIS) befasst. Die erste Runde der Beratungen über die drei Vorschläge in den Arbeitsgruppen des Rates wird unter maltesischem Ratsvorsitz abgeschlossen. Der Berichterstatter des Europäischen Parlaments beabsichtigt, Ende Juni 2017 im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) einen Berichtsentwurf vorzulegen. Was den Legislativvorschlag zur Stärkung von **Eurodac** anbelangt, so erzielte der Rat im Dezember 2016 Einigung über eine partielle allgemeine Ausrichtung, während der Ausschuss des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres (LIBE) voraussichtlich im Mai 2017 über seinen Bericht abstimmen wird. Die Trilog-Phase dürfte unmittelbar danach beginnen.

3. Die Arbeit der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität

Im Juni 2016 setzte die Kommission eine hochrangige Expertengruppe für Informationssysteme und Interoperabilität ein. Die Expertengruppe erhielt den Auftrag, **sich mit den rechtlichen, technischen und operativen Herausforderungen im Zusammenhang mit den vier Optionen** zur Erreichung der Interoperabilität, einschließlich

[16] Gemeinsame Erklärung zu den gesetzgeberischen Prioritäten der EU für 2017 vom 13.12.2016, https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-legislative-priorities-2017-jan2017_en.pdf.

www.parlament.gv.at

ihrer Notwendigkeit, technischen Durchführbarkeit, Verhältnismäßigkeit und ihrer datenschutzrelevanten Auswirkungen, **auseinanderzusetzen**.[17] Die Expertengruppe sollte zudem Defizite und etwaige Informationslücken, die auf die Komplexität und Fragmentierung der Informationssysteme zurückzuführen sind, ermitteln und beseitigen.[18] Ihr gehörten Sachverständige aus den Mitgliedstaaten und den assoziierten Schengen-Ländern an sowie aus den EU-Agenturen eu-LISA, Europol, dem Europäischen Unterstützungsbüro für Asylfragen, der Europäischen Agentur für die Grenz- und Küstenwache und der Agentur für Grundrechte. Der EU-Koordinator für die Terrorismusbekämpfung und der Europäische Datenschutzbeauftragte beteiligten sich als Vollmitglieder an den Arbeiten der Expertengruppe. Vertreter des Sekretariats des Ausschusses des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres (LIBE) und des Generalsekretariats des Rates nahmen als Beobachter teil.

Die Kommission begrüßt den Abschlussbericht[19] der hochrangigen Expertengruppe vom 11. Mai 2017. Die Expertengruppe kam zu dem Schluss, dass **es notwendig und technisch möglich ist, auf die folgenden drei Lösungen für die Interoperabilität hinzuarbeiten**, und dass diese Lösungen grundsätzlich sowohl **operative Verbesserungen bewirken** als auch **im Einklang mit den Datenschutzvorschriften** umgesetzt werden können:

- europäisches Suchportal[20],
- gemeinsamer Dienst für den Abgleich biometrischer Daten und
- gemeinsamer Speicher für Identitätsdaten.

Nach Ansicht der Expertengruppe sollte die Option der Vernetzung von Systemen nur im Einzelfall erwogen werden. Ein solcher Fall ist die Vernetzung des vorgeschlagenen Einreise-/Ausreisesystems der EU und des Visa-Informationssystems[21]. Der Vorschlag der Kommission für ein Einreise-/Ausreisesystem der EU sieht vor, dass die im Visa-Informationssystem erfassten Daten systematisch und automatisch vom Einreise-/Ausreisesystem der EU abgefragt würden, damit ein kleiner Teilsatz von Daten (Visummarke, Zahl der Einreisen, Aufenthaltsdauer) gespeichert wird, anhand dessen das Einreise-/Ausreisesystem der EU Daten zu Visuminhabern im Einklang mit den Erfordernissen der Datenminimierung und der Datenkonsistenz korrekt verarbeiten kann. Nach Auffassung der Expertengruppe müssen die Systeme ausschließlich zur Verbesserung des Datenaustauschs nicht unbedingt vernetzt werden, vorausgesetzt, dass hinreichende Fortschritte bei den anderen drei Lösungen für die Interoperabilität erzielt werden.

In dem Abschlussbericht der Expertengruppe wird auch hervorgehoben, **wie wichtig die vollständige Umsetzung und Anwendung der bestehenden Informationssysteme ist**. Gegenstand des Berichts ist auch der dezentrale **Prüm-Rahmen** für den Austausch von

---

17 Beschluss 2016/C 257/03 der Kommission vom 17.6.2016.

18 Siehe das Konzeptpapier der Expertengruppe vom Juni 2016: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=24081&no=2.

19 Der Abschlussbericht der Expertengruppe ist abrufbar unter: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1. Seine Anhänge enthalten eine Zusammenfassung eines Berichts der Grundrechteagentur sowie Erklärungen des Europäischen Datenschutzbeauftragten und des EU-Koordinators für die Terrorismusbekämpfung.

20 Der Begriff „zentrale Schnittstelle für Datenabfragen“ wurde in „europäisches Suchportal“ umgeändert, damit eine Verwechslung mit nationalen zentralen Schnittstellen, die in den Mitgliedstaaten für nationale Informationssysteme bestehen, vermieden wird.

21 Verordnung (EG) Nr. 767/2008 vom 9.7.2008.

DNA-, Fingerabdruck- und Fahrzeugregisterdaten[22]. Empfohlen wird eine Durchführbarkeitsstudie zur Einführung einer zentralen Routing-Komponente und zur etwaigen Hinzufügung neuer Funktionen. In Bezug auf das dezentrale System nach Maßgabe der **EU-Richtlinie über Fluggastdatensätze (PNR-Richtlinie)**[23] empfahl die Expertengruppe eine Durchführbarkeitsstudie über eine zentrale Komponente für vorab zu übermittelnde Fluggastdaten und Fluggastdatensätze, die als technisches Unterstützungstool die Vernetzung mit den Fluggesellschaften erleichtern soll. Sobald die Mitgliedstaaten die PNR-Richtlinie umgesetzt haben, würde diese Maßnahme nach Ansicht der Expertengruppe die Effektivität der PNR-Zentralstellen stärken.

Die Kommission wird ihr Hauptaugenmerk weiterhin auf die **vollständige Anwendung der bestehenden Informationssysteme** legen. Es ist unerlässlich, dass die Mitgliedstaaten diese Systeme in vollem Umfang nutzen und deren Potenzial gänzlich ausschöpfen. Im Einklang mit ihrem Umsetzungsplan[24] wird die Kommission auch künftig umfassende Unterstützung leisten, um sicherzustellen, dass alle Mitgliedstaaten die EU-Richtlinie über Fluggastdatensätze bis Mai 2018 umsetzen. Bei der vollständigen Verwirklichung des Prüm-Rahmens wird sie eng mit allen Mitgliedstaaten zusammenarbeiten, insbesondere mit den fünf Mitgliedstaaten, die die Prüm-Beschlüsse noch umsetzen müssen. Im Sinne der Empfehlungen der Expertengruppe wird die Kommission prüfen, wie sich Funktionsweise und Wirksamkeit dieser Systeme verbessern lassen, wenn sie von den Mitgliedstaaten angewandt werden.

Die Expertengruppe ermittelte eine **Informationslücke in Bezug auf Außengrenzübertritte von EU-Bürgern**. In ihrem Abschlussbericht verweist sie auf die unlängst erfolgte Einführung der Verpflichtung, alle Personen, die nach dem Unionsrecht das Recht auf Freizügigkeit genießen, beim Verlassen des Schengen-Raums und bei der Einreise in den Schengen-Raum einem systematischen Abgleich mit den einschlägigen Datenbanken zu unterziehen.[25] Sie hebt hervor, dass die Zeit und der Ort eines solchen Abgleichs nicht erfasst werden, diese Informationen aber für Strafverfolgungszwecke nützlich sein könnten. Die Expertengruppe empfahl daher, die Verhältnismäßigkeit und Durchführbarkeit einer systematischen Erfassung der Außengrenzübertritte aller EU-Bürger weiter zu analysieren.[26]

Die Kommission merkt an, dass im Bericht der Expertengruppe nicht nachgewiesen wird, dass die Erfassung der Außengrenzübertritte aller EU-Bürger notwendig und verhältnismäßig ist. Sollte eine solche Erfassung aufgrund neuer Erkenntnisse nachweislich notwendig und verhältnismäßig sein, ist die Kommission bereit zu prüfen, ob weitere Maßnahmen getroffen werden müssen. In der Zwischenzeit wird sich die Kommission mit der damit in Zusammenhang stehenden Empfehlung der Expertengruppe befassen, auf eine etwaige Erfassung von „Treffern“ hinsichtlich ausgeschriebener Personen im Schengener Informationssystem hinzuarbeiten, um die Reisebewegungen jener EU-Bürger erfassen zu können, die als möglicherweise an Terrorismus oder anderen Formen schwerer Kriminalität beteiligte Personen ermittelt wurden.

---

22 Beschluss 2008/615/JI des Rates vom 23.6.2008.

23 Richtlinie (EU) 2016/681 vom 27.4.2016.

24 SWD(2016) 426 final vom 28.11.2016.

25 Verordnung (EU) 2017/458 vom 15.3.2017.

26 Die Expertengruppe erörterte außerdem die Optionen einer Ausweitung des vorgeschlagenen Einreise-/Ausreisesystems der EU auf EU-Bürger oder einer erweiterten Verwendung der Protokolle des Schengener Informationssystems. Beide Optionen wurden verworfen.

www.parlament.gv.at

Die Expertengruppe erkannte zudem eine **Informationslücke in Bezug auf Visa für einen längerfristigen Aufenthalt, Aufenthaltstitel und Aufenthaltskarten**. Wie sie feststellte, haben die Mitgliedstaaten kaum Möglichkeiten, diese Dokumente auf ihre Gültigkeit hin zu überprüfen, wenn sie von einem anderen Mitgliedstaat ausgestellt wurden. Sie schlug daher vor zu sondieren, ob ein zentraler EU-Datenspeicher mit Informationen über Visa für einen längerfristigen Aufenthalt, Aufenthaltstitel und Aufenthaltskarten eine Option wäre. Die Kommission wird prüfen, ob ein solcher Speicher notwendig, technisch realisierbar und verhältnismäßig ist.

Des Weiteren heißt es im Bericht der Expertengruppe, dass die **Zollbehörden** ein maßgeblicher Akteur der dienststellenübergreifenden Zusammenarbeit an den Außengrenzen sind. Gemeinsam mit den Zollbehörden prüft die Kommission deshalb die technischen, operativen und rechtlichen Aspekte der Interoperabilität eingehender.

III. HERSTELLUNG DER INTEROPERABILITÄT DER INFORMATIONSSYSTEME

1. Die Kommission strebt die Interoperabilität der Informationssysteme bis zum Jahr 2020 an

In erster Linie geht es darum sicherzustellen, dass Grenzschutz- und Strafverfolgungsbeamte sowie Mitarbeiter von Einwanderungs- und Justizbehörden über die Informationen verfügen, die notwendig sind, um die Außengrenzen besser zu schützen und die innere Sicherheit im Interesse aller Bürger zu erhöhen. Daher muss zunächst dafür gesorgt werden, dass die verschiedenen einschlägigen Informationssysteme effektiv funktionieren und die bereits vorgelegten Legislativvorschläge zügig angenommen werden.

Im Einklang mit der Mitteilung vom April 2016 und auch mit den Erkenntnissen und Empfehlungen der Expertengruppe schlägt die Kommission ein **neues Konzept für die Verwaltung grenz- und sicherheitsrelevanter Daten** vor, das unter uneingeschränkter Achtung der Grundrechte die Interoperabilität aller zentralen EU-Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung[27] gewährleistet, damit

- die Systeme – in vollem Einklang mit den Zweckbindungen und Zugangsrechten – mithilfe eines **europäischen Suchportals** gleichzeitig abgefragt werden können, um die vorhandenen Informationssysteme besser zu nutzen, wobei gegebenenfalls straffere Regeln für den Zugang der Strafverfolgungsbehörden festgelegt werden[28];

[27] Schengener Informationssystem, Visa-Informationssystem, Eurodac, vorgeschlagenes Einreise-/Ausreisesystem der EU, vorgeschlagenes Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) und vorgeschlagenes Europäisches Strafregisterinformationssystem (ECRIS) für Drittstaatsangehörige.

[28] Am 2. März 2017 erteilte der Ausschuss der Ständigen Vertreter (AStV) des Rates dem Ratsvorsitz ein Mandat für die Aufnahme von interinstitutionellen Verhandlungen über das Einreise-/Ausreisesystem der EU und forderte die Kommission anschließend auf, einen umfassenden Rahmen für den Zugang der Strafverfolgungsbehörden zu den verschiedenen Datenbanken im Bereich Justiz und Inneres im Hinblick auf eine stärkere Vereinfachung, eine größere Einheitlichkeit und Wirksamkeit sowie eine bessere Berücksichtigung operativer Erfordernisse vorzuschlagen. Die Expertengruppe empfiehlt, den Rahmen für den Zugang der Strafverfolgungsbehörden auf ein zweistufiges Konzept zu stützen, bei dem nur dann eine Visualisierung von Daten in Betracht gezogen würde, wenn bereits überprüft wurde, dass die betreffenden Daten existieren, wodurch die Wirksamkeit erhöht, die Zahl und der Umfang der Datenzugriffe durch Strafverfolgungsbehörden aber verringert würde.

www.parlament.gv.at

- die Informationssysteme einen **gemeinsamen Dienst für den Abgleich biometrischer Daten** nutzen, der die gleichzeitige Abfrage verschiedener Informationssysteme, in denen biometrische Daten erfasst sind, ermöglicht, gegebenenfalls mit der Kennzeichnung „Treffer“ oder „kein Treffer“, der sich entnehmen lässt, ob ein Zusammenhang mit entsprechenden biometrischen Daten in einem anderen System besteht[29];
- die Systeme auf einen **gemeinsamen Speicher für Identitätsdaten**, in dem alphanumerische Identitätsdaten erfasst sind[30], zurückgreifen, um zu ermitteln, ob eine Person in verschiedenen Datenbanken unter mehreren Identitäten registriert ist.

Dieses neue Konzept muss gewährleisten, dass die **spezifischen Datenschutzbestimmungen** der einzelnen Systeme beibehalten, aber spezielle Vorschriften für den Zugang der zuständigen Behörden, separate Zweckbindungsbestimmungen für jede Datenkategorie und spezielle Vorschriften für die Datenspeicherung festgelegt werden. Das Konzept für die Interoperabilität hätte nicht die Vernetzung aller Einzelsysteme zur Folge.

Mit dem neuen Konzept würden die derzeitigen Mängel der EU-Datenverwaltungsarchitektur behoben und die ermittelten Informationslücken geschlossen. Unter anderem mit den bereits laufenden und weiteren technischen Analysen wird die Agentur **eu-LISA** maßgeblich zu den Arbeiten an der Interoperabilität der Informationssysteme beitragen (siehe Abschnitt III.2). Der Legislativvorschlag, den die Kommission im Juni 2017 vorlegen wird, wird das Mandat der Agentur stärken, damit diese für die Umsetzung des neuen Konzepts sorgen kann. Die Kommission wird auch künftig den Europäischen Datenschutzbeauftragten und die Grundrechteagentur in die Arbeiten an der Interoperabilität einbeziehen.

Die Gewährleistung einer hohen **Datenqualität ist eine wesentliche Voraussetzung für die Effektivität der Informationssysteme**. Die Interoperabilität kann nur funktionieren, wenn genaue und vollständige Daten in die Informationssysteme eingespeist werden. Die Kommission hat bereits darauf hingewiesen, dass in Bezug auf die Datenqualität noch Handlungsbedarf auf EU-Ebene besteht.[31] Gemeinsam mit eu-LISA wird sie unverzüglich den Empfehlungen der Expertengruppe zur Verbesserung der Qualität der Daten in den EU-Informationssystemen nachkommen.

Die Kommission wird die Empfehlungen der Expertengruppe zur automatisierten Qualitätskontrolle, zur Schaffung eines „Data Warehouse“, mit dem aus den relevanten Informationssystemen extrahierte anonymisierte Daten zu statistischen und Berichterstattungszwecken ausgewertet werden können, und zu Schulungsmodulen betreffend die Datenqualität für das für die Eingabe von Daten in die Systeme auf nationaler Ebene verantwortliche Personal umsetzen. Der künftige Legislativvorschlag wird auch vorsehen, dass eu-LISA eine wichtige Rolle bei der Sicherstellung einer hohen Datenqualität in den zentralen EU-Informationssystemen zukommt.

Die Interoperabilität setzt das technische Zusammenwirken der bestehenden Informationssysteme voraus. Das **universelle Nachrichtenformat** (Universal Message Format – UMF) soll auf EU-Ebene dieses Zusammenwirken erleichtern. Zusammen mit eu-

[29] Es bedarf weiterer technischer Analysen hinsichtlich der etwaigen Einbeziehung von Kennzeichnungsfunktionen in einen gemeinsamen Dienst für den Abgleich biometrischer Daten und hinsichtlich der datenschutzrelevanten Auswirkungen – siehe Abschnitt III.2.

[30] Dazu würden auch gebräuchliche biografische Attribute wie Name, Geburtsdatum und Geschlecht gehören.

[31] Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Vierter Fortschrittsbericht (COM(2017) 41 final vom 25.1.2017).

www.parlament.gv.at

LISA wird die Kommission die Empfehlungen der Expertengruppe zur Verbesserung des UMF im Einklang mit den laufenden Arbeiten umsetzen, um dafür Sorge zu tragen, dass die Weiterentwicklung des Formats ihren Niederschlag in den zentralen EU-Informationssystemen findet.

2. Vorgehen zur Erreichung der Interoperabilität der Informationssysteme bis zum Jahr 2020

Die Kommission ersucht das Europäische Parlament und den Rat, parallel zu den Arbeiten an der Umsetzung der Prioritäten für die Informationssysteme eine **gemeinsame Debatte über das weitere Vorgehen** in Bezug auf die in dieser Mitteilung dargelegte Interoperabilität abzuhalten. Zu diesem Zweck wird die Kommission am 29. Mai 2017 dem Ausschuss des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres (LIBE) und am 8. Juni 2017 den Mitgliedstaaten im Rat „Justiz und Inneres" diese Ideen vorstellen und mit ihnen erörtern. Auf der Grundlage dieser Beratungen sollten die drei Organe im Herbst 2017 im Rahmen von trilateralen Fachsitzungen[32] über das weitere Vorgehen in Bezug auf die in dieser Mitteilung erläuterte Interoperabilität eingehender diskutieren, unter anderem auch darüber, welche operativen Erfordernisse im Bereich Grenzen und Sicherheit zu berücksichtigen und wie die Verhältnismäßigkeit und die uneingeschränkte Achtung der Grundrechte zu gewährleisten sind. So bald wie möglich, spätestens aber bis Ende 2017 soll **Einvernehmen über das weitere Vorgehen** und die Schritte erzielt werden, die erforderlich sind, um die Interoperabilität der Informationssysteme bis zum Jahr 2020 zu erreichen.

Parallel zu den gemeinsamen Beratungen zwischen den drei Organen und ohne deren Ergebnis vorzugreifen, werden die Kommission und eu-LISA die **technische Analyse der für die Interoperabilität ermittelten Lösungen** im Laufe des Jahres 2017 anhand einer Reihe von technischen Studien und Konzeptnachweisen fortsetzen. Die Kommission wird das Europäische Parlament und den Rat regelmäßig über die bei dieser technischen Analyse erzielten Fortschritte unterrichten.

Unter Berücksichtigung des Austauschs mit dem Europäischen Parlament und dem Rat sowie des Ergebnisses der laufenden gesetzgeberischen Arbeiten zu den Informationssystemen und der weiteren technischen Analyse **arbeitet die Kommission intensiv daran, so bald wie möglich**[33] **einen Legislativvorschlag über die Interoperabilität vorzulegen**. Im Einklang mit den Grundsätzen der besseren Rechtsetzung werden im Zuge der Ausarbeitung des Legislativvorschlags eine öffentliche Konsultation und eine Folgenabschätzung – unter anderem auch zu den Grundrechten und insbesondere dem Recht auf Schutz personenbezogener Daten – durchgeführt. Zusammen mit dem Legislativvorschlag über die Interoperabilität wird die Kommission außerdem einen Legislativvorschlag zur Überarbeitung der Rechtsgrundlage des Visa-Informationssystems[34] vorlegen, der dem im Oktober 2016 vorgelegten Evaluierungsbericht[35] Rechnung trägt. Das Visa-Informationssystem ist eines der zentralen Informationssysteme, die Teil des neuen Konzepts für die Verwaltung grenz- und sicherheitsrelevanter Daten sein sollten.

---

[32] Die Fachsitzungen könnten dem Vorbild der Sitzung zum Thema „Intelligente Grenzen" vom Februar 2015 folgen.

[33] Dies erfordert eine Einigung der beiden gesetzgebenden Organe über die entsprechenden derzeit erörterten Gesetzgebungsdossiers – siehe Abschnitt II.2.

[34] Verordnung (EG) Nr. 767/2008 vom 9.7.2008.

[35] COM(2016) 655 final vom 14.10.2016.

www.parlament.gv.at

Die **gemeinsamen Beratungen zwischen den drei Organen über das weitere Vorgehen zur Erreichung der Interoperabilität bis zum Jahr 2020 dürfen nicht die Arbeiten an den Legislativvorschlägen** zu den Informationssystemen **verzögern**, die derzeit vom Europäischen Parlament und vom Rat erörtert werden. Die meisten dieser Vorschläge wurden in der Gemeinsamen Erklärung bereits als dringlich und als wichtige Prioritäten eingestuft. Sie alle sollen erhebliche Informationslücken schließen, bei denen im Einklang mit den Empfehlungen der Expertengruppe unmittelbarer Handlungsbedarf besteht. Der ergänzende Legislativvorschlag betreffend ein Europäisches Strafregisterinformationssystem (ECRIS) für Drittstaatsangehörige, den die Kommission im Juni 2017 vorlegen wird, wird den Empfehlungen der Expertengruppe zur Interoperabilität und dem in dieser Mitteilung dargelegten Konzept ebenfalls in vollem Umfang Rechnung tragen. Um dieses neue Konzept auf praktikable Weise umsetzen zu können, ist es von entscheidender Bedeutung, dass sich alle betroffenen Informationssysteme auf stabile Rechtsgrundlagen stützen. Daher muss zunächst eine Einigung über die derzeit erörterten Legislativvorschläge erzielt werden.

IV. UMSETZUNG WEITERER PRIORITÄTEN IM BEREICH DER SICHERHEIT

1. Legislative Initiativen

Am 1. Mai 2017 trat die neue **Europol-Verordnung**[36] in Kraft. Sie stellt einen Wendepunkt für Europol dar und enthält einige neue Elemente, die es der EU-Strafverfolgungsagentur ermöglichen werden, zu einem echten EU-Knotenpunkt für den Austausch von Informationen über schwere grenzüberschreitende Kriminalität und Terrorismus zu werden. Europol wird über die Instrumente verfügen, die erforderlich sind, um wirkungsvoller, effizienter und rechenschaftspflichtiger handeln zu können. Insbesondere aufgrund der veränderten Rahmenbedingungen für die Datenverarbeitung wird die Agentur besser in der Lage sein, strafrechtliche Analysen für die Mitgliedstaaten zu erstellen. Zudem wird eine solidere Datenschutzregelung für eine unabhängige und wirksame datenschutzrechtliche Überwachung sorgen.

Wie im Vertrag festgeschrieben, werden die Tätigkeiten von Europol auch künftig vom Europäischen Parlament in Zusammenarbeit mit den nationalen Parlamenten kontrolliert, was die Transparenz und Legitimität der Agentur in den Augen der Bürger weiter erhöhen wird.

Um die negativen Auswirkungen des Ausscheidens Dänemarks aus Europol nach dem Ausgang des Referendums vom 3. Dezember 2016 in Dänemark zu minimieren, wurde am 30. April 2017 ein **Abkommen über operative Kooperation zwischen Europol und Dänemark** unterzeichnet. Wie Kommissionspräsident Juncker, Ratspräsident Tusk und der dänische Ministerpräsident Rasmussen in ihrer gemeinsamen Erklärung vom 15. Dezember 2016[37] übereinkamen, wurden in dem Abkommen besondere operative Vereinbarungen festgelegt, die eine ausreichende operative Zusammenarbeit zwischen Dänemark und Europol, wie etwa den Austausch von operativen Daten und Verbindungsbeamten, vorbehaltlich angemessener Garantien gewährleisten. Wenn auch dieses Abkommen kein Ersatz für die Vollmitgliedschaft Dänemarks bei Europol, d. h. den Zugang zu den Europol-Datenbeständen oder die Vollmitgliedschaft in den Gremien zur Steuerung von Europol, ist, so hat Dänemark doch die Zuständigkeit des Europäischen Gerichtshofs und des

[36] Verordnung (EU) 2016/794 vom 11.5.2016.

[37] Erklärung des Präsidenten der Europäischen Kommission, Jean-Claude Juncker, des Präsidenten des Europäischen Rates, Donald Tusk, und des dänischen Ministerpräsidenten, Lars Løkke Rasmussen, vom 15.12.2016, http://europa.eu/rapid/press-release_IP-16-4398_de.htm.

www.parlament.gv.at

Europäischen Datenschutzbeauftragten anerkannt und die einschlägigen EU-Datenschutzvorschriften[38] in dänisches Recht umgesetzt. Wie in der gemeinsamen Erklärung festgehalten, sind diese Vereinbarungen an den Verbleib Dänemarks in der EU und im Schengen-Raum geknüpft.

Am 28. April 2017 erließ die Kommission einen Durchführungsbeschluss über die gemeinsamen Protokolle und Datenformate, die von den Fluggesellschaften für die Übermittlung von **Fluggastdatensätzen (PNR-Daten)** an die PNR-Zentralstellen gemäß der EU-Richtlinie über Fluggastdatensätze[39] zu verwenden sind. Mit diesem Durchführungsbeschluss werden die technischen Aspekte der Übermittlung von Fluggastdatensätzen durch Fluggesellschaften harmonisiert. Die vereinbarten Datenformate und Übertragungsprotokolle werden ab dem 28. April 2018 für alle Übermittlungen von Fluggastdatensätzen durch die Fluggesellschaften an die PNR-Zentralstellen verbindlich sein.

Am 25. April 2017 nahm der Rat die neue **Feuerwaffen-Richtlinie**[40] förmlich an. Die Mitgliedstaaten haben nun 15 Monate Zeit, um die erforderlichen Kontrollen in Bezug auf den Erwerb und den Besitz von Feuerwaffen einzuführen und somit dafür zu sorgen, dass sich kriminelle Gruppierungen oder Terroristen nicht die uneinheitlichen Vorschriften in der Union zunutze machen können. Im Hinblick auf die Annahme einer überarbeiteten Fassung der Verordnung (EU) 2015/2403 der Kommission vor Juli 2017 erzielte die Expertengruppe für Deaktivierungsstandards am 28. April 2017 Einvernehmen über die neuen Deaktivierungsstandards. Ziel der derzeitigen überarbeiteten Fassung ist es, einige technische Standards zu präzisieren, um die ordnungsgemäße Anwendung aller technischen Verfahren für die Deaktivierung von Feuerwaffen zu gewährleisten.

2. Umsetzung nichtlegislativer Maßnahmen

Der schwere weltweite Ransomware-Angriff vom 12. Mai 2017 hat deutlich gemacht, dass die EU und ihre Agenturen sowie die Mitgliedstaaten ihre Maßnahmen zur Bekämpfung der zunehmenden Bedrohung durch **Cyberkriminalität** intensivieren und auch stärker auf die Aufdeckung und Abschreckung ausrichten müssen. Aufgrund der bisherigen einschlägigen Arbeiten des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität bei Europol (EC3), insbesondere der Kampagne „No More Ransom“, hat das EC3 eine führende Rolle bei der Reaktion der Strafverfolgungsbehörden auf den jüngsten Angriff gespielt. Das IT-Notfallteam der EU (Computer Emergency Response Team – CERT) stand in engem Kontakt mit dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität, den Reaktionsteams für Computersicherheitsverletzungen (Computer Security Incident Response Teams – CSIRT) der betroffenen Länder, Einrichtungen zur Bekämpfung der Cyberkriminalität und maßgeblichen Partnern aus der Industrie, um die Bedrohung zu mindern und den Opfern Unterstützung zu leisten. In der Halbzeitbewertung zum digitalen Binnenmarkt vom 10. Mai 2017 kündigte die Kommission ihre Absicht an, die Cybersicherheitsstrategie der EU aus dem Jahr 2013 bis September 2017 zu überprüfen. Diese Arbeit wird beschleunigt, um sicherzustellen, dass die gegenwärtige Fokussierung auf die Prävention dahin gehend erweitert wird, dass der Aufdeckung und Abschreckung mehr Gewicht eingeräumt wird. Es sollte angestrebt werden, die Wahrscheinlichkeit von Cyberangriffen zu verringern, deren Auswirkungen durch Stärkung der Widerstandsfähigkeit abzuschwächen und die Arbeiten der Mitgliedstaaten beim Ausbau nationaler Kapazitäten und der vollständigen Umsetzung

[38] Richtlinie (EU) 2016/680 vom 27.4.2016.
[39] Richtlinie (EU) 2016/681 vom 27.4.2016.
[40] http://www.consilium.europa.eu/de/press/press-releases/2017/04/25-control-acquisition-possession-weapons/

der Richtlinie für Netz- und Informationssicherheit[41] voranzutreiben. Das Potenzial für Cyberkriminalität (und durch den Cyberraum ermöglichte Kriminalität) ergibt sich nicht nur aus Mängeln in Systemen und Software, sondern geht auch auf Verhaltensweisen zurück, die zu einer schlechten Cyberhygiene führen. Die Kommission wird zum einen das Mandat der EU-Agentur für Netz- und Informationssicherheit (ENISA) stärken und zum anderen Vorschläge zur Entwicklung von Cybersicherheitsnormen sowie zur Zertifizierung und Kennzeichnung vorlegen, um die Cybersicherheit von Systemen und Geräten zu erhöhen. Außerdem wird sie einen Schwerpunkt auf den Aufbau von Cyber-Kompetenzen und technischen Kapazitäten in der Union legen.

Angesichts der derzeitigen Bedrohungen für die öffentliche Ordnung oder die innere Sicherheit können **verstärkte Polizeikontrollen** im Hoheitsgebiet der Mitgliedstaaten, unter anderem auch in den Grenzgebieten, sowohl notwendig als auch gerechtfertigt sein, um die Sicherheit im Schengen-Raum zu erhöhen. Daher unterbreitete die Kommission am 2. Mai 2017 eine Empfehlung zu verhältnismäßigen Polizeikontrollen und zur polizeilichen Zusammenarbeit im Schengen-Raum[42]. Die Empfehlung enthält Maßnahmen, die die Schengen-Staaten ergreifen sollten, damit die bestehenden polizeilichen Befugnisse wirksamer zur Bewältigung von Bedrohungen für die öffentliche Ordnung oder die innere Sicherheit ausgeübt werden können. Falls notwendig und gerechtfertigt, sollten die Mitgliedstaaten die Polizeikontrollen in Grenzgebieten und entlang der Hauptverkehrsrouten verstärken. Die Entscheidung darüber, ob, wo und in welcher Intensität diese Kontrollen durchgeführt werden, bleibt voll und ganz den Mitgliedstaaten überlassen und sollte stets in einem angemessenen Verhältnis zu den festgestellten Bedrohungen stehen. Des Weiteren empfiehlt die Kommission, dass alle Mitgliedstaaten die grenzüberschreitende polizeiliche Zusammenarbeit im Hinblick auf die Bewältigung von Bedrohungen für die öffentliche Ordnung oder die innere Sicherheit intensivieren.

Im Bereich der **Luftverkehrssicherheit** gab es in den letzten Wochen einige Entwicklungen, in deren Verlauf die Vereinigten Staaten und das Vereinigte Königreich neue Sicherheitsmaßnahmen für Flüge aus einer Reihe von Ländern im Nahen Osten und in Nordafrika sowie aus der Türkei vorschrieben, wonach größere elektronische Geräte nur im aufgegebenen Gepäck erlaubt sind. Auf Seiten der EU kamen die Arbeiten zur Risikobewertung in Bezug auf Bedrohungen und Schwachstellen für Flüge aus Drittländern voran. Aufgrund von Informationen, wonach die Vereinigten Staaten möglicherweise planen, ähnliche Maßnahmen für Flüge von EU-Flughäfen einzuführen, hat die Kommission Kontakte auf politischer Ebene hergestellt, um eine Abstimmung des Vorgehens zwischen den Vereinigten Staaten und der EU zu gewährleisten. Am 17. Mai 2017 findet in Brüssel ein Treffen zwischen Vertretern der Vereinigten Staaten und der EU statt, bei dem die potenziellen Risiken zusammen bewertet werden sollen und ein gemeinsames Konzept für die Eindämmung der zunehmenden Bedrohungen entwickelt werden soll.

Im Ständigen Ausschuss des Rates für die operative Zusammenarbeit im Bereich der inneren Sicherheit (COSI) laufen Arbeiten zum nächsten **EU-Politikzyklus zur Bekämpfung der organisierten und schweren internationalen Kriminalität** für die Jahre 2018 bis 2021, bei denen die acht Prioritäten für die Bekämpfung krimineller Bedrohungen, die die Kommission

---

41 Richtlinie (EU) 2016/1148 vom 6.7.2016.

42 Am 2. Mai 2017 billigte die Kommission grundsätzlich die Empfehlung zu verhältnismäßigen Polizeikontrollen und zur polizeilichen Zusammenarbeit im Schengen-Raum (C(2017) 2923). Die förmliche Annahme erfolgte am 12. Mai 2017.

im letzten Fortschrittsbericht zur Sicherheitsunion[43] aufgeführt hatte, berücksichtigt werden. Der Rat wird voraussichtlich am 18. Mai 2017 Schlussfolgerungen des Rates zum neuen EU-Politikzyklus annehmen.

Nach dem Fortschrittsbericht über die laufenden Arbeiten zur Verbesserung des grenzüberschreitenden Zugangs von Strafermittlern zu **elektronischen Beweismitteln**[44], den die Kommission dem Rat „Justiz und Inneres" im Dezember 2016 vorgelegt hatte, schließt sie derzeit ihre Bewertung ab und wird auf der Tagung des Rates „Justiz und Inneres" am 8. Juni 2017 einen Vorschlag für das weitere Vorgehen zur Diskussion stellen.

Die Kommission hat die aktuellen Arbeiten einer Gruppe von Mitgliedstaaten zur Pflege von e-CODEX, einem System für die grenzüberschreitende justizielle Zusammenarbeit und den elektronischen Zugang zu Gerichtsverfahren, unterstützt. Sie hat zur Kenntnis genommen, dass es sich dabei nach Ansicht dieser Mitgliedstaaten nicht um eine dauerhafte Lösung handelt. In den Arbeitsgruppen des Rates haben die Mitgliedstaaten verschiedene Optionen geprüft und kamen zu dem Schluss, dass eu-LISA am besten dazu in der Lage wäre, für die Pflege und Operabilität des e-CODEX-Systems zu sorgen. Um herauszufinden, welche Lösung die beste ist, unterzieht die Kommission die verschiedenen Optionen für die Pflege von e-CODEX einer Folgenabschätzung. Das Ergebnis dieser Folgenabschätzung wird im Herbst 2017 vorliegen.

Dass die Feuerwaffen-Richtlinie wie bereits erwähnt erlassen wurde, ist ein wichtiger Schritt zur Durchsetzung der Vorschriften über den rechtmäßigen Erwerb und Besitz von Feuerwaffen. Die Kommission will sowohl innerhalb als auch außerhalb der EU gegen den **illegalen Handel mit Feuerwaffen** vorgehen. Am 16. März 2017 wurden in Kiew im Rahmen eines Runden Tisches zwischen der EU und der Ukraine technische Fragen im Zusammenhang mit der Bekämpfung des illegalen Handels mit Feuerwaffen erörtert. Dabei handelte es sich um das erste Treffen dieser Art, das zwischen der EU und der Ukraine stattfand, um den Informationsaustausch in Bezug auf den illegalen Handel mit Feuerwaffen zu verbessern. Am 28. März 2017 fand in Tunis unter Beteiligung der EU und Tunesiens ein zweiter Runder Tisch zu technischen Fragen im Zusammenhang mit der Bekämpfung des illegalen Handels mit Feuerwaffen statt. Sowohl für die Ukraine als auch für Tunesien wurde ein Aktionsplan vereinbart, der auch Besuche von Sachverständigen der EU vorsieht, die den Verwaltungsrahmen jedes Landes beurteilen, eine hochrangige Konferenz über die entsprechenden Rechtsvorschriften organisieren und Schulungen, Studienbesuche und Workshops zur Datenverwaltung in der Praxis sowie eine operative Zusammenarbeit vorschlagen sollen.

Die Kommission und der Europäische Auswärtige Dienst legten dem Rat am 12. Mai 2017 ein **gemeinsames Non-Paper über die externen Maßnahmen der EU zur Terrorismusbekämpfung** vor, in dem die vorrangigen Länder, Bereiche und Instrumente für einschlägige EU-Maßnahmen aufgezeigt werden. Dieses gemeinsame Papier liefert einen

---

[43] COM(2017) 213 final vom 12.4.2017. Die von der Kommission ermittelten acht Prioritäten für die Bekämpfung krimineller Bedrohungen sind: Cyberkriminalität, Drogenkriminalität, Schleusung von Migranten, organisierte Eigentumskriminalität, Menschenhandel, illegaler Handel mit Feuerwaffen, Mehrwertsteuerbetrug und Umweltkriminalität.

[44] Siehe das Non-Paper der Kommissionsdienststellen: „Progress report following the Conclusions of the Council of the European Union on improving criminal justice in cyberspace" vom 2.12.2016: http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf. Der Rat forderte in seinen Schlussfolgerungen zur Verbesserung der Strafjustiz im Cyberspace vom 9. Juni 2016 die Kommission auf, konkrete Maßnahmen zu ergreifen, ein gemeinsames Konzept der EU zu entwickeln und bis Juni 2017 Ergebnisse vorzulegen.

Beitrag zu der Diskussion über die Überarbeitung der Schlussfolgerungen des Rates vom Februar 2015 über externe Maßnahmen der EU zur Terrorismusbekämpfung[45] mit dem Ziel, auf der Tagung des Rates „Auswärtige Angelegenheiten“ im Juni 2017 neue Schlussfolgerungen des Rates anzunehmen.

Im Zuge der Erweiterung der externen Dimension des Europäischen Programms für den Schutz kritischer Infrastrukturen fand am 16. und 17. März 2017 in Bukarest ein erster Workshop zwischen der EU und Nachbarländern über den **Schutz kritischer Infrastrukturen** statt. Neben Vertretern aus den Mitgliedstaaten gehörten zu den Teilnehmern Vertreter aus acht Ländern Osteuropas und des westlichen Balkans. Ziel dieses Workshops war es, Kontakte zu knüpfen und Informationen über Maßnahmen und Instrumente für den Schutz kritischer Infrastrukturen auszutauschen. Etwaige Bereiche für eine weitere Zusammenarbeit wurden ermittelt, darunter auf praktische (operative) Aspekte ausgerichtete gemeinsame Schulungen oder Übungen, Studien über regionale Interdependenzen und wechselseitige Überprüfungen nationaler Strategien für den Schutz kritischer Infrastrukturen.

V. FAZIT

Die Kommission fordert das Europäische Parlament und den Rat auf, die Arbeiten zu den legislativen Prioritäten in Bezug auf die Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung voranzubringen. Dadurch werden die vorhandenen Systeme gestärkt und die bereits ermittelten Informationslücken geschlossen. Somit wird den Erfordernissen von Grenzschutz- und Strafverfolgungsbeamten einschließlich Zollbeamten und Mitarbeitern von Einwanderungs- und Justizbehörden Rechnung getragen sowie die Grundlage für eine größere Interoperabilität dieser Systeme geschaffen.

Im Nachgang zu der Mitteilung „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“ vom April 2016 und unter Berücksichtigung der Empfehlungen der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität hat die Kommission ein neues Konzept für die Verwaltung grenz- und sicherheitsrelevanter Daten vorgeschlagen, das unter uneingeschränkter Wahrung der Grundrechte die Interoperabilität aller zentralen EU-Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung gewährleistet. Zu diesem Zweck wird die Kommission auf der Grundlage der laufenden gesetzgeberischen und technischen Arbeiten zu den Informationssystemen im Juni 2017 einen Legislativvorschlag zur Stärkung des Mandats von eu-LISA im Hinblick auf die Umsetzung des neuen Konzepts durch die Agentur vorlegen, dem so bald wie möglich ein Legislativvorschlag über die Interoperabilität folgen soll. Die Kommission ersucht das Europäische Parlament und den Rat, eine gemeinsame Debatte über das vorgeschlagene weitere Vorgehen abzuhalten. So könnten die drei Organe Einvernehmen über das weitere Vorgehen in Bezug auf die Interoperabilität und die Schritte erzielen, die erforderlich sind, um in vollem Einklang mit den Grundrechten die Interoperabilität der Informationssysteme bis zum Jahr 2020 zu erreichen. Die Umsetzung des erläuterten Konzepts für die Interoperabilität würde für eine wirksamere und effizientere Datenverwaltung in der EU sorgen, damit ein besserer Schutz der Außengrenzen gewährleistet und die innere Sicherheit im Interesse aller Bürger erhöht wird.

---

[45] Schlussfolgerungen des Rates vom 9.2.2015 zur Terrorismusbekämpfung: http://www.consilium.europa.eu/en/press/press-releases/ 2015/02/150209-council-conclusions-counter-terrorism/.

www.parlament.gv.at