

## **Zusammenfassung der Stellungnahme des Europäischen Datenschutzbeauftragten zu den Vorschlägen für zwei Verordnungen über die Einrichtung eines Rahmens für die Interoperabilität von IT-Großsystemen der EU**

*(Der vollständige Text dieser Stellungnahme ist in deutscher, englischer und französischer Sprache auf der Internetpräsenz des EDSB unter [www.edps.europa.eu](http://www.edps.europa.eu) erhältlich)*

(2018/C 233/07)

Die aktuellen drängenden Herausforderungen in den Bereichen Sicherheit und Grenzmanagement erfordern eine intelligenter Nutzung der den zuständigen Behörden bereits vorliegenden Informationen. Dies war Anlass für die Europäische Kommission, einen Prozess in Richtung Interoperabilität der (bestehenden und künftigen) IT-Großsysteme der EU in den Bereichen Migration, Asyl und Sicherheit in die Wege zu leiten. Im Dezember 2017 legte die Kommission zwei Vorschläge für Verordnungen über die Einrichtung eines Rechtsrahmens für Interoperabilität zwischen IT-Großsystemen der EU vor.

Unter der Voraussetzung, dass Interoperabilität durchdacht und unter umfassender Wahrung der Grundrechte einschließlich des Rechts auf Privatsphäre und Datenschutz umgesetzt wird, kann sie ein nützliches Instrument sein, um auf legitime Bedürfnisse zuständiger Behörden einzugehen, die IT-Großsysteme nutzen, und um zum Aufbau eines wirksamen und effizienten Informationsaustauschs beizutragen. Die Entscheidung für Interoperabilität ist nicht nur oder nicht vorrangig eine technische, sondern vielmehr eine politische Entscheidung, die geeignet ist, weitreichende rechtliche und gesellschaftliche Konsequenzen zu haben, die nicht hinter angeblich technischen Veränderungen verborgen werden können. Die Entscheidung des EU-Gesetzgebers, Interoperabilität zwischen IT-Großsystemen herzustellen, würde sich nicht nur auf Dauer und in erheblichem Umfang auf deren Struktur und Funktionsweise auswirken, sondern würde auch die Art und Weise verändern, in der bisher Rechtsgrundsätze in diesem Bereich ausgelegt wurden, und würde insofern einen „Punkt ohne Wiederkehr“ darstellen.

Interoperabilität mag zwar anfänglich als Instrument gedacht gewesen sein, mit dem sich die Nutzung der Systeme erleichtern lässt, doch würden die Vorschläge neue Möglichkeiten für den Zugriff auf in den verschiedenen Systemen gespeicherte Daten und deren Verwendung zur Bekämpfung von Identitätsbetrug, zur Erleichterung von Identitätskontrollen und zur Straffung des Zugriffs von Strafverfolgungsbehörden auf Informationssysteme eröffnen, die nicht im Bereich Strafverfolgung angesiedelt sind.

Die Vorschläge sehen insbesondere den Aufbau einer neuen zentralen Datenbank vor, in der Informationen über Millionen von Drittstaatsangehörigen einschließlich ihrer biometrischen Daten gespeichert würden. Aufgrund der Größe dieser Datenbank und der Art der darin gespeicherten Daten könnte jeder Verstoß gegen die Datenschutzvorschriften einer potenziell sehr großen Zahl natürlicher Personen schweren Schaden zufügen. Sollten solche Informationen in die falschen Hände geraten, könnte die Datenbank ein gefährliches, gegen die Grundrechte gerichtetes Instrument werden. Es ist daher unbedingt erforderlich, starke rechtliche, technische und organisatorische Garantien vorzusehen. Besondere Wachsamkeit ist auch bezüglich der Zweckbestimmungen der Datenbank sowie der Bedingungen und Modalitäten für ihre Nutzung geboten.

In diesem Zusammenhang unterstreicht der EDSB die Bedeutung einer weiteren Klärung des Umfangs des Problems des Identitätsbetrugs unter Drittstaatsangehörigen, damit sichergestellt ist, dass die vorgeschlagene Maßnahme angemessen und verhältnismäßig ist. Für die Möglichkeit der Abfrage der zentralen Datenbank zwecks Erleichterung von Identitätskontrollen im Hoheitsgebiet der Mitgliedstaaten sollten strengere Vorgaben formuliert werden.

Der EDSB hat Verständnis dafür, dass es für Gefahrenabwehr- und Strafverfolgungsbehörden wichtig ist, über die bestmöglichen Instrumente für eine rasche Identifizierung von Terroristen oder anderen Schwerverkriminellen zu verfügen. Aus der Grundrechtsperspektive ist jedoch die Erleichterung des Zugriffs für Strafverfolgungsbehörden auf nicht bei der Strafverfolgung angesiedelte Systeme (also auf Informationen, die von Behörden zu anderen Zwecken als der Strafverfolgung erhoben wurden) alles andere als unerheblich. Ein routinemäßiger Zugriff wäre ein schwerwiegender Verstoß gegen den Grundsatz der Zweckbindung. Der EDSB fordert daher die Beibehaltung echter Garantien, damit die Grundrechte von Drittstaatsangehörigen gewahrt werden.

Schließlich möchte der EDSB noch unterstreichen, dass sowohl in rechtlicher als auch in technischer Hinsicht die Vorschläge die bestehenden sowie die noch in Vorbereitung befindlichen Systeme noch komplexer machen und dies Implikationen mit sich bringt, die heute nur schwer abschätzbar sind. Diese Komplexität wird Auswirkungen nicht nur auf den Datenschutz, sondern auch auf die Governance und Kontrolle der Systeme haben. Sehr schwer zu beurteilen ist derzeit auch, welche genauen Folgen sich für die Rechte und Freiheiten ergeben, die den Kern des EU-Projekts ausmachen. Aus diesen Gründen fordert der EDSB eine umfassende Debatte über die Zukunft der Systeme für den Informationsaustausch in der EU, ihre Governance und die Möglichkeiten, in diesem Zusammenhang Grundrechte zu schützen.

## 1. EINLEITUNG

### 1.1. Hintergrund

1. Im April 2016 verabschiedete die Kommission eine Mitteilung *Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit* <sup>(1)</sup>, die eine Diskussion darüber in Gang setzte, wie Informationssysteme in der Europäischen Union für ein besseres Grenzmanagement und mehr innere Sicherheit sorgen könnten.
2. Im Nachgang zur Mitteilung setzte die Kommission im Juni 2016 eine hochrangige Sachverständigengruppe „Informationssysteme und Interoperabilität“ („HLEG“) ein. Die HLEG sollte sich mit den rechtlichen, technischen und operativen Aspekten der Herstellung der Interoperabilität zentraler EU-Systeme für Grenzen und Sicherheit befassen <sup>(2)</sup>.
3. Die HLEG legte Empfehlungen zunächst in ihrem Zwischenbericht vom Dezember 2016 <sup>(3)</sup> und später in ihrem Abschlussbericht vom Mai 2017 <sup>(4)</sup> vor. Der EDSB war zur Teilnahme an den Arbeiten der HLEG eingeladen und gab eine Erklärung zum Konzept der Interoperabilität im Bereich Migration, Asyl und Sicherheit ab, die in den Abschlussbericht der HLEG aufgenommen wurde.
4. Aufbauend auf der Mitteilung von 2016 und den Empfehlungen der HLEG schlug die Kommission einen neuen Ansatz vor, dem zufolge alle zentralisierten IT-Systeme der EU für Sicherheit, Grenzmanagement und Migrationssteuerung interoperabel werden sollen <sup>(5)</sup>. Die Kommission verkündete ihre Absicht, auf die Einrichtung eines europäischen Suchportals, eines gemeinsamen biometrischen Dienstes und eines gemeinsamen Speichers für Identitätsdaten hinzuwirken.
5. Am 8. Juni 2017 begrüßte der Rat die Haltung der Kommission und ihren Vorschlag für das weitere Vorgehen für das Erreichen der Interoperabilität von Informationssystemen bis 2020 <sup>(6)</sup>. Am 27. Juli 2017 leitete die Kommission eine öffentliche Konsultation zur Interoperabilität der EU-Informationssysteme im Bereich Grenzen und Sicherheit ein <sup>(7)</sup>. Als Begleitdokument zur Konsultation lag eine erste Folgenabschätzung vor.
6. Am 17. November 2017 legte der EDSB als weiteren Beitrag ein Reflexionspapier zur Interoperabilität von Informationssystemen im Raum der Freiheit, der Sicherheit und des Rechts vor <sup>(8)</sup>. In diesem Papier räumte er ein, dass Interoperabilität, sofern sie sorgfältig durchdacht und im Einklang mit den grundlegenden Erfordernissen der Notwendigkeit und Verhältnismäßigkeit umgesetzt wird, ein hilfreiches Instrument zur Deckung bestimmter Erfordernisse zuständiger Behörden sein kann, die IT-Großsysteme nutzen, und unter anderem die Informationsweitergabe verbessern kann.
7. Am 12. Dezember 2017 stellte die Kommission zwei Legislativvorschläge vor („die Vorschläge“), und zwar 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 des Beschlusses 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, im Folgenden „Vorschlag zu Grenzen und Visa“.
  - 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), im Folgenden „Vorschlag polizeiliche und justizielle Zusammenarbeit, Asyl und Migration“.

<sup>(1)</sup> Mitteilung der Kommission an das Europäische Parlament und den Rat „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“, 6. April 2016, COM(2016) 205 final.

<sup>(2)</sup> A. a. O., S. 17.

<sup>(3)</sup> Zwischenbericht des Vorsitzes der von der Europäischen Kommission eingesetzten hochrangigen Sachverständigengruppe „Informationssysteme und Interoperabilität“, Zwischenbericht des Vorsitzes der hochrangigen Sachverständigengruppe, Dezember 2016, abrufbar unter: <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435>

<sup>(4)</sup> Abschlussbericht der von der Europäischen Kommission eingesetzten hochrangigen Sachverständigengruppe „Informationssysteme und Interoperabilität“, 11. Mai 2017, abrufbar unter: <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435>.

<sup>(5)</sup> Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat und den Rat „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion — Siebter Fortschrittsbericht“, 16. Mai 2017, COM(2017) 261 final.

<sup>(6)</sup> Schlussfolgerungen des Rates zum weiteren Vorgehen zur Verbesserung der Informationsaustauschs und zur Sicherstellung der Interoperabilität der EU-Informationssysteme, 8. Juni 2017: <http://data.consilium.europa.eu/doc/document/ST-10151-2017-INIT/de/pdf>.

<sup>(7)</sup> Öffentliche Konsultation und Folgenabschätzung sind abrufbar unter: [https://ec.europa.eu/home-affairs/content/consultation-interoperability-eu-information-systems-borders-and-security\\_en](https://ec.europa.eu/home-affairs/content/consultation-interoperability-eu-information-systems-borders-and-security_en).

<sup>(8)</sup> [https://edps.europa.eu/sites/edp/files/publication/17-11-16\\_opinion\\_interoperability\\_de.pdf](https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_de.pdf).

## 1.2. Ziele der Vorschläge

8. Allgemeines Ziel der Vorschläge ist es, das Grenzmanagement an den Schengen-Außengrenzen zu verbessern und einen Beitrag zur inneren Sicherheit der Europäischen Union zu leisten. Zu diesem Zweck errichten sie einen Rahmen für die Sicherstellung der Interoperabilität zwischen bestehenden und künftigen IT-Großsystemen der EU in den Bereichen Grenzkontrollen, Asyl und Einwanderung, polizeiliche Zusammenarbeit und justizielle Zusammenarbeit in Strafsachen.
9. Zu den Interoperabilitätskomponenten, die von den Vorschlägen abgedeckt werden, gehören:
  - drei bestehende Systeme: das Schengen-Informationssystem (SIS), das Eurodac-System und das Visa-Informationssystem (VIS);
  - drei vorgeschlagene Systeme, die noch in Vorbereitung oder Entwicklung sind:
    - eines, über das die EU-Gesetzgeber kürzlich Einigung erzielt haben und das noch weiterentwickelt werden muss, nämlich das Einreise-/Ausreise-System (EES) <sup>(1)</sup>, und
    - zwei, über die noch verhandelt wird, nämlich das vorgeschlagene Europäische Reiseinformations- und -genehmigungssystem (ETIAS) <sup>(2)</sup> und das vorgeschlagene Europäische Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN) <sup>(3)</sup>;
  - die Interpol-Datenbank für gestohlene und verlorene Reisedokumente (SLTD) und
  - Europol-Daten <sup>(4)</sup>.
10. Die Interoperabilität zwischen diesen Systemen wird durch vier Komponenten bewirkt:
  - ein Europäisches Suchportal (European search portal — „ESP“),
  - einen gemeinsamen Dienst für den Abgleich biometrischer Daten (biometric matching service — „gemeinsamer BMS“),
  - einen gemeinsamen Speicher für Identitätsdaten (common identity repository — „CIR“) und
  - einen Detektor für Mehrfachidentitäten (multiple-identity detector — „MID“).
11. Das ESP würde als Schnittstelle fungieren. Es soll eine einfache Schnittstelle bieten, die auf transparente Weise bei Abfragen schnelle Ergebnisse erbringt. Es würde die gleichzeitige Abfrage der verschiedenen Systeme unter Verwendung von Identitätsdaten (sowohl biografischer als auch biometrischer Art) ermöglichen. Oder anders ausgedrückt: Der Endnutzer wäre in der Lage, eine Abfrage vorzunehmen und aus allen Systemen, für die er zugangsberechtigt ist, Ergebnisse zu erhalten und müsste nicht mehr jedes System einzeln abfragen.
12. Ein gemeinsamer BMS wäre ein technisches Instrument, das die Identifizierung einer natürlichen Person erleichtert, die möglicherweise in mehreren Datenbanken erfasst wurde. Er würde Templates der biometrischen Daten (Fingerabdrücke und Gesichtsbilder) speichern, die in den zentralen EU-Informationssystemen (also dem SIS, dem Eurodac-System, dem EES, dem VIS und dem ECRIS-TCN) enthalten sind. Mit seiner Hilfe könnten gleichzeitig einerseits in den verschiedenen Systemen gespeicherte biometrische Daten abgefragt und andererseits diese Daten abgeglichen werden.
13. Der CIR würde die Identifizierung von Personen auch im Hoheitsgebiet der Mitgliedstaaten erleichtern und ferner dazu beitragen, den Zugang der Strafverfolgungsbehörden zu Informationssystemen anderer Behörden einheitlich zu regeln. Im CIR würden biografische und biometrische Daten gespeichert, die im VIS, im ECRIS-TCN, im EES, im Eurodac-System und im ETIAS erfasst wurden. Die Daten würde dort — logisch voneinander getrennt — entsprechend dem System, aus dem die Daten generiert wurden, gespeichert.

<sup>(1)</sup> Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisensystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011 (ABl. L 327 vom 9.12.2017, S. 20).

<sup>(2)</sup> Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/794 und (EU) 2016/1624, COM(2016) 731 final, 16. November 2016.

<sup>(3)</sup> Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (TCN) vorliegen, sowie zur Ergänzung und Unterstützung des Europäischen Strafregisterinformationssystems (ECRIS) und zur Änderung der Verordnung (EU) Nr. 1077/2011 (ECRIS-TCN), COM(2017) 344 final, 29. Juni 2017.

<sup>(4)</sup> Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI (ABl. L 135 vom 24.5.2016, S. 53).

14. Der MID wäre ein Instrument, mit dem sich Identitäten innerhalb des CIR und des SIS miteinander verknüpfen ließen, und würde Verknüpfungen zwischen Datensätzen speichern. Er würde Verknüpfungen mit Informationen dazu speichern, wo ein oder mehrere eindeutige oder mögliche Treffer ermittelt werden und/oder wo eine Identität betrügerisch verwendet wird. Er würde zur Aufdeckung von Mehrfachidentitäten überprüfen, ob abgefragte oder eingegebene Daten in mehr als einem der Systeme vorhanden sind (z. B. die gleichen biometrischen Daten in Verbindung mit unterschiedlichen biografischen Daten oder gleiche/ähnliche biografische Daten in Verbindung mit unterschiedlichen biometrischen Daten). Der MID würde biografische Identitätsdatensätze anzeigen, die in den verschiedenen Systemen verknüpft sind.
15. Mit Hilfe der vier Interoperabilitätskomponenten sollen die Vorschläge
  - befugten Nutzern einen raschen, unterbrechungsfreien, systematischen und kontrollierten Zugang zu relevanten Informationssystemen verschaffen;
  - Identitätsprüfungen von Drittstaatsangehörigen im Hoheitsgebiet von Mitgliedstaaten vereinfachen;
  - mit dem gleichen Datensatz verknüpfte Mehrfachidentitäten aufdecken und
  - den Zugang von Strafverfolgungsbehörden zu Informationssystemen anderer Behörden einheitlich regeln.
16. Darüber hinaus sollen mit den Vorschlägen ein zentraler Speicher für Berichte und Statistiken (Central Repository for Reporting and Statistics — „CRRS“) und das universelle Nachrichtenformat (Universal Message Format — „UMF“) eingerichtet und Mechanismen für die automatische Datenqualitätskontrolle eingeführt werden.
17. Die Veröffentlichung von zwei Legislativvorschlägen anstatt eines Vorschlags ist auf die Notwendigkeit zurückzuführen, zwischen Systemen zu unterscheiden, die Folgendes betreffen:
  - den Schengen-Besitzstand im Bereich Grenzen und Visa (also das VIS, das EES, das ETIAS und das SIS in seiner in der Verordnung (EG) Nr. 1987/2006 geregelten Form),
  - den Schengen-Besitzstand im Bereich der polizeilichen Zusammenarbeit oder Systeme, die nichts mit dem Schengen-Besitzstand zu tun haben (das Eurodac-System, das ECRIS-TCN und das SIS in seiner im Beschluss 2007/533/JI des Rates geregelten Form).
18. Die beiden Vorschläge sind „Parallelvorschläge“, die zusammen gelesen werden müssen. Die Nummerierung der Artikel ist in beiden Vorschlägen inhaltlich im Wesentlichen ähnlich. Sofern nicht anders angegeben, beziehen wir uns daher bei der Nennung eines bestimmten Artikels auf einen Artikel in einem der beiden Vorschläge.

## 5. SCHLUSSFOLGERUNGEN

142. Der EDSB räumt ein, dass Interoperabilität, sofern sie sorgfältig durchdacht und im Einklang mit den grundlegenden Erfordernissen der Notwendigkeit und Verhältnismäßigkeit umgesetzt wird, ein hilfreiches Instrument zur Deckung bestimmter Erfordernisse zuständiger Behörden sein kann, die IT-Großsysteme nutzen, und unter anderem die Informationsweitergabe verbessern kann.
143. Er unterstreicht, dass die Entscheidung für Interoperabilität nicht vorrangig eine technische, sondern an erster Stelle eine politische Entscheidung ist, die in den kommenden Jahren weitreichende rechtliche und gesellschaftliche Konsequenzen haben kann. Vor dem Hintergrund der sich klar abzeichnenden Tendenz, verschiedene Ziele des EU-Rechts und der EU-Politik miteinander zu vermengen (also Grenzkontrollen, Asyl und Einwanderung, polizeiliche Zusammenarbeit und nun auch justizielle Zusammenarbeit in Strafsachen) sowie der Gewährung des routinemäßigen Zugriffs von Strafverfolgungsbehörden auf Datenbanken anderer Behörden würde die Entscheidung des EU-Gesetzgebers, IT-Großsysteme interoperabel zu machen, nicht nur deren Struktur und Funktionsweise auf Dauer und weitreichend berühren, sondern auch die bisherige Auslegung der Rechtsgrundsätze in diesem Bereich verändern und somit unumkehrbar sein. Aus diesen Gründen fordert der EDSB eine umfassende Debatte über die Zukunft der Systeme für den Informationsaustausch in der EU, ihre Governance und die Möglichkeiten, in diesem Zusammenhang Grundrechte zu schützen.
144. Auch wenn die Vorschläge in der vorliegenden Form den Eindruck vermitteln könnten, Interoperabilität sei der letzte Baustein bereits voll funktionsfähiger Informationssysteme (oder zumindest von Systemen, deren Rechtsgrundlage bereits „stabil“ ist und sich in den letzten Phasen des Gesetzgebungsverfahrens befindet), möchte der EDSB daran erinnern, dass dies nicht der Fall ist. Die Realität sieht so aus, dass von den sechs EU-Informationssystemen, die mit den Vorschlägen miteinander verbunden werden sollen, drei derzeit noch gar nicht bestehen (ETIAS, ECRIS-TCN und EES), zwei momentan überarbeitet werden (SIS und Eurodac) und eines noch im Laufe dieses Jahres überarbeitet werden soll (VIS). Eine Beurteilung der genauen Auswirkungen eines solchen Systems mit so vielen „beweglichen Teilen“ auf Privatsphäre und Datenschutz ist praktisch unmöglich. Der EDSB erinnert an die Bedeutung der Kohärenz zwischen den bereits in der Verhandlung befindlichen (oder anstehenden) Rechtstexten und den Vorschlägen, damit es ein einheitliches rechtliches, organisatorisches und technisches Umfeld für alle Datenverarbeitungsaktivitäten innerhalb der Union gibt. In diesem Zusammenhang weist er nachdrücklich darauf hin, dass diese Stellungnahme unbeschadet weiterer Wortmeldungen seinerseits abgegeben wird, zu denen es bei der Behandlung der verschiedenen miteinander verknüpften Rechtsakte im weiteren Gesetzgebungsverfahren kommen kann.

145. Der EDSB stellt fest, dass Interoperabilität zwar anfänglich als Instrument gedacht gewesen sein mag, mit dem sich die Nutzung der Systeme erleichtern lässt, doch eröffnen die Vorschläge neue Möglichkeiten für den Zugriff auf in den verschiedenen Systemen gespeicherte Daten und deren Verwendung zur Bekämpfung von Identitätsbetrug, zur Erleichterung von Identitätskontrollen und zur Straffung des Zugriffs von Strafverfolgungsbehörden auf Informationssysteme, die nicht im Bereich Strafverfolgung angesiedelt sind.
146. Wie schon in seinem Reflexionspapier betont der EDSB die Bedeutung einer weiteren Klärung des Umfangs des Problems des Identitätsbetrugs unter Drittstaatsangehörigen, damit sichergestellt ist, dass die vorgeschlagene Maßnahme angemessen und verhältnismäßig ist.
147. Im Hinblick auf die Verwendung der in den verschiedenen Systemen gespeicherten Daten zur Erleichterung von Identitätskontrollen im Hoheitsgebiet der Mitgliedstaaten weist der EDSB darauf hin, dass die Zwecke einer solchen Verwendung, also die Bekämpfung irregulärer Migration und das Beitragen zu einem hohen Maß an Sicherheit, zu breit gefasst sind und in den Vorschlägen „strikt beschränkt“ und „genau abgegrenzt“ werden sollten, um im Einklang mit der Rechtsprechung des Gerichtshofs der Europäischen Union zu stehen. Nach seiner Auffassung sollte der Zugang zum CIR zur Feststellung der Identität eines Drittstaatsangehörigen zum Zweck der Gewährleistung eines hohen Maßes an Sicherheit nur dann erlaubt sein, wenn für die gleichen Zwecke und unter gleichen Bedingungen ein Zugang auch zu ähnlichen nationalen Datenbanken (z. B. Register von Staatsangehörigen/wohnhaften Personen usw.) besteht. Er empfiehlt, dies in den Vorschlägen klar zum Ausdruck zu bringen. Andernfalls würde durch die Vorschläge die Vermutung im Raum stehen, dass Drittstaatsangehörige *per definitionem* eine Bedrohung der Sicherheit darstellen. Er empfiehlt weiter, dafür zu sorgen, dass der Zugang zu Daten zum Zweck der Identifizierung einer Person während einer Identitätskontrolle in folgenden Fällen zulässig ist:
- grundsätzlich, in Anwesenheit der Person, und
  - wenn die Person zur Kooperation nicht in der Lage ist und kein Dokument vorlegen kann, aus dem ihre Identität hervorgeht, oder
  - wenn sie die Kooperation verweigert, oder
- wenn der berechtigte und begründete Verdacht besteht, dass vorgelegte Dokumente falsch sind oder dass die Person über ihre Identität nicht die Wahrheit sagt.
148. Der EDSB hat Verständnis dafür, dass es für Gefahrenabwehr- und Strafverfolgungsbehörden notwendig ist, über die bestmöglichen Instrumente für eine rasche Identifizierung von Terroristen oder anderen Schwermisdätern zu verfügen. Es wäre allerdings nicht hinnehmbar, wenn echte Garantien, die zur Wahrung von Grundrechten eingeführt wurden, hauptsächlich im Interesse der Beschleunigung eines Verfahrens aufgehoben würden. Er empfiehlt daher, in Artikel 22 Absatz 1 der Vorschläge noch die Bedingungen „Vorliegen berechtigter Gründe“, „vorherige Durchführung einer Suche in nationalen Datenbanken“ und „Einleitung einer Abfrage des automatisierten Fingerabdruck-Identifizierungssystems der anderen Mitgliedstaaten gemäß dem Beschluss 2008/615/JI“ vor einer Abfrage im gemeinsamen Speicher für Identitätsdaten aufzunehmen. Darüber hinaus ist er der Ansicht, dass die Einhaltung der Bedingungen für den Zugang selbst zu beschränkten Informationen wie „Treffer/kein Treffer“ stets überprüft werden sollte, und dies unabhängig davon, ob weitere Zugang zu den in dem System gespeicherten Daten besteht, das den Treffer ausgelöst hat.
149. Nach Auffassung des EDSB sollten die Notwendigkeit und Verhältnismäßigkeit der Verwendung von im ECRIS-TCN gespeicherten Daten zur Aufdeckung von Mehrfachidentitäten und zur Erleichterung von Identitätskontrollen klarer dargelegt werden und sollte ihre Vereinbarkeit mit dem Grundsatz der Zweckbindung klargestellt werden. Er empfiehlt daher, in den Vorschlägen Sorge dafür zu tragen, dass die im ECRIS-TCN gespeicherten Daten ausschließlich für die Zwecke des ECRIS-TCN abgerufen und verwendet werden dürfen, wie sie in dessen Rechtsakt festgelegt sind.
150. Der EDSB begrüßt, dass mit den Vorschlägen ein harmonisiertes technisches Umfeld von Systemen geschaffen werden soll, die zusammenarbeiten werden und einen raschen, unterbrechungsfreien, kontrollierten und systematischen Zugang zu den Informationen bieten, die verschiedene Stakeholder benötigen, um ihre Aufgaben wahrzunehmen. Er erinnert daran, dass die Grundsätze des Datenschutzes in allen Phasen der Implementierung der Vorschläge zu berücksichtigen sind und empfiehlt daher, in die Vorschläge die Verpflichtung für eu-LISA und die Mitgliedstaaten aufzunehmen, sich an die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu halten.
151. Über die allgemeinen Anmerkungen und vorstehend identifizierten Hauptprobleme hinaus formuliert der EDSB weitere Empfehlungen bezüglich folgender Aspekte der Vorschläge:
- Funktionalität des ESP, des gemeinsamen BMS, des CIR und des MID,
  - Fristen für die Speicherung der Daten im CIR und im MID,
  - manuelle Verifizierung von Verknüpfungen,
  - zentraler Speicher für Berichte und Statistiken,

- Verteilung von Rollen und Verantwortlichkeiten auf eu-LISA und die Mitgliedstaaten,
- Sicherheit der Interoperabilitätskomponenten,
- Rechte der betroffenen Personen,
- Zugang durch Bedienstete von eu-LISA,
- Übergangszeitraum,
- Protokolle und
- Rolle der nationalen Aufsichtsbehörden und des EDSB.

152. Der EDSB steht gerne für weitere Beratung zu den Vorschlägen zur Verfügung, auch im Hinblick auf gemäß den vorgeschlagenen Verordnungen angenommene delegierte Rechtsakte oder Durchführungsrechtsakte, die Auswirkungen auf die Verarbeitung personenbezogener Daten haben könnten.

Brüssel, den 19. März 2018

Giovanni BUTTARELLI  
*Europäischer Datenschutzbeauftragter*

---