Europäischer Wirtschafts- und Sozialausschuss

SOC/573
Paket zur Interoperabilität

STELLUNGNAHME

Europäischer Wirtschafts- und Sozialausschuss

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (Grenzen und Visa) und zur Änderung der Entscheidung 2004/512/EG des Rates, der Verordnung (EG) Nr. 767/2008, des Beschlusses 2008/633/JI des Rates, der Verordnung (EU) 2016/399 und der Verordnung (EU) 2017/2226
[COM(2017) 793 final – 2017/0351 (COD)]
Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration)
[COM(2017) 794 final – 2017/0352 (COD)]

Berichterstatterin: **Laure BATUT**

Befassung	Europäische Kommission, 19/01/2018
Rechtsgrundlage	Artikel 304 des Vertrags über die Arbeitsweise der Europäischen Union
Zuständige Fachgruppe	Fachgruppe Beschäftigung, Sozialfragen, Unionsbürgerschaft
Annahme in der Fachgruppe	25/04/2018
Verabschiedung auf der Plenartagung	23/05/2018
Plenartagung Nr.	535
Ergebnis der Abstimmung (Ja-Stimmen/Nein-Stimmen/Enthaltungen)	160/3/2

1. **Schlussfolgerungen und Empfehlungen**

1.1 Der Europäische Wirtschafts- und Sozialausschuss (EWSA) hält den Vorschlag der Europäischen Kommission zur Verbesserung der Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa sowie polizeiliche und justizielle Zusammenarbeit, Asyl und Migration für nützlich und positiv.

1.2 Der EWSA ist der Auffassung, dass diese Interoperabilität ein strategisches Ziel für die EU sein muss, damit sie ein offener Raum bleibt, in dem die Grundrechte und die Mobilität gewährleistet werden. Die EU und die Mitgliedstaaten sind dazu verpflichtet, für den Schutz des Lebens und die Sicherheit aller Menschen zu sorgen; der Grundsatz der Nichtzurückweisung sollte voll und ganz geachtet werden.

1.3 Maßnahmen zugunsten der Interoperabilität werden umso besser verstanden, wenn sie:

- im Rahmen der EU-Migrationsstrategie die Voraussetzungen für ein Gleichgewicht zwischen Freiheit und Sicherheit unter Achtung der Gewaltenteilung garantieren;
- die Wahrung der Grundrechte der betroffenen Personen gewährleisten, insbesondere die Sicherung ihrer personenbezogenen Daten und ihres Privatlebens, das Recht auf Zugang zu ihren Daten, auf Berichtigung der Daten sowie auf deren Löschung innerhalb einer angemessenen Frist und durch zugängliche Verfahren;
- die Forderung der Aufnahme der Grundsätze des Datenschutzes bereits in der Konzeptionsphase („eingebauter Datenschutz“) und in allen Durchführungsvorschriften bekräftigen;
- keine neuen Hindernisse beim normalen Personen- und Güterverkehr schaffen.

1.4 Der EWSA fordert Verfahren und Garantien in Bezug auf die Nutzung von Daten zu Strafverfolgungszwecken, die:

- in diesem Bereich die Anwendung des europäischen Gesetzes mit dem stärksten Schutz (Datenschutz-Grundverordnung) vorsehen;
- ermöglichen, die Feststellung des Mitgliedstaats zu beschleunigen, der für die Prüfung der Anträge auf internationalen Schutz zuständig ist;
- das Recht der betroffenen Personen auf zwei Instanzen garantieren;
- Minderjährigen, insbesondere unbegleiteten Minderjährigen (unabhängig davon, ob es sich um illegal aufhältige, verfolgte oder kriminelle Personen handelt) das Recht, ein Visum zu erhalten, das Recht auf Schutz und Integration und die Möglichkeit, das Recht auf Vergessen in Anspruch zu nehmen, garantieren, wobei eine kürzere Frist als für volljährige Personen gelten sollte.

1.5 Der EWSA ist der Auffassung, dass die derzeitige Rechtsgrundlage für die Informationssysteme verstärkt und dabei die Skalierbarkeit der Datenerhebungssysteme berücksichtigt werden sollte. Er fordert:

- die Stärkung der Sicherheit der bestehenden Datenbanken und ihrer Kommunikationskanäle;
- die Bewertung der Auswirkungen einer verstärkten Vorabkontrolle auf das Risikomanagement;
- eine Kontrolle und eine ständige Evaluierung der Struktur durch die Datenschutzbehörden (EDSB); er fordert, dass die Verantwortlichen gegenüber den Entscheidungsbehörden und der Kommission jährlich über die Sicherheit der Interoperabilitätskomponenten sowie zweijährlich über die Auswirkungen der Maßnahmen auf die Grundrechte Bericht erstatten.

1.6 Der EWSA ist der Auffassung, dass sich das Projekt auf qualifiziertes Personal stützen muss, und empfiehlt:

- solide Schulungsprogramme für die betroffenen Behörden und die Beamten von eu-LISA;
- eine strikte Kontrolle der Kompetenzen der Beamten und Bewerber für diese Agentur.

1.7 Der EWSA äußert Bedenken gegen die Finanzierung des neuen Systems. Die Überwachung der Planung wird von entscheidender Bedeutung sein, um die Verschwendung von Haushaltsmitteln zu vermeiden und das Projekt bis 2029 zu beenden.

1.8 Der EWSA empfiehlt, die Bürger bis zum Abschluss des Projekts über dessen Fortschritte zu informieren und die betroffenen Personen über die Kontrollen, denen sie unterworfen werden, aufzuklären. Seiner Ansicht nach muss die Möglichkeit vorgesehen werden, den gesamten Prozess zu stoppen, wenn die Freiheit und die Grundrechte durch Missbrauch des Systems bedroht würden.

2. Einführung

2.1 Im internationalen Kontext des Jahres 2017, der sowohl auf geopolitischer Ebene als auch im Hinblick auf die innere Sicherheit in den Mitgliedstaaten als instabil gilt, hat der Rat die Kommission mehrfach aufgefordert, Mittel vorzusehen, um als „Gefährder“ eingestufte Personen aufzuspüren, die bereits in einem der Mitgliedstaaten erfasst sind. Die Ermittlung ihrer Grenzübertritte, Reisen und Wege in Europa könnte für die Sicherheit in der Union von entscheidender Bedeutung sein.

2.2 In seiner Entschließung vom 6. Juli 2016 forderte das Parlament die Kommission auf, die erforderlichen Datenschutzvorkehrungen zu treffen.

2.3 Die hier behandelten Dokumente sind Teil der Zielsetzung „Schengen bewahren und stärken“[1]. Die Union verfügt in den Bereichen, die mit der Kontrolle der Grenzübertritte von Personen und Waren zusammenhängen, bereits über mehrere Regelungen und digitale Informationsdienste.

1 COM(2017) 570 final.

2.4 Zur Erinnerung:

- **SIS: Schengener Informationssystem**, einer der ältesten Mechanismen; mit dem überarbeiteten System wird ein breites Spektrum an Warnmeldungen zu Personen und Waren verwaltet;
- **Eurodac: Europäisches System zum Vergleich der Fingerabdruckdaten** von Asylbewerbern und illegal aufhältigen Drittstaatsangehörigen an den Grenzen und in den Mitgliedstaaten und zur Feststellung des für die Anträge zuständigen Mitgliedstaats (CESE 2016-02981, Berichterstatter: Herr Moreno Díaz[2]);
- **VIS: Visa-Informationssystem** (Visakodex), durch das Visa für Kurzzeitaufenthalte verwaltet werden (CESE 2014-02932, Berichterstatter: Herr Pezzini und Herr Pariza Castaños[3]);
- **EES: Einreise-/Ausreisesystem**, über das noch entschieden werden muss; mit dem System werden die Daten der Reisepässe und die Zeitpunkte der Ein- und Ausreise von Drittstaatsangehörigen elektronisch verwaltet, die den Schengenraum besuchen (CESE 2016-03098, SOC/544, Berichterstatter: Herr Pîrvulescu[4]);
- **ETIAS: Europäisches Reiseinformations- und -genehmigungssystem**, über das noch entschieden werden muss; es soll ein umfassendes automatisiertes System zur Erfassung und Ex-ante-Überprüfung der Daten von der Visumpflicht befreiter Drittstaatsangehöriger werden, die in den Schengen-Raum einreisen (CESE 2016-06889 SOC/556, Berichterstatter: Herr Simons[5]);
- **ECRIS-TCN: Europäisches Informationssystem für Strafregister von Drittstaatsangehörigen**, derzeit von der Kommission vorgeschlagen; ein elektronisches System für den Austausch von Informationen über bereits von den nationalen Gerichten erlassene Entscheidungen.

2.5 Man kann die derzeitigen Mittel einer berechtigten Behörde mit einem Smartphone mit verschiedenen Anwendungen vergleichen, die alle voneinander getrennt sind und jeweils „ihre“ Informationen liefern.

2.6 Abgesehen vom SIS sind diese Systeme auf die **Verwaltung der Drittstaatsangehörigen** ausgerichtet. Es bestehen sechs einander ergänzende und dezentralisierte Systeme. Die Summe der gesuchten Informationen entspricht den verschiedenen Antworten, die die Untersuchungsdienste entsprechend ihren Zugriffsberechtigungen von den einzelnen Datenbanken erhalten haben.

2 ABl. C 34 vom 2.2.2017, S. 144.

3 ABl. C 458 vom 19.12.2014, S. 36.

4 ABl. C 487 vom 28.12.2016, S. 66.

5 ABl. C 246 vom 28.7.2017, S. 28.

2.7 Die Kommission beabsichtigt, folgend Frage zu beantworten:

– Mit welcher Methode können ohne Veränderung der bereits entwickelten Strukturen und unter Beibehaltung ihrer Komplementarität alle Datenbanken aufeinander abgestimmt werden, damit an einer Einreisestelle auf europäischem Gebiet und über eine einzige Abfrage des Systems alle bereits in den bestehenden Datenbanken erfassten Informationen bei der abfrageberechtigten Aufsichtsbehörde zusammenlaufen, wobei die Regelungen über den Datenschutz und die Grundrechte eingehalten werden müssen?

2.8 Mit den vorliegenden Vorschlägen möchte die Europäische Kommission:

2.8.1 zusätzliche Möglichkeiten eines Zugangs zu den Datenbanken von Europol und Interpol schaffen, die bereits mit den europäischen Aufsichtsbehörden zusammenarbeiten;

2.8.2 die Informationsabfragen „synchronisieren“, um die Zeit zur Bearbeitung der Akten von Migranten zu verkürzen und die Sicherheitsreaktion im Notfall zu beschleunigen. Zu diesem Zweck schlägt sie die Schaffung neuer Stellen vor, die eine übereinstimmende Arbeitsweise der derzeitigen Datenbanken ermöglichen würden.

2.9 **Ihre Ziele bestehen darin, die Mängel der verschiedenen Systeme so weit wie möglich zu beheben**, den Schutz der Außengrenzen des Schengen-Raums **zu verbessern**, zur inneren Sicherheit der Union beizutragen, den Identitätsbetrug zu bekämpfen, Fälle von Mehrfachidentitäten zu lösen, verdächtige oder bereits verurteilte Personen ausfindig zu machen und ihre Wege im Schengen-Raum nachzuverfolgen.

2.10 Um noch einmal auf das Bild des Smartphones zurückzukommen: Der berechtigten Behörde stünden nicht nur zahlreiche Anwendungen zur Verfügung, sondern sie könnte auch gleichzeitig und im Rahmen der gleichen Abfrage unter Verwendung ihrer Zugriffscodes die in allen ihren Informationsträgern, PC, Laptop, Telefon, Tablet, Notebook usw. gespeicherten Daten erfassen.

3. Funktionsweise des Systems

3.1 Die Kommission hat Konsultationen durchgeführt und eine hochrangige Expertengruppe für Informationssysteme und Interoperabilität[6] eingesetzt, deren Mitglieder von den Mitgliedstaaten, der Gruppe der Schengen-Länder sowie den europäischen Agenturen wie eu-LISA[7] und FRA[8] ernannt wurden und die von der GD HOME koordiniert wird.

Die Methode: Interkonnektivität oder Interoperabilität?

6 GD HOME, Referat B/3; Beschluss C/2016/3780 der Kommission vom 17 Juni 2016; http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=DEhttp://ec.europa.eu/transparency/regexpert/index.cfm?Lang=DE.

7 eu-LISA: Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts.

8 FRA: Agentur der Europäischen Union für Grundrechte.

3.1.1 **Interkonnektivität** der Informationssysteme ist die Möglichkeit, die Systeme untereinander zu verbinden, damit die Daten des einen automatisch von einem anderen konsultiert werden können.

3.1.2 **Interoperabilität**[9] ist die Fähigkeit der verschiedenen Systeme, zu kommunizieren, Daten auszutauschen und die ausgetauschten Informationen unter Wahrung der Zugriffsberechtigungen zu verwenden.

3.2 Die Entscheidung für Interoperabilität

3.2.1 Die Kommission ist der Ansicht, dass sie den Besitzstand und die derzeitigen Zuständigkeiten nicht grundlegend verändert und dass die Daten „abgeschottet“ bleiben. Dadurch würde trotz der verstärkten Kommunizierbarkeit ein Sicherheitsvorteil für die Systeme und die Daten erreicht, die natürlich nicht über das Internet zugänglich wären. Die zur Stellungnahme vorgelegten Vorschläge weisen starke Ähnlichkeiten auf. Dabei geht es

- zum einen im Dokument COM(2017) 793 um die Interoperabilität zwischen Informationssystemen hinsichtlich Grenzen und Visa
- und zum anderen im Dokument COM(2017) 794 um die polizeiliche und justizielle Zusammenarbeit, Asyl und Migration.

3.3 Die neuen Instrumente

3.3.1 Im Interesse einer interoperablen Funktionsweise muss eine aus vier neuen Instrumenten bestehende Architektur die sechs Grundlagen ergänzen, um schnelles Arbeiten durch eine einzige Systemabfrage sicherzustellen, wobei die Abfragen jedoch immer von den dazu berechtigen Personen durchzuführen sind.

3.4 Nutzung des Europäischen Suchportals (ESP)

3.4.1 Die berechtigte Aufsichtsbehörde (der Endnutzer) sollte über einen einzigen Zugang zum gesamten System verfügen. Statt sechs Abfragen führt sie nur noch eine (Polizei, Zoll usw.) durch, um gleichzeitig mehrere Datenbanken abzufragen, wobei aber keine der abgefragten Daten gespeichert werden. Existieren Daten, findet das System sie. Im Falle des Verdachts auf eine Straftat oder eine terroristische Handlung wird bei der ersten Abfrage nach der kontrollierten Person möglicherweise kein Treffer erzielt („no-hit“); stimmt der Datensatz jedoch mit einer zweiten Auskunft („hit“) überein, die in den Datenbanken wie SIS, EES, ETIAS vorhanden ist, kann dies zu umfassenden Nachforschungen und einer Untersuchung führen.

9 Kommission, COM(2016) 205 final, Mitteilung „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“.

3.5 **Gemeinsamer Dienst für den Abgleich biometrischer Daten (shared BMS)**

3.5.1 Diese gemeinsame Plattform für den Abgleich ermöglicht gleichzeitig die Suche und den Vergleich mathematischer und biometrischer Daten, Fingerabdrücke und Passfotos von unterschiedlichen Datenbanken wie SIS, Eurodac, VIS, EES[10], ECRIS, nicht jedoch ETIAS; ihre Daten müssen kompatibel sein.

3.5.2 Die mathematischen Daten werden nicht in ihrer ursprünglichen Form gespeichert.

3.6 **Gemeinsamer Speicher für Identitätsdaten (CIR)**

3.6.1 Der „gemeinsame Speicher für Identitätsdaten" enthält Daten zur biografischen und biometrischen Identität der kontrollierten Drittstaatsangehörigen, unabhängig davon, ob sie sich an der Grenze oder in den (Schengen-)Mitgliedstaaten befinden. Durch eine Trefferkennzeichnung der Auskünfte in den einzelnen Datenbanken werden die Abfragen beschleunigt. Unter der Verantwortung und mit der Sicherheitsausrüstung der Agentur eu-LISA werden diese Daten so gespeichert, dass niemand Zugriff auf mehr als eine alphanumerische Zeile gleichzeitig hat. Der CIR, der ausgehend von EES und ETIAS entwickelt wurde, dürfte nicht zu einer Duplizierung der Daten führen. Der Speicher kann auch für Abfragen zu zivilen Zwecken genutzt werden.

3.7 **Detektor für Mehrfachidentitäten (MID)**

3.7.1 Seine Aufgabe ist es, durch eine Abfrage in allen Datenbanken gleichzeitig die korrekte Identität von Bona-fide-Reisenden zu überprüfen und Identitätsbetrug zu bekämpfen. Keine Verwaltung hat bisher ein derartiges Instrument verwendet, das es ermöglichen sollte, Identitätsbetrug zu vermeiden.

3.8 **Die Rolle der Agentur eu-LISA**[11]

3.8.1 Die 2011 gegründete Agentur soll die Politik der EU in den Bereichen Justiz, Sicherheit und Freiheit vereinfachen. Die in Tallinn (Estland) ansässige Agentur gewährleistet bereits den Informationsaustausch zwischen den verschiedenen Strafverfolgungsbehörden der Mitgliedstaaten und das unterbrechungsfreie Funktionieren der IT-Großsysteme sowie die Freizügigkeit im Schengen-Raum.

3.8.2 Sie arbeitet an dem Projekt „Smart Borders" und wird in der neuen Architektur für den Datenaustausch die Aufgabe der Speicherung der personenbezogenen Elemente sowie der auf Behörden, Ermittlungen und Ermittler bezogenen Elemente übernehmen. Sie wird die Berechtigungen der Antragsteller prüfen und für die Sicherheit der Daten sorgen, einschließlich im Falle von „Vorfällen" (Art. 44, Vorschläge (2017) 793 und 794).

---

10 Durch die Kursivsetzung wird darauf hingewiesen, dass die Rechtstexte zu diesen Systemen noch nicht angenommen wurden.

11 Verordnung (EU) Nr. 1077/2011, eu-LISA, Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts.

3.8.3 **Die Verwendung des UMF (Universal Message Format)**, das noch zu entwickeln ist, dürfte die Arbeit mit den neuen, obligatorischen Systemen erleichtern, da es die Einrichtung von Schnittstellen zwischen den Mitgliedstaaten, die noch keine besitzen, sowie ein temporäres System für die Übersetzung von einer Sprache in die andere vorschreibt.

3.9 **Schutz der personenbezogenen Daten** (Art. 8 und 7 der Charta):

3.9.1 Im Verordnungsvorschlag wird eingeräumt, dass es zu Sicherheitsunfällen kommen kann. Die Mitgliedstaaten und ihre Datensysteme müssen in erster Instanz Datenschutzgrundsätze einhalten, die in den Rechtsvorschriften, im Vertrag, in der Charta der Grundrechte und in der Datenschutz-Grundverordnung[12], die am 25. Mai 2018 in Kraft treten wird, vorgesehen sind.

4. Diskussion

4.1 Mehrwert der Interoperabilität im Rahmen der Demokratie

4.1.1 Die EU benötigt Regelungen und Untersuchungsmechanismen, die sie vor Kriminalität schützen. Die Interoperabilität der Informationssysteme ist eine Gelegenheit, für Rechtsstaatlichkeit und den Schutz der Menschenrechte zu sorgen.

4.1.2 *EES und ETIAS*, gekoppelt an BMS und CIR, werden es ermöglichen, die Grenzübertritte nicht nur verdächtiger Personen, sondern auch aller europäischen Bürger zu kontrollieren und ihre Daten zu speichern. Jedoch kann die Möglichkeit des Zugangs „von Strafverfolgungsbehörden zu den Informationssystemen anderer Behörden“ der EU (Art. 17/CIR, Vorschläge 2017/794 und 793) nicht mit den Zielen vereinbar sein, die als Grundlagen der vorliegenden Vorschläge genannt werden. Der EWSA (Art. 300 Abs. 4 AEUV) muss hier auf den Grundsatz der Verhältnismäßigkeit hinweisen und fordert die Kommission auf, jede Art von „Big Brother“-System[13] und die Schaffung von Hindernissen für die Freizügigkeit der Europäer zu vermeiden (Art. 3 AEUV).

4.1.3 Das vorgeschlagene Modell für die Sammlung und Verwendung personenbezogener Daten, die an der Grenze und innerhalb des Gebiets der Union bei Personen- und Dokumentenkontrollen erhoben werden, wird als absolut sicheres System dargestellt, das nur für berechtigte Personen und zu Zwecken der Sicherheit und Verwaltung zugänglich ist.

4.1.4 Außerdem wird es dazu beitragen, dass die Verfahren reibungsloser verlaufen. Der EWSA hat Bedenken bezüglich der Sicherheit des Systems: Es bestehen weiterhin Mängel; der auf neun Jahre angelegte Aufbau stützt sich auf „Fundamente“, die noch nicht bestehen, wie die Datenbanken EES und ETIAS oder nationale Schnittstellen. Der technische Kontext entwickelt sich ständig weiter, das Projekt basiert zwangsläufig auf dem aktuellen Stand der Technik, und

---

12 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Stellungnahme des EWSA: ABl. C 229 vom 31.7.2012, S. 90 und ABl. C 345 vom 13.10.2017, S. 138.

13 In „1984“, George Orwell.

im Haushalt ist die Bewältigung der Überalterung nicht berücksichtigt, zu der es in einigen digitalen Bereichen kommen wird.

4.1.5 Zudem hätte bei dem Projekt die rasche Entwicklung des Einsatzes der sogenannten Algorithmen der künstlichen Intelligenz (KI) berücksichtigt werden können, die als ein Kontrollinstrument der Systeme und gleichzeitig als Sicherheitsinstrument dienen könnten, das den Entscheidungsbehörden an die Hand gegeben wird, um die demokratische Verwendung der Struktur zu gewährleisten.

4.1.6 Mit dem Vorschlag wird ein System für vertrauenswürdige Akteure entwickelt, die die Gesetze einhalten. Die Tatsache, dass Menschen das Sagen haben, ist beruhigend, kann jedoch auch eine Schwachstelle darstellen. Der EWSA schlägt die Aufnahme eines Artikels vor, der „Fehlerstromschutzschalter" für den Fall von politischen Krisen und/oder „Management"-Krisen vorsieht, da jedes Problem in einer Datenbank ein Risiko für die gesamte Struktur darstellen könnte.[14] Die allgemeine Verbreitung des UMF könnte zu einer internationalen Verwendung führen, die sehr positiv, für den Datenschutz aber auch sehr riskant wäre. Die zuständigen Behörden werden diesbezüglich eine große Verantwortung tragen. Diese Aspekte werden in den hier untersuchten Texten nicht berücksichtigt.

4.2 **Schutz der Grundrechte**

4.2.1 Die Grundrechte haben absoluten Charakter; Einschränkungen dürfen nur vorgenommen werden, wenn sie erforderlich sind und den von der EU anerkannten, dem Gemeinwohl dienenden Zielsetzungen tatsächlich entsprechen und wenn ihr Wesensgehalt geachtet wird (Art. 52 Abs. 1 Charta). Der EWSA fragt sich, wie die Verhältnismäßigkeit der Kontrollmaßnahmen im Falle von Migranten bewerten werden kann, die vor Verfolgungen fliehen und an den Küsten der Union um Asyl ersuchen [COM(2017) 794, S. 20 – Begründung]. Die Suche nach Verdächtigen, um kriminelle und insbesondere terroristische Handlungen zu verhindern, **darf nicht dazu führen, dass unsere Demokratien einen Straftatbegriff verwenden, der auf Antizipation beruht**; es muss weiterhin zwischen die öffentliche Ordnung gefährdenden „Handlungen" und „Meinungen" unterschieden werden.

4.2.2 Durch die Wahrung der in der Charta verankerten Rechte für alle Personen muss sichergestellt werden, dass ein Gleichgewicht zwischen Sicherheit und Freiheit besteht, ohne dass die Demokratie zugrunde geht. Der EWSA ist der Ansicht, dass dieses Gleichgewicht von grundlegender Bedeutung ist und ein ständiges Ziel aller Behörden einschließlich der Aufsichtsbehörden auf nationaler und europäischer Ebene sein muss.

4.2.3 Die Kette der an der Abfrage beteiligten Behörden und die damit zusammenhängenden Metadaten werden im System gespeichert. Im Fall eines böswilligen Eindringens in die Struktur und eines Missbrauchs der Daten zwischen dem Erfassen und Löschen müssen auch die Grundrechte der berechtigten Behörden selbst im Zusammenhang mit den erzeugten Daten gewahrt werden, insbesondere hinsichtlich ihrer Sicherheit und ihres Privatlebens.

14 CEPD, Anhang, Abschlussbericht der hochrangigen Expertengruppe, Mai 2017.

4.3 **Datenschutz**

4.3.1 Die Vorschläge beruhen auf den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen, auch wenn in der Begründung darauf hingewiesen wird, dass nach Ansicht des Gerichtshofs (EuGH) das Recht auf Schutz der personenbezogenen Daten keine uneingeschränkte Geltung beanspruchen kann. Der EWSA erkennt die Vorteile von Präventivmaßnahmen zur Gewährleistung der Sicherheit, zur Bekämpfung falscher Identitäten und zur Garantie des Asylrechts an. Er möchte jedoch auf die Grenzen der Mathematisierung und Anonymisierung der Daten hinweisen: Die betroffenen Personen benötigen ihre Daten möglicherweise zu einem späteren Zeitpunkt.

4.3.2 Er betont zudem, dass die Art der gespeicherten biometrischen und biologischen Daten für bestimmte Unternehmen und die Verbrechensbekämpfung von besonderem Interesse sein kann. Die Cybersicherheit ist hier genauso wichtig wie die physische Sicherheit; sie findet in den Vorschlägen zu wenig Berücksichtigung. Die erfassten Daten werden an einem einzigen physischen Ort gespeichert, der zwar abgesichert ist, aber dennoch Gefahren ausgesetzt sein kann.

4.3.3 Der EWSA weist darauf hin, dass die Einrichtungen und Organe der Union im Hinblick auf den Datenschutz und das Recht auf Löschung (Recht auf Vergessen) an die Verordnung 45/2001 (EG) gebunden sind, die weniger Schutz bietet als die Datenschutz-Grundverordnung[15] von 2016 (die im Mai 2018 in Kraft tritt), die von den Mitgliedstaaten eingehalten werden muss. Der EWSA hebt die Komplexität der Umsetzung dieses Rechts hervor und befürchtet, dass Reisende, Migranten und Asylbewerber nicht in der Lage sind, für seine Durchsetzung zu sorgen:

1) Der Schutz der personenbezogenen Daten muss für alle bestehenden nationalen und europäischen Datenbanken validiert werden, damit die Gesamtheit der Daten geschützt ist.
2) Der Datenschutz ist äußerst wichtig, damit die Bürger dieses immense Überwachungsnetz akzeptieren, das über ihren Köpfen schwebt.

4.3.4 In den Vorschlägen gibt es keine genauen Angaben darüber, wie lange die von den berechtigten Behörden erfassten Daten gespeichert werden. In den Vorschlägen wird das Verfahren für das Recht auf Berichtigung bzw. Löschung erwähnt, das zwischen dem Staat, in dem der Antrag gestellt wurde, und dem zuständigen Staat stattfindet, es sind jedoch keine Fristen für die Dauer der Datenspeicherung festgelegt (Art. 47 der Vorschläge). Der EWSA spricht sich dafür aus, diese Fristen festzulegen, die für Minderjährige, ausgenommen im Fall von Terrorismus, kürzer sein sollten (Charta, Art. 24), damit diese die Möglichkeit haben, sich zu integrieren.

4.4 **Governance und Rechenschaftspflicht**

4.4.1 Internationale Datenbanken unterliegen nicht den gleichen Regeln wie europäische Informationssysteme. Die Einführung eines einheitlichen Zugriffsformats, das internationale Geltung erhalten könnte, ist lediglich ein technischer Aspekt, durch den die Regelungen nicht

15 Verordnung (EU) 2016/679.

vereinheitlicht werden, auch wenn Interpol zweifellos Artikel 17 des Paktes der Vereinten Nationen[16] einhalten muss. Zudem sind für die Berechtigungen weiterhin die Mitgliedstaaten zuständig. Der EWSA ist der Ansicht, dass dieser Punkt in den Vorschlägen behandelt werden sollte.

4.4.2 Eine einzige Abfrage – und der Verbund der europäischen Datenbanken spricht sein Urteil. Der EWSA unterstreicht, dass die erzeugte Bürokratie hinsichtlich der erreichten Geschwindigkeit mehr als verhältnismäßig ist. Die Steuerung wird von der Kommission im Rahmen eines Kontrollverfahrens mit den Mitgliedstaaten sichergestellt. Dreh- und Angelpunkt wird die Agentur eu-LISA sein, die insbesondere damit beauftragt ist, die Verfahren für die Sammlung von Informationen über das Funktionieren der Interoperabilität einzurichten; sie wird die Informationen von den Mitgliedstaaten und Europol erhalten und dem Rat, dem EP und der Kommission alle vier Jahre einen Bericht über die technische Bewertung vorlegen; die Kommission wird ein Jahr später einen allgemeinen Bericht ausarbeiten (Art. 68 der Vorschläge). Nach Ansicht des EWSA sind diese Zeiträume viel zu lang. Die Bewertung der Sicherheit der Interoperabilitätskomponenten (Art. 68 Abs. 5 Buchstabe d) sollte mindestens jedes Jahr stattfinden, und die Bewertung der Auswirkungen auf die Grundrechte mindestens alle zwei Jahre (ebenda Buchstabe b).

4.4.3 Der EWSA bedauert, dass für die grundlegenden Fragen, die in den Vorschlägen behandelt werden, europäische Agenturen zuständig sind, deren Einstellungsverfahren und Arbeitsweise vielen Bürgern nicht bekannt sind. Er hält es für wichtig, bewährte Methoden auszutauschen und alle unabhängigen Behörden, die für die Kontrolle der Verwendung von Daten zuständig sind (DSB), sowie andere Agenturen wie FRA und ENISA zur Stellungnahme einzubinden.

4.4.4 Die Einrichtung all dieser neuen Strukturen und Verfahren geschieht über delegierte Rechtsakte und Durchführungsrechtsakte der Kommission. Der EWSA spricht sich dafür aus, dass das Ziel der Wahrung der Grundrechte und des Schutzes personenbezogener Daten im Rahmen des Ansatzes einer verbesserten Aufnahme der Personen an den Grenzen in allen diesen Rechtsakten verankert bleibt. Er empfiehlt, die europäischen Bürger bis zum Abschluss des Projekts über die jeweiligen Etappen zu informieren und die betroffenen Personen über die Kontrollen, denen sie unterzogen werden, aufzuklären.

5. Notwendige Schulungen der Aufsichtsbehörden in der gesamten Union

5.1 Im Gegensatz zu den Vorstellungen, die die Kommission in ihrer Zusammenfassung der Folgenabschätzung (C) äußert, hält es der EWSA für wichtig, im ersten Zeitraum (nach 2021) eine Vielzahl von Schulungen durchzuführen. Die Kommission nennt diesbezüglich einen Betrag von 76 Millionen EUR jährlich. Der Übergang zu neuen Verfahren erfordert immer eine Weiterqualifizierung. Es geht hier um alle Grenzen der EU und um nationale Systeme. Einige Mitgliedstaaten besitzen noch keine kompatiblen Systeme und müssen große Anstrengungen unternehmen und Schnittstellen einrichten, damit sie teilnehmen können. Im Hinblick auf eine

16 Internationaler Pakt über bürgerliche und politische Rechte – VN – Artikel 17 Absatz 1. „Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. 2. Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen."

funktionierende Interoperabilität müssen die Unterschiede zwischen den Mitgliedstaaten aus dem Weg geräumt werden.

5.2 Schulungen zur Nutzung hochwertiger Daten und des UMF sind wesentlich. Der EWSA schlägt vor, dass mit CEPOL[17], Frontex, Europol usw. gemeinsame Schulungen für die berechtigten Behörden organisiert werden, auch für die Mitglieder von eu-LISA, deren Kenntnisse genau überprüft werden sollten.

5.3 Ein Instrument wie der MID besteht an keinem anderen Ort. Im Falle eines Erfolgs würde das Instrument große Schlagkraft haben. Für die neue Struktur ist höchste Datenqualität erforderlich. Damit das gesamte System den Erwartungen des Projekts gerecht wird, müssen alle Mitgliedstaaten auf dem gleichen Niveau teilnehmen, anderenfalls wird es noch schwerwiegendere Mängel als zuvor geben. In diesem Fall wären das Recht auf Asyl und das Recht auf Zugang zu internationalem Schutz gefährdet (Art. 18 und 19 der Charta).

6. **Finanzierung**

6.1 Die gesamte vorgeschlagene Struktur beruht auf einer Reihe von Hypothesen: die Annahme der Systeme *EES, ETIAS, UMF* durch die Entscheidungsbehörden, das reibungslose Funktionieren des *MID* und die Absicherung des *CIR*. Werden beide Stellen, der EDSB und die Agentur eu-LISA, sowie vielleicht auch die Agentur ENISA über ausreichende personelle und finanzielle Mittel verfügen? Die Kommission schlägt eine Kofinanzierung der EU und der Mitgliedstaaten vor. Der EWSA stellt fest, dass die Verwaltung des „Semesters“ weiterhin mit Sparhaushalten finanziert wird und die derzeitige Verwendung der bestehenden Datenbanken (SIS, VIS, Prüm, *EES*) im Hinblick auf die Erfüllung der rechtlichen Anforderungen noch optimiert werden muss (Bericht der Expertengruppe).

6.2 Der EWSA fragt sich, welche Haushaltsfolgen der Brexit haben wird, obwohl das Vereinigte Königreich nicht dem Schengen-System angehört, und ganz allgemein, wie komplex es in Zukunft sein wird, die Interoperabilität in den Ländern zu steuern, die nicht dem SIS angehören, sondern an anderen Datenbanken wie beispielsweise dem Eurodac beteiligt sind.

17 CEPOL, Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (Budapest, Ungar).

6.3 Als Fonds ist der ISF (Fonds für die innere Sicherheit – Grenzen) vorgesehen. Die Inbetriebnahme ist für 2023 geplant. Der EWSA fragt sich, ob fünf Jahre ausreichen werden, um die Unterschiede in Europa abzubauen und die Bedingungen für einen Erfolg zu schaffen. Der vorgesehene Haushalt beläuft sich auf 424,7 Millionen EUR über neun Jahre (2019-2027), die von der Union (ISF) und den Mitgliedstaaten gezahlt werden müssen. Die Mitgliedstaaten müssen die Voraussetzungen schaffen, damit die derzeitigen Systeme mit der neuen IT-Architektur ordnungsgemäß funktionieren. Der EWSA ist der Ansicht, dass die Wiederbelebung des Wachstums dazu genutzt werden sollte, diese Investitionen zu tätigen.

Brüssel, den 23. Mai 2018

Luca JAHIER
Präsident des Europäischen Wirtschafts- und Sozialausschusses