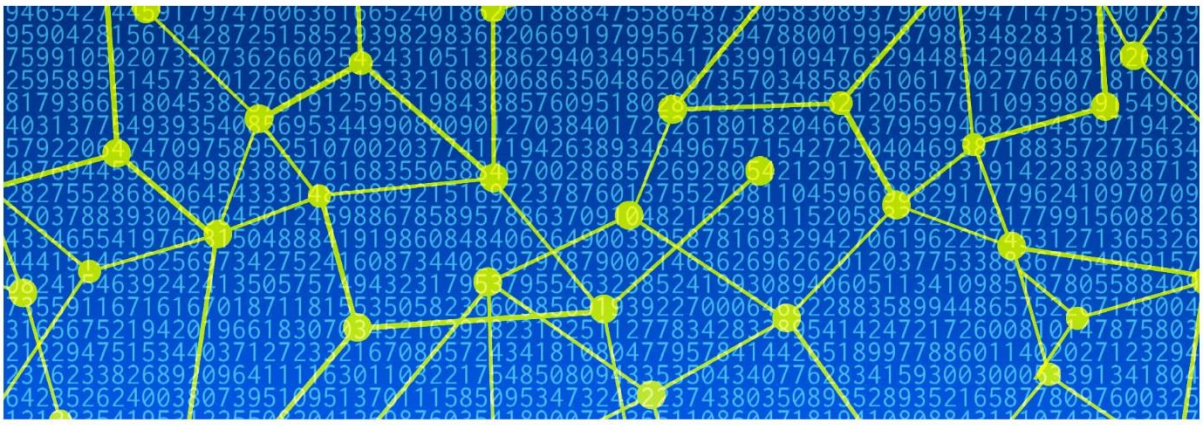

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 4/2018 zu den Vorschlägen für zwei Verordnungen über die Einrichtung eines Rahmens für die Interoperabilität von IT-Großsystemen der EU

EDPS

16. April 2018

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 „im Hinblick auf die Verarbeitung personenbezogener Daten (...) sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden"; er ist „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten" zuständig. Gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 ist die Kommission zur Konsultation des EDSB verpflichtet, „wenn [sie] einen Vorschlag für Rechtsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten annimmt".

Er wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und spezifisch mit einem konstruktiven und proaktiven Vorgehen beauftragt. In seiner im März 2015 veröffentlichten Fünf-Jahres-Strategie legt der EDSB dar, wie er diesen Auftrag auf verantwortungsvolle Weise zu erfüllen gedenkt.

In dieser Stellungnahme geht es um den Auftrag des EDSB, die EU-Organe bezüglich der Datenschutzauswirkungen ihrer Politiken zu beraten und eine verantwortliche Politikgestaltung zu fördern, im Einklang mit Maßnahme 9 der Strategie des EDSB: „Förderung einer verantwortungsvollen und fundierten politischen Entscheidungsfindung". Sie knüpft an das vom EDSB am 17. November 2017 herausgegebene Reflexionspapier an. Der EDSB ist der Auffassung, dass die Einhaltung der Datenschutzbestimmungen ein Schlüsselelement für die erfolgreiche Herstellung der Interoperabilität der IT-Großsysteme im Raum der Freiheit, der Sicherheit und des Rechts ist.

Zusammenfassung

Die aktuellen drängenden Herausforderungen in den Bereichen Sicherheit und Grenzmanagement erfordern eine intelligentere 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 Schwerkriminellen zu verfügen. Aus der Grundrechteperspektive 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.

INHALT

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 7 und 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1] und auf die 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)[2],

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[3], insbesondere auf Artikel 28 Absatz 2, Artikel 41 Absatz 2 und Artikel 46 Buchstabe d,

gestützt auf den Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden[4], und auf die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates[5] —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 Einleitung

1.1 Hintergrund

1 Im April 2016 verabschiedete die Kommission eine Mitteilung *Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit*[6], 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.[7]

3 Die HLEG legte Empfehlungen zunächst in ihrem Zwischenbericht vom Dezember 2016[8] und später in ihrem Abschlussbericht vom Mai 2017[9] 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.[10] Die Kommission verkündete ihre Absicht, auf die Einrichtung eines europäischen Suchportals, eines gemeinsamen biometrischen Dienstes und eines gemeinsamen Speichers für Identitätsdaten hinzuarbeiten.

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.[11] Am 27. Juli 2017 leitete die Kommission eine öffentliche Konsultationzur Interoperabilität der EU-Informationssysteme im Bereich Grenzen und Sicherheit ein.[12] 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.[13] 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“.

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)[14], und
  - zwei, über die noch verhandelt wird, nämlich das vorgeschlagene Europäische Reiseinformations- und genehmigungssystem (ETIAS)[15] und das vorgeschlagene Europäische Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN)[16];
- die Interpol-Datenbank für gestohlene und verlorene Reisedokumente (SLTD) und
- Europol-Daten.[17]

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.

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.

2 Allgemeine Kommentare

19 Die aktuellen drängenden Herausforderungen in den Bereichen Sicherheit und Grenzmanagement erfordern eine intelligentere Nutzung der den Behörden bereits vorliegenden Informationen. Sofern Interoperabilität durchdacht umgesetzt wird, kann sie einen Beitrag zum Aufbau eines wirksamen und effizienten Informationsaustauschs leisten. In diesem Zusammenhang hat der EDSB die Initiative der Kommission unterstützt, mit Überlegungen über eine strategische Gesamtvision dazu zu beginnen, wie bei voller Wahrung des Datenschutzes das Management und die Verwendung von Daten wirksamer und effizienter gestaltet werden können.[18] Er räumt ein, dass Interoperabilität,

sofern sie unter umfassender Wahrung der Grundrechte entwickelt wird, ein hilfreiches Instrument sein kann, mit dem auf berechtigte Anliegen zuständiger Behörden eingegangen werden kann, die IT-Großsysteme nutzen.

20 In den letzten Jahren hat der EDSB eine wachsende Tendenz beobachtet, Fragen des Managements von Sicherheit und Migration gemeinsam anzugehen. Als Beispiele für diese Tendenz seien die Gewährung des Zugangs zu bestehenden Migrationsinformationssystemen für Zwecke der Strafverfolgung[19], der Aufbau von EU-Informationssystemen mit zweifacher Zielsetzung[20] oder die Erweiterung des Auftrags von EU-Agenturen[21] genannt. Mit der Herstellung von Interoperabilität zwischen Instrumenten in den Bereichen Migration, polizeiliche Zusammenarbeit und auch justizielle Zusammenarbeit sind die Vorschläge Teil dieser Tendenz. Wie bereits in seinem Reflexionspapier unterstrichen, befürchtet der EDSB, dass dadurch, dass Migration, innere Sicherheit und Terrorismusbekämpfung verstärkt als austauschbare Begriffe verwendet werden, die Grenzen zwischen Migrationssteuerung und Bekämpfung von Kriminalität und Terrorismus zu verwischen drohen. Dies könnte sogar dazu führen, dass Terroristen, Kriminelle und Ausländer gleichgesetzt werden.

21 Des Weiteren hält er fest, 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.

22 Eine Beurteilung der genauen Auswirkungen eines solchen Systems mit so vielen „beweglichen Teilen“ auf Privatsphäre und Datenschutz ist praktisch unmöglich. Sowohl aus technischer als auch aus rechtlicher Sicht machen die Vorschläge die vorhandenen sowie die noch im Entstehen begriffenen Systeme noch komplexer. Eine auf diese Weise umgesetzte Interoperabilität führt zu mehr Komplexität, nicht jedoch zu Vereinfachung. Der EDSB hat zwar Verständnis für die hinter den Vorschlägen stehenden Gründe, ist jedoch der Ansicht, dass weitere Komplexität möglicherweise das ureigenste, in Artikel 2 Absatz 2 Buchstabe e der Vorschläge niedergelegte Ziel gefährdet, nämlich die Verschärfung, Vereinfachung und Vereinheitlichung der für die einzelnen Informationssysteme der EU geltenden Bedingungen für die Sicherheit und den Schutz der Daten.

23 Diese Komplexität wird Auswirkungen nicht nur auf den Datenschutz, sondern auch auf die Governance und Kontrolle der Systeme haben. In diesem Zusammenhang erinnert der EDSB daran, dass IT-Großsysteme der EU im Raum der Freiheit, der Sicherheit und des Rechts gewaltige Auswirkungen auf die Grundrechte natürlicher Personen haben, darunter ihr Recht auf Datenschutz, und somit eine effiziente und starke unabhängige Aufsicht erfordern. Daher unterstreicht er die Notwendigkeit, die Datenschutzbehörden einschließlich des EDSB mit den erforderlichen zusätzlichen Finanzmitteln und Humanressourcen auszustatten, damit sie ihre Aufsichtsfunktion ordnungsgemäß wahrnehmen können.

24 In ihrer jetzigen Fassung vermitteln die Vorschläge den Eindruck, Interoperabilität sei der Schlussbaustein bereits voll funktionsfähiger Informationssysteme (oder zumindest derjenigen, für die die Gründungsrechtsakte im Gesetzgebungsverfahren bereits stabil sind). Wie bereits erwähnt, ist dies jedoch nicht der Fall; aus dem Blickwinkel der

Kohärenz und aus Achtung vor dem demokratischen Verfahren wäre es besser gewesen, die Vorschläge nach der Annahme der verschiedenen anhängigen Rechtsinstrumente vorzulegen bzw. zumindest alle relevanten Legislativvorschläge zum gleichen Zeitpunkt gemeinsam vorzustellen. Es kommt darauf an, für Kohärenz zwischen den bereits in der Verhandlung befindlichen (oder anstehenden) Rechtstexten und den Vorschlägen zu sorgen, damit es ein einheitliches rechtliches, organisatorisches und technisches Umfeld für alle Datenverarbeitungsaktivitäten innerhalb der Union gibt. In diesem Zusammenhang weist der EDSB 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.

25 Der EDSB räumt ein, dass heute mehr denn je Bedarf an einem besseren Informationsaustausch und einer effizienteren Nutzung der IT-Großsysteme der EU besteht, um einerseits die durch Migration entstehenden Herausforderungen bewältigen und andererseits durch Terrorismus und Kriminalität entstehende Probleme lösen zu können. Das Erfordernis einer besseren Verwertung der Daten darf jedoch nie die Verletzung des Grundrechts auf Datenschutz zur Folge haben. Interoperabilität ist nicht vorrangig eine technische Entscheidung, sondern insbesondere eine politische Entscheidung. 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.

26 Schließlich möchte der EDSB in Erinnerung rufen, dass der Schutz der Grundrechte, darunter das in der EU-Charta der Grundrechte verankerte Recht auf Privatsphäre und Datenschutz, nicht auf EU-Staatsangehörige beschränkt ist. Die EU und die Mitgliedstaaten haben dieses Recht zu wahren, wenn sie EU-Recht auf natürliche Personen anwenden, unabhängig davon, ob es sich um einen EU-Bürger, einen Drittstaatsangehörigen, einen (legalen oder illegalen) Migranten oder einen Asylbewerber handelt. Die Charta muss die Richtschnur für alle Maßnahmen und Rechtsvorschriften der EU sein. Der EDSB ist gerne bereit, dem EU-Gesetzgeber dabei behilflich zu sein, dass dem wirklich so ist.

3 Hauptempfehlungen

3.1 Einleitung

27 Wie bereits in seinem Reflexionspapier zum Ausdruck gebracht, ist der EDSB der Auffassung, dass Interoperabilität kein Selbstzweck sein, sondern stets einem Ziel dienen sollte, das wirklich im öffentlichen Interesse liegt. Er begrüßt daher, dass in den

Vorschlägen die dem Gemeinwohl dienenden Zielsetzungen sowie die eher spezifischen Ziele aufgeführt werden, die mit Interoperabilität erreicht werden sollen.

28 Seiner Auffassung nach ist die in den Vorschlägen dargestellte Interoperabilität mehr als die Summe ihrer Teile, da ihre Komponenten letztendlich gemeinsam zum Aufbau einer zentralen Datenbank von Drittstaatsangehörigen beitragen, insbesondere eines zentralen biometrischen Registers von Drittstaatsangehörigen. Im Gegensatz zu dezentralen Datenbanken birgt eine zentrale Datenbank implizit die Gefahr des Missbrauchs und weckt sie eher den Wunsch nach einer Nutzung des Systems über die Zwecke hinaus, für die sie eigentlich gedacht war. Daher ist es notwendig, die Vorschläge sehr genau zu prüfen und dabei besondere Aufmerksamkeit der Frage zu schenken, ob alle erforderlichen Garantien gegeben sind.

29 Die Vorschläge führen insbesondere neue Verwendungen der bereits in anderen Systemen erhobenen Daten sowie Änderungen bei den derzeitigen Rechten und Bedingungen für den Zugriff auf diese Daten und bei der Architektur der Systeme ein. Sie bringen also neue Datenverarbeitungsvorgänge mit sich, die durch bestehende Rechtsgrundlagen nicht abgedeckt sind. Dies hat Auswirkungen auf die Grundrechte auf Privatsphäre und Datenschutz, die sorgfältig geprüft werden müssen.

3.2 Verwendung von Daten für neue Zwecke

30 Mit den Vorschlägen wird ein CIR (gemeinsamer Speicher für Identitätsdaten) geschaffen, der eine individuelle Datei für jede der in mindestens einem der folgenden Systeme erfassten Personen enthält: EES, VIS, ETIAS, Eurodac und ECRIS-TCN. In der individuellen Datei werden Daten zusammengetragen, die in den verschiedenen Systemen über diese Person erfasst wurden (aus technischen Gründen mit Ausnahme der im SIS gespeicherten Daten). Diese Daten umfassen biografische Daten (Namen, Vornamen, Geburtsort und Geburtsdatum, Geschlecht, Staatsangehörigkeiten, Reisedokumente) und biometrische Daten (Fingerabdrücke und Gesichtsbilder). Für jeden Datensatz enthält der CIR einen Verweis auf die Informationssysteme, zu dem die Daten gehören. Der gemeinsame BMS und der MID ermöglichen einen Abgleich mit den im CIR sowie den im SIS gespeicherten Daten.

31 Einleitend unterstreicht der EDSB, dass im CIR Daten über alle Drittstaatsangehörigen gespeichert werden, die die EU-Grenzen überschritten haben bzw. dies zu tun gedenken (mit einigen Ausnahmen), also über Millionen von Menschen. Zu diesen Daten gehören biometrische Daten, die von Natur aus höchst sensibel sind. Denn anders als andere personenbezogene Daten werden biometrische Daten weder von einem Dritten zur Verfügung gestellt noch von der betreffenden Person ausgewählt; sie sind untrennbar mit dem Körper verknüpft und beziehen sich eindeutig und dauerhaft auf eine Person. Außerdem ist eine Datenbank erst recht angreifbar, begehrt und wird sie vielfältig genutzt, wenn sie groß und mit Tausenden von Zugangspunkten verbunden ist und in ihr sensible Daten wie biometrischen Daten gespeichert werden.

32 Aufgrund der Größe einer zentralen Datenbank und der Art der darin gespeicherten Daten könnte beim CIR jeder Verstoß gegen die Datenschutzvorschriften einer potenziell sehr großen Zahl natürlicher Personen schweren Schaden zufügen. Sollte der CIR jemals in die falschen Hände geraten, könnte er ein gefährliches, gegen die Grundrechte gerichtetes Werkzeug werden, sofern er nicht von strengen und ausreichenden rechtlichen,

technischen und organisatorischen Garantien umgeben ist. Besondere Wachsamkeit ist daher sowohl bezüglich der Zweckbestimmungen des CIR als auch der Bedingungen und Modalitäten für die Nutzung geboten.

33 Der EDSB erinnert daran, dass zwar die Systeme, aus denen Daten in den CIR eingegeben werden, zur Unterstützung des Grenzmanagements und/oder der Strafverfolgung aufgebaut wurden[22], dass aber jedes von ihnen für einen ganz konkreten Zweck eingerichtet wurde (z. B. das EES zur Identifizierung von Overstayern, das Eurodac-System zur Bestimmung des für die Prüfung eines Asylantrags zuständigen Mitgliedstaats usw.).

34 Er stellt fest, dass die Vorschläge die Möglichkeit einer umfassenderen Nutzung der Systeme vorsehen, also über die spezifischen Zweckbestimmungen hinaus, für die sie eingerichtet wurden. So werden insbesondere in den verschiedenen Systemen gespeicherte Daten zusammengeführt, um gegen Identitätsbetrug vorzugehen, aber auch, um Identitätsprüfungen innerhalb des Hoheitsgebietes von Mitgliedstaaten zu erleichtern.

3.2.1 Bekämpfung von Identitätsbetrug

35 Den Folgenabschätzungen ist zu entnehmen, dass eines der Hauptziele der Vorschläge die Bekämpfung von Identitätsbetrug ist. Der EDSB erkennt an, dass die Bekämpfung von Identitätsbetrug ein legitimes Ziel des öffentlichen Interesses ist. Wie bereits deutlich zum Ausdruck gebracht, dürfte jedoch die vorgeschlagene Lösung, also die Schaffung einer Datenbank mit Informationen über Millionen von Drittstaatsangehörigen (einschließlich ihrer biometrischen Daten) aus der Perspektive der Grundrechte auf Privatsphäre und Datenschutz höchst zudringlich sein. Wie es in Erwägungsgrund 38 heißt, bedeuten die neuen Datenverarbeitungsverfahren, die eine korrekte Identifizierung der Personen ermöglichen, einen Eingriff in die nach den Artikeln 7 und 8 der Charta geschützten Grundrechte dieser Personen. Folglich sind sie auf ihre Notwendigkeit und Verhältnismäßigkeit zu testen (Artikel 52 Absatz 1 der Charta).

36 Wie es im Reflexionspapier des EDSB heißt, sollten die Probleme, die mit den Vorschlägen gelöst werden sollen, ausreichend und klar dargestellt werden und sollte ihre Existenz durch objektive Beweise belegt werden. Der EDSB stellt fest, dass in der Folgenabschätzung lediglich darauf hingewiesen wird, dass die in den EU-Systemen enthaltenen Informationen nicht immer vollständig, genau und zuverlässig sind. Sie assoziiert dies (ohne nähere Erläuterungen) mit dem Fehlen von Verbindungen zwischen Daten in den verschiedenen Systemen, das es wiederum sehr schwierig macht, Mehrfachidentitäten aufzudecken oder Identitätsbetrug zu bekämpfen.[23] Die Folgenabschätzung hebt im Wesentlichen auf die Wahrscheinlichkeit von Identitätsbetrug und auf die Schwierigkeiten, potenziellen Betrug aufzudecken, ab, doch bietet sie keinerlei Erklärungen oder Einschätzungen des Umfangs des Problems und macht auch keine Angaben zu Fällen von Identitätsbetrug, mit denen zuständige Behörden zu tun hatten. Ohne nähere Angaben zum Vorliegen von Identitätsbetrug kann nur schwer gewährleistet werden, dass die vorgeschlagene Maßnahme angemessen und verhältnismäßig ist.

3.2.2 Erleichterung der Identifizierung einer Person bei einer Identitätskontrolle (Artikel 20)

37 Gemäß Artikel 20 der Vorschläge dürfen mitgliedstaatliche Polizeibehörden ausschließlich zum Zwecke der Identifizierung einer Person anhand der bei einer Identitätskontrolle erhobenen biometrischen Daten dieser Person Abfragen im CIR vornehmen. Dieser Zugriff muss in einer einzelstaatlichen Rechtsvorschrift geregelt sein. In dieser Rechtsvorschrift sind die genauen Zwecke der Identitätskontrollen im Rahmen (als Teil) der Verhütung und Bekämpfung irregulärer Migration und/oder als Beitrag zu einem hohen Maß an Sicherheit festzulegen. Ferner werden dort die befugten Polizeibehörden benannt sowie die Verfahren, Bedingungen und Kriterien der Kontrollen festgelegt.

38 Als Begründung der Notwendigkeit einer solchen Verwendung wird in der Folgenabschätzung darauf hingewiesen, dass zwar die Behörden der Mitgliedstaaten Register von EU-Staatsangehörigen und in der EU wohnhaften Personen führen, sie aber keine vollständigen Register von kurzzeitig aufhältigen Drittstaatsangehörigen führen können, da diese Drittstaatsangehörigen über verschiedene Mitgliedstaaten einreisen, reisen und ausreisen können. Der CIR könnte diese Lücke schließen, indem er Behörden der Mitgliedstaaten den Zugriff auf das Eurodac-System, das VIS, das EES, das ETIAS und das ECRIS-TCN zum Zweck der Identifizierung von Personen im Hoheitsgebiet der EU gewährt und sie in die Lage versetzt, ihre verschiedenen Aufgaben und Pflichten korrekt und effizient wahrzunehmen.[24]

39 Der EDSB weist noch einmal nachdrücklich darauf hin, dass die Identifizierung einer Person kein Selbstzweck ist, sondern einem konkreten Ziel dienen muss, beispielsweise der Prüfung der Frage, ob die Person polizeilich gesucht wird oder sich in der EU aufhalten darf (z. B. im Besitz eines gültigen Visums ist).

40 Er hält fest, dass gemäß Artikel 20 die Identifizierung der Person zur Verhütung und Bekämpfung irregulärer Migration oder zur Gewährleistung eines hohen Maßes an Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts beitragen muss, einschließlich der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie des Schutzes der inneren Sicherheit im Hoheitsgebiet der Mitgliedstaaten. Mit anderen Worten: Die Verwendung der Daten im CIR zur Identifizierung einer Person wäre zulässig, wenn dies zur Bekämpfung irregulärer Migration erforderlich ist oder zu einem hohen Maß an Sicherheit beiträgt.

41 Der EDSB unterstreicht, dass „Bekämpfung irregulärer Migration und Gewährleistung eines hohen Maßes an Sicherheit“ eine sehr vage Beschreibung von (ansonsten legitimen) Zwecken ist. Er merkt an, dass Artikel 20 den Erlass einer nationalen Rechtsvorschrift verlangt, in der diese näher bestimmt werden. Er erinnert jedoch daran, dass der Gerichtshof der Europäischen Union („EuGH“) in seinem Urteil in *Digital Rights Ireland* befand, dass die Richtlinie 2006/24 *„kein objektives Kriterium vorsieht, das es ermöglicht, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zwecks Verhütung, Feststellung oder strafrechtlicher Verfolgung auf Straftaten zu beschränken“*, weil sie *„lediglich allgemein auf die von jedem Mitgliedstaat in seinem nationalen Recht bestimmten Straftaten Bezug nimmt“*.[25] Der Gerichtshof vertrat ferner die Auffassung, der Zugang zu diesen Daten und deren spätere Nutzung sei

nicht *„strikt auf den Zweck der Verhütung und Feststellung genau abgegrenzter schwerer Straftaten oder der sie betreffenden Strafverfolgung“* beschränkt.[26]

42 **Nach Auffassung des EDSB sind die Zwecke der Bekämpfung irregulärer Migration und des Beitrags zu einem hohen Maß an Sicherheit vor dem Hintergrund von Artikel 20 zu breit gefasst und erfüllen sie in den Vorschlägen nicht die Vorgaben des Gerichtshofs, *„strikt beschränkt“* und *„genau abgegrenzt“* zu sein. Er empfiehlt daher, sie in den Vorschlägen genauer zu definieren.** „Irreguläre Migration“ könnte beispielsweise auf die Einreise- und Aufenthaltsbedingungen verweisen, wie sie in Artikel 6 der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates niedergelegt sind. Mit Blick auf die Sicherheit empfiehlt der EDSB, auf die Straftaten abzuheben, die ein hohes Maß an Sicherheit besonders bedrohen könnten; hier könnte beispielsweise auf die in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI aufgelisteten Straftaten verwiesen werden, sofern sie nach nationalem Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind.

43 Im Hinblick auf die Bedingungen für den Zugriff auf im CIR gespeicherte Daten weist der EDSB darauf hin, dass der Gerichtshof in seinem Urteil *Digital Rights Ireland* auch kritisiert hat, dass die *„Richtlinie 2006/24 keine materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung“* enthält, da sie *„lediglich vorsieht, dass jeder Mitgliedstaat das Verfahren und die Bedingungen festlegt, die für den Zugang zu den auf Vorrat gespeicherten Daten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind“*.[27]

44 Der EDSB stellt fest, dass in Artikel 20 einige Bedingungen und Kriterien festgelegt sind, denn er beschränkt den Zugang auf Polizeibehörden, die Abfragen ausschließlich zum Zwecke der Identifizierung einer Person bei einer Identitätskontrolle vornehmen dürfen. Seiner Auffassung nach sollten diese Bedingungen jedoch in den Vorschlägen näher ausgeführt werden, damit sie den Vorgaben des Gerichtshofs entsprechen. **Nach Auffassung des EDSB 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 gleichwertigen Bedingungen ein Zugang auch zu ähnlichen nationalen Datenbanken (z. B. Register von Staatsangehörigen/wohnhaften Personen) 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.

45 Des Weiteren weist er darauf hin, dass eine Identitätskontrolle üblicherweise so abläuft, dass eine Polizeibehörde Personen im Einklang mit den im nationalen Recht festgelegten Anforderungen auffordert, ihre Identität durch geeignete Mittel wie einen Personalausweis oder ein anderes gültiges Dokument zu beweisen.

46 In diesem Zusammenhang hält er fest, dass gemäß Artikel 20 Absatz 1 für den Fall, dass die biometrischen Daten der Person nicht verwendet werden können oder die Abfrage anhand dieser Daten nicht erfolgreich ist, die Abfrage anhand von Identitätsdaten in Verbindung mit dem Reisedokument oder anhand der von der Person bereitgestellten Identitätsdaten vorzunehmen ist. Das bedeutet, dass die Identitätskontrolle zunächst

anhand biometrischer Daten und erst bei einem Scheitern dieser Vorgehensweise anhand anderer Daten wie Namen und Reisedokument vorgenommen würde. Nach Ansicht des EDSB sollte eine Abfrage des CIR zur Identifizierung einer Person bei einer Identitätskontrolle anhand biometrischer Daten nur als letzte Möglichkeit erfolgen, nämlich

- wenn die Person zur Kooperation nicht in der Lage ist (weil die Person z. B. nicht versteht, was von ihr verlangt wird) und kein Dokument bei sich hat, aus dem ihre Identität hervorgeht, oder
- wenn sie die Kooperation verweigert, oder
- wenn der berechtigte und begründete Verdacht besteht, dass Dokumente falsch sind oder dass die Person über ihre Identität nicht die Wahrheit sagt.

47 Würden systematisch bei einer Identitätskontrolle biometrische Daten einer Person herangezogen, entstünde die Gefahr der Stigmatisierung bestimmter Menschen (oder Gruppen von Menschen) aufgrund ihres Erscheinungsbilds und käme es zu einer nicht gerechtfertigten Ungleichbehandlung von EU-Bürgern und Drittstaatsangehörigen.

48 **Der EDSB empfiehlt daher eine Änderung von Artikel 20 dahingehend, dass der Zugang zum CIR erlaubt 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.**

3.2.3 Nutzung des vorgeschlagenen ECRIS-TCN

49 Einleitend möchte der EDSB betonen, dass es das ECRIS-TNC noch nicht gibt. Der Vorschlag zu seiner Einrichtung[28] wird derzeit von den EU-Gesetzgebern erörtert.

50 Der EDSB hält fest, dass gemäß den Artikeln 17 und 18 des Vorschlags polizeiliche und justizielle Zusammenarbeit, Asyl und Migration der CIR die folgenden im ECRIS-TCN gespeicherten Daten enthalten würde: Nachname oder Familienname, Vorname(n), Geschlecht, Geburtsdatum, Geburtsort und -land, Staatsangehörigkeit(en), Gender sowie gegebenenfalls frühere Namen, Pseudonym(e) und/oder Aliasname(n); Gesichtsbild, Fingerabdruckdaten sowie das Aktenzeichen der Fingerabdruck-Daten der verurteilten Person einschließlich des Codes des Urteilsmitgliedstaats. Im Ergebnis bedeutet dies, dass diese Daten für die Zwecke des CIR abgerufen und verwendet werden könnten, vor allem für die Erleichterung von Identitätskontrollen und die Aufdeckung von Mehrfachidentitäten.

51 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. Das Argument, der CIR sollte Daten aus dem vorgeschlagenen ECRIS-TCN enthalten, da die Identitäten von in diesem System gespeicherten Drittstaatsangehörigen von einer Justizbehörde überprüft würden[29] – und daher zuverlässiger seien – dürfte für

ein Bestehen der in Artikel 52 Absatz 1 der Charta vorgesehenen Tests der Notwendigkeit und Verhältnismäßigkeit nicht ausreichen.

52 Darüber hinaus erinnert der EDSB daran, dass das Ziel des ECRIS-TCN darin besteht, die justizielle Zusammenarbeit in Strafsachen durch einen besseren Austausch von Informationen über Strafregistereinträge in der gesamten EU zu verstärken. In Artikel 22 des Vorschlags über die Errichtung des ECRIS-TCN[30] ist konkret vorgesehen, dass die Daten im System nur zum Zweck der Ermittlung der Mitgliedstaaten verarbeitet werden dürfen, in denen Strafregisterinformationen zu Drittstaatsangehörigen vorliegen. Die Verwendung der im vorgeschlagenen ECRIS-TCN gespeicherten Daten zur Aufdeckung von Mehrfachidentitäten und zur Erleichterung von Identitätskontrollen dürfte weit über die Ziele des ECRIS-TCN hinausgehen, wie sie in dem Vorschlag zu seiner Einrichtung festgelegt sind, und wirft die Frage nach ihrer Vereinbarkeit mit dem Grundsatz der Zweckbindung auf.

53 **Der EDSB 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 Gründungsrechtsakt festgelegt sind.**

3.3 Erleichterung des Zugangs zu den Daten zu Strafverfolgungszwecken (Artikel 22)

54 Die Möglichkeit der Verwendung von im EES, VIS, ETIAS oder Eurodac-System gespeicherten Identitätsdaten zur Verhütung, Aufdeckung und Untersuchung terroristischer Straftaten oder schwerer Straftaten ist nicht neu. Diese Möglichkeit ist in den (bestehenden oder in der Aushandlung befindlichen) Gründungsinstrumenten dieser Systeme vorgesehen. Allerdings bringen die Vorschläge erhebliche Änderungen an den Bedingungen für den Zugang zu diesen in diesen Instrumenten vorgesehenen Daten mit sich.

55 Der EDSB hat wiederholt deutlich seine Bedenken bezüglich der allgemeinen, in der EU in den letzten Jahren zu beobachtenden Tendenz geäußert, Strafverfolgungsbehörden Zugang zu Systemen zu gewähren, die für andere als Strafverfolgungszwecke eingerichtet wurden. Sollte der Bedarf an einem solchen Zugang nachgewiesen werden, hat er darauf bestanden, dass er nicht systematisch gewährt werden sollte, sondern nur unter besonderen Umständen, fallweise und unter strengen Auflagen. Zu diesen Auflagen gehört, dass Ersuchen um Zugang zu den Daten genau gezielt sind und aufgrund eines Verdachts gegen bestimmte Personen erfolgen.[31]

56 Artikel 22 Absatz 1 der Vorschläge besagt, dass Strafverfolgungsbehörden und Europol im konkreten Einzelfall den CIR abfragen könnten, um terroristische oder sonstige schwere Straftaten zu verhüten, aufzudecken oder zu untersuchen und um in Erfahrung zu bringen, ob im EES, im VIS, im ETIAS oder im Eurodac-System Daten zu einer spezifischen Person gespeichert sind.

57 Die Abfrage des CIR würde in zwei Stufen erfolgen: Anfangs wird nur ein Verweis auf ein System („Treffer/kein Treffer“) angezeigt; der volle Zugriff wird dann erst in einer späteren Phase gewährt. Für den Fall, dass die Daten in der Abfrage mit Daten übereinstimmen, die in mindestens einem der Systeme gespeichert sind, wird eine

Trefferkennzeichnung angezeigt und angegeben, welche(s) System(e) betroffen ist/sind. (Artikel 22 Absatz 3, Abfrage auf der ersten Ebene). Der vollständige Zugang zu den Daten unterläge jedoch weiterhin den Bedingungen und Verfahren, die in den einschlägigen Rechtsvorschriften festgelegt sind (Artikel 22 Absatz 4, Abfrage auf der zweiten Ebene).

58 Der EDSB räumt ein, dass eine „Trefferkennzeichnung" nur begrenzte Informationen enthält. Im Gegensatz zu den Ausführungen in Erwägungsgrund 33 besteht eine „Trefferkennzeichnung" aus Informationen über eine identifizierte (oder identifizierbare) Person und somit aus personenbezogenen Daten. Wie der EDSB bereits in seinem Reflexionspapier deutlich ausgeführt hat, ist das Vorliegen (oder Ausbleiben) eines „Treffers" stets als personenbezogenes Datum zu betrachten, da selbst bei einem absoluten Informationsminimum (z. B. in einem bestimmten System bekannt oder unbekannt) die Anzeige „Treffer" oder „kein Treffer" personenbezogene Informationen sind (z. B. die Person ist (kein) Asylbewerber). Folglich stellt die Verarbeitung solcher Daten einen Eingriff in die durch die Artikel 7 und 8 der Charta geschützten Grundrechte dar und muss im Hinblick auf Notwendigkeit und Verhältnismäßigkeit im Einklang mit Artikel 52 Absatz 1 der Charta stehen.

59 In der Begründung wird auf die verschiedenen Zugangsbedingungen und Garantien der einzelnen Systeme eingegangen, jedoch auch unterstrichen, dass einige der derzeitigen Vorschriften die Strafverfolgungsbehörden in einer raschen rechtmäßigen Nutzung der Systeme behindern könnten. Mit Hilfe der Abfrage auf der ersten Ebene würden die Vorschläge tatsächlich die Bedingungen und Modalitäten für den Zugang von Strafverfolgungsbehörden für Strafverfolgungszwecke lockern.

60 Der EDSB weist darauf hin, dass derzeit alle (bestehenden und vorgeschlagenen) Gründungsinstrumente für die betreffenden Systeme die folgenden kumulativen Zugangsbedingungen vorsehen:

- Der Zugang muss für die Prävention, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerwiegender Straftaten erforderlich sein;
- der Zugang muss in einem konkreten Fall erforderlich sein;
- es liegen berechtigte Gründe für die Annahme vor, dass die Abfrage wesentlich zur Verhütung, Aufdeckung oder Untersuchung der fraglichen Straftaten beitragen wird.

Abgesehen davon machen die verschiedenen Instrumente eine Überprüfung der Frage durch eine unabhängige Behörde erforderlich, ob vor dem Zugang die genannten Bedingungen erfüllt sind. Im Fall von ETIAS, EES und Eurodac sind die Strafverfolgungsbehörden außerdem verpflichtet, zunächst andere einschlägige Systeme abzufragen (z. B. nationale Datenbanken, Europol-Daten, Prüm, VIS).

61 In der Folgenabschätzung wird behauptet, dass dieser „Kaskadenmechanismus" (also die Verpflichtung zu vorheriger Überprüfung und vorheriger Abfrage) erheblichen Verwaltungsaufwand mit sich bringt und zu Verzögerungen führt und Gelegenheiten verstreichen lässt, benötigte Informationen aufzudecken. Es heißt dort, die Strafverfolgungsbehörde müssten ihre Abfrage beenden, sobald in einem System Informationen gefunden wurden. Das bedeutet jedoch nicht, dass nicht das nächste oder auch ein späteres System in der Kaskade noch wertvolle Informationen für Strafverfolgungszwecke enthalten kann.[32]

62 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 Schwerkriminellen zu verfügen. Aus der Grundrechteperspektive ist jedoch die Erleichterung des Zugriffs für Strafverfolgungsbehörden auf nicht bei der Strafverfolgung angesiedelte Systeme (selbst auf begrenzte Informationen wie Treffer/kein Treffer) alles andere als unerheblich. Es ist zu bedenken, dass diese Systeme aufgebaut und entwickelt wurden für die Anwendung spezifischer Politiken und nicht als Instrument der Strafverfolgung. Ein routinemäßiger Zugriff wäre ein Verstoß gegen den Grundsatz der Zweckbindung. Er hätte ein unverhältnismäßiges Eindringen in die Privatsphäre beispielsweise von Reisenden zur Folge, die zwecks Erhalt eines Visums in die Verarbeitung ihrer Daten eingewilligt haben und nun erwarten, dass ihre Daten auch für diesen Zweck erhoben, abgefragt und übermittelt werden. Des Weiteren wäre es nicht hinnehmbar, wenn echte Garantien, die zur Wahrung von Grundrechten eingeführt wurden, hauptsächlich im Interesse der Beschleunigung eines Verfahrens aufgehoben würden. Besteht Bedarf an einer Verbesserung des Verfahrens, sollte diese nicht zu Lasten von Garantien vorgenommen werden.

63 Nach Ansicht des EDSB ergibt sich aus Artikel 22 der Vorschläge, dass eine der Hauptbedingungen für den Zugang zu den Systemen nicht länger gilt, nämlich das Vorliegen berechtigter Gründe für die Annahme, dass die Abfrage wesentlich zur Verhütung, Aufdeckung oder Untersuchung einer terroristischen oder sonstigen schwerwiegenden Straftat beitragen wird. Ein berechtigter Grund könnte beispielsweise ein an einem Tatort gefundenes gefälschtes Reisedokument sein. Seiner Auffassung nach ist das Vorliegen berechtigter Gründe eine wesentliche Voraussetzung für jeden Zugang von Strafverfolgungsbehörden zu Systemen anderer Behörden. Es bietet tatsächlich eine wesentliche Garantie gegen mögliche „Fishing Expeditions".

64 Des Weiteren ist der EDSB nicht davon überzeugt, dass eine vorherige Suche in den nationalen Datenbanken wirklich ein Hindernis darstellt. Man kann wohl davon ausgehen, dass Strafverfolgungsbehörden zunächst ihre eigenen nationalen (Kriminal-) Datenbanken abfragen, zu denen sie unmittelbaren Zugang haben. Wird die Person zweifelsfrei als EU-Bürger identifiziert, kann der EDSB keine Notwendigkeit einer Abfrage des CIR erkennen. Die vorherige Suche in den nationalen Datenbanken sollte dann Voraussetzung für den Zugriff auf den CIR bleiben, würde aber nicht automatisch einen späteren Zugang zum CIR verhindern, falls die anderen Bedingungen erfüllt sind (also spezifischer Fall, Strafverfolgungszwecke und berechtigte Gründe).

65 Der EDSB fragt sich ferner, warum die Abfrage der automatisierten Fingerabdruck-Identifizierungssysteme der anderen Mitgliedstaaten nach dem Beschluss 2008/615/JI („Prüm-Beschluss")[33] nicht länger vorgesehen ist. Der EDSB erinnert daran, dass es heute dank des Prüm-Beschlusses[34] in der Strafverfolgung ein spezifisches System gibt, mit dem der Austausch polizeilicher Informationen einschließlich Fingerabdruckdaten erleichtert werden soll, um die grenzüberschreitende Zusammenarbeit zwischen den Polizei- und Justizbehörden der Mitgliedstaaten bei der Bekämpfung von Terrorismus und grenzüberschreitender Kriminalität zu intensivieren. Probleme mit seiner Wirksamkeit, die (unter anderem) darauf zurückzuführen sind, dass es von den Mitgliedstaaten nicht voll umgesetzt wurde oder nicht genutzt wird, können nicht als stichhaltiges Argument zugunsten eines einfacheren Zugang von

Strafverfolgungsbehörden zu Systemen anderer Behörden angeführt werden. Nach Auffassung des EDSB sollte die Abfrage anderer Systeme nach dem Prüm-Beschluss Bedingung für den Zugriff auf den CIR bleiben und zumindest parallel zur Abfrage des CIR erfolgen.

66 Daher vertritt der EDSB die Ansicht, dass der Zugang zum CIR zur Beantwortung der Frage, ob eine bestimmte Person in einem der an den CIR angeschlossenen Systeme erfasst ist (Angabe „Treffer/kein Treffer“) nur unter folgenden Bedingungen erlaubt sein sollte:

- für Zwecke der Prävention, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten,
- in einem konkreten Einzelfall,
- wenn berechtigte Gründe für die Annahme vorliegen, dass die Abfrage wesentlich zur Verhütung, Aufdeckung oder Untersuchung einer terroristischen oder sonstigen schwerwiegenden Straftat beitragen wird; insbesondere wenn ein begründeter Verdacht besteht, dass der Tatverdächtige, der Urheber oder das Opfer einer terroristischen oder sonstigen schweren Straftat in eine Kategorie von Drittstaatsangehörigen fällt, deren Daten im EES, im VIS, im ETIAS und im Eurodac-System gespeichert sind, und
- wenn zuvor eine Abfrage der nationalen Datenbanken stattgefunden hat und eine Abfrage der automatisierten Fingerabdruck-Identifizierungssysteme der anderen Mitgliedstaaten gemäß dem Beschluss 2008/615/JI eingeleitet wurde.

67 Nach Ansicht des EDSB sollten alle genannten Bedingungen in Artikel 22 der Vorschläge erwähnt werden. Er merkt an, dass in Artikel 22 Absatz 1 lediglich von den Bedingungen „Strafverfolgungszwecke“ und „konkreter Einzelfall“ die Rede ist. **Er empfiehlt daher, in Artikel 22 Absatz 1 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“ aufzunehmen.** Der EDSB nimmt ferner zur Kenntnis, dass gemäß Artikel 22 Absatz 4 bei einem „Treffer“ der vollständige Zugang zu den im System gespeicherten Daten weiterhin den Bedingungen und Verfahren unterliegt, die in den einschlägigen Rechtsvorschriften festgelegt sind.

68 Da ein „Treffer“ als persönliches Datum zu betrachten ist, vertritt der EDSB darüber hinaus die Ansicht, dass – unabhängig von einem weiterem Zugriff auf die in dem System gespeicherten Daten, das den Treffer ausgelöst hat – die Einhaltung der Zugangsbedingungen stets kontrolliert werden sollte. **Mit anderen Worten: Die Strafverfolgungsbehörde, die einen Treffer erhält, sollte sich immer an die Kontrollbehörde wenden, die überprüft, ob die Bedingungen für den Zugang zum CIR erfüllt waren. Sollte die nachträgliche unabhängige Überprüfung ergeben, dass die Abfrage des CIR nicht gerechtfertigt war, hat die Behörde alle aus dem CIR stammenden Daten zu löschen. Wir empfehlen eine entsprechende Änderung von Artikel 22 der Vorschläge.**

3.4 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

69 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. Dessen ungeachtet unterstreicht der EDSB, dass die Grundsätze des Datenschutzes in allen Phasen der Umsetzung der Vorschläge zu berücksichtigen sind.

70 In diesem Zusammenhang weist der EDSB auf das bevorstehende Inkrafttreten der Verordnung 2016/679[35] und insbesondere auf die Einführung des Konzepts des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in ihrem Artikel 25 hin. Der EDSB erinnert daran, dass dieses Konzept auch in die neue Verordnung (EG) Nr. 45/2001 Eingang finden wird.[36]

71 Nach diesem Konzept sollten eu-LISA und die Mitgliedstaaten die geeigneten technischen und organisatorischen Maßnahmen ergreifen, damit eine wirksame Wahrung der Grundsätze des Datenschutzes gewährleistet ist und die erforderlichen Garantien vorgesehen werden, damit den Anforderungen der DSGVO Genüge getan wird und insbesondere die Rechte der betroffenen Personen geschützt werden. Ferner sollten eu-LISA und die Mitgliedstaaten dafür Sorge tragen, dass standardmäßig nur die personenbezogenen Daten verarbeitet werden, die für die einzelnen Zwecke der Verarbeitung notwendig sind.

72 Der EDSB empfiehlt, in die Vorschläge einen Hinweis auf die Verpflichtung für eu-LISA und die Mitgliedstaaten aufzunehmen, die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen einzuhalten.

4 Spezifische Empfehlungen

4.1 Verweis auf das geltende Datenschutzrecht

73 Einleitend stellt der EDSB fest, dass manche Artikel der Vorschläge auf bestimmte Vorschriften im geltenden Datenschutzrecht verweisen (also die Verordnung 2016/679, die Richtlinie 2016/680 und die Verordnung (EG) Nr. 45/2001), z. B. die Artikel 46 und 47 der Vorschläge. Nach dem Verständnis des EDSB werden in diesen Bestimmungen die einschlägigen Artikel der genannten Rechtsakte näher spezifiziert. Um jedoch klarzustellen, dass diese Verweise unbeschadet der Anwendung anderer relevanter Bestimmungen dieser Rechtsakte erfolgen, **empfiehlt der EDSB, in die Vorschläge eine Bestimmung bezüglich der Anwendbarkeit der Verordnung 2016/679, der Richtlinie 2016/680 und der Verordnung (EG) Nr. 45/2001 aufzunehmen.**

4.2 Nutzerprofile für das ESP

74 Der EDSB begrüßt, dass die Vorschläge ein zentrales Management für die Einrichtung von Nutzerprofilen mit Zuweisung der rechtmäßigen Zugangsrechte vorsehen. Er betont jedoch, dass **diese Profile regelmäßig überprüft und bei Bedarf auf den neuesten**

Stand gebracht werden sollten. **Der EDSB empfiehlt, diese Verpflichtung in den Wortlaut der Vorschläge aufzunehmen.**

75 In Artikel 7 Absatz 4 der Vorschläge ist festgelegt, welche EU-Stellen Zugang zum ESP haben. Der EDSB empfiehlt, nach **EU-Stellen** einzufügen **„wie in Absatz 1 genannt“**.

76 Artikel 8 Absatz 1 der Vorschläge besagt, dass für jede Kategorie von Nutzerprofil eine Verknüpfung mit drei Elementen vorgenommen wird, nämlich den für die Datenabfrage zu verwendenden Suchfeldern, den Informationssystemen, die abgefragt werden dürfen, und der Art der als Abfrageergebnis auszugebenden Daten. Nach Auffassung des EDSB ist der Zweck der Abfrage gleich wichtig, wird in dem Artikel jedoch nicht erwähnt. **Der EDSB empfiehlt** daher, **in Artikel 8 der Vorschläge auch auf den Zweck der Abfrage zu verweisen**.

4.3 Der gemeinsame BMS - Kategorien von Daten

77 Im Verständnis des EDSB besteht gemäß Erwägungsgrund 17 der Vorschläge der Zweck des gemeinsamen BMS darin, sämtliche biometrischen Templates an einem einzigen Ort zusammenzufassen und zu speichern, um den systemübergreifenden Vergleich anhand biometrischer Daten zu vereinfachen und so Mehrfachidentitäten aufzudecken, insbesondere mit Hilfe des CIR. In diesem Zusammenhang sind in Artikel 13 der Vorschläge alle relevanten biometrischen Daten aufgelistet, die im gemeinsamen BMS gespeichert werden sollen.

78 Mit Blick auf das VIS ist in Artikel 13 Absatz 1 Buchstabe b der Vorschläge bestimmt, dass im gemeinsamen BMS nur die biometrischen Templates von Fingerabdrücken der VIS-Antragsteller gespeichert werden sollen. In Artikel 18 Absatz 1 Buchstabe b des Vorschlags zu Grenzen und Visa ist jedoch festgelegt, dass auch ein Foto des VIS-Antragstellers zu speichern ist. Nach Auffassung des EDSB gehört das Foto des VIS-Antragstellers zu den relevanten biometrischen Daten im Sinne von Artikel 13, was die Aufdeckung von Mehrfachidentitäten spürbar verbessern würde. **Der EDSB fragt sich** daher, **warum das Foto des VIS-Antragstellers in Artikel 13 Absatz 1 Buchstabe b der Vorschläge nicht erwähnt wird**.

79 Bezüglich des SIS verweist Artikel 13 Absatz 1 Buchstabe c der Vorschläge auf Artikel 20 Absatz 2 Buchstaben w und x des Vorschlags für eine Verordnung über das SIS II im Bereich Strafverfolgung. Die Definition daktylografischer Daten im SIS-Vorschlag umfasst jedoch auch Handabdrücke. Der EDSB empfiehlt, in den Vorschlägen klarzustellen, dass der Verweis auf daktylografische Daten im SIS sich lediglich auf Fingerabdrücke, nicht hingegen auf Handabdrücke bezieht. Weiter stellt er fest, dass im Zusammenhang mit dem SIS-Vorschlag für eine Verordnung im Bereich Strafverfolgung Artikel 13 Absatz 1 Buchstabe d der Vorschläge auf Artikel 20 Absatz 3 Buchstaben w und x des Vorschlags für eine Verordnung über das SIS II im Bereich Strafverfolgung verweist. Der EDSB weist darauf hin, dass Artikel 20 Absatz 3 Buchstabe x des Vorschlags für eine Verordnung im Bereich Strafverfolgung ausdrücklich von DNA-Daten spricht. **Der EDSB empfiehlt daher, Artikel 13 Absatz 1 Buchstabe c und Artikel 13 Absatz 1 Buchstabe d der Vorschläge abzuändern, um sicherzustellen, dass weder die DNA-Daten noch die Handabdrücke im gemeinsamen BMS gespeichert werden.**

80 **Mit Blick auf Artikel 16 Absatz 1 Buchstabe d der Vorschläge empfiehlt der EDSB, eine Definition der Länge der Abfrage vorzusehen, da der Begriff sich nicht selbst erklärt.**

4.4 Der CIR - Duplizierung von Einträgen

81 In der Begründung wird unterstrichen, dass eines der Ziele der Vorschläge darin besteht, Verfahren zu vereinfachen und Duplizierung zu verringern.[37] Der EDSB erwartet, dass der CIR daher eine einmalige Eingabe von Daten über eine bestimmte Person unterstützt, falls in den verschiedenen Systemen identische personenbezogene Daten erfasst sind oder korrigiert werden. Dies wird allerdings nicht klar, betrachtet man Artikel 17 in Verbindung mit Artikel 18.

82 Während es in Artikel 17 der Vorschläge heißt, dass im CIR eine individuelle Datei für jede in einem der Systeme erfassten Personen angelegt wird, enthält Artikel 18 der Vorschläge lediglich eine Liste der relevanten Daten, die im CIR gespeichert werden sollten. Das bedeutet, dass für den Fall, dass eine Person mehrere identische Einträge in einem der zugrunde liegenden Systeme hat, der CIR auch diese identischen Daten abrufen wird. Weiter besagt Artikel 23 Absatz 2 der Vorschläge, dass eine individuelle Datei so lange im CIR gespeichert bleiben wird, wie die entsprechenden Daten in mindestens einem der zugrunde liegenden Systeme gespeichert sind.

83 **Der EDSB befürchtet** daher, **dass die Vorschläge die Möglichkeit der Duplizierung personenbezogener Daten nicht in ausreichendem Maße verhindern**. **Er empfiehlt daher, in den entsprechenden Artikeln konkreter zu werden und die erforderlichen Änderungen vorzunehmen.**

4.5 Frist für die Speicherung der Daten im CIR und im MID

84 In Artikel 23 Absatz 2 und Artikel 35 der Vorschläge sind die Fristen für die Aufbewahrung der im CIR bzw. MID gespeicherten Daten festgelegt. Eine individuelle Datei wird aus dem CIR nur dann gelöscht, wenn die entsprechenden Daten aus allen Informationssystemen gelöscht werden. Die Identitätsbestätigungsdateien und die in ihnen enthaltenen Daten einschließlich der Verknüpfungen werden im MID so lange gespeichert, wie die verknüpften Daten in zwei oder mehr Informationssystemen gespeichert sind.

85 In den Vorschlägen wird jedoch nicht spezifiziert, nach welcher Methode Daten nach ihrem Verfall gelöscht werden. Werden Informationen für einen bestimmten Zeitraum in ein System eingegeben, besteht die Gefahr, dass personenbezogene Daten über das Datum hinaus, an dem sie eigentlich hätten gelöscht werden müssen, im System verbleiben – sofern die Speicherfrist nicht vom System überwacht und die automatische Löschung technisch erzwungen wird. **Der EDSB empfiehlt daher, in den einschlägigen Artikeln festzulegen, dass es eine automatische Löschung geben wird.**

4.6 Manuelle Verifizierung von Verknüpfungen

4.6.1 Automatisierte Entscheidungsfindung

86 Der EDSB weist darauf hin, dass die automatisierte Herstellung von Verknüpfungen zum Zweck der Aufdeckung von Mehrfachidentitäten eine automatisierte Entscheidungsfindung im Sinne des Datenschutzrechts wäre. In Anbetracht des Fehlens eines menschlichen Eingreifens sowie des potenziellen Eindringens in die Privatsphäre gewähren die Datenschutzvorschriften unter diesen Umständen natürlichen Personen ein hohes Maß an Schutz. So sehen beispielsweise Artikel 22 der Verordnung 2016/679 und Artikel 19 der Verordnung (EG) Nr. 45/2001 diesbezüglich vor, dass die betroffene Person das Recht hat, keiner Entscheidung – was eine Maßnahme einschließen kann – zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, und dies ohne jegliches menschliches Eingreifen.

87 Auch wenn Artikel 22 Absatz 2 der Verordnung 2016/679 und Artikel 19 der Verordnung (EG) Nr. 45/2001 vorsehen, dass dieses Recht durch eine Rechtsvorschrift eingeschränkt werden kann, erinnert der EDSB doch daran, dass eine solche Rechtsvorschrift „angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten“ muss. Um unter diesen Umständen der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten, muss die Logik der Entscheidungsfindung den betroffenen Personen klar erläutert werden (siehe Artikel 13 Absatz 2 Buchstabe f und Artikel 14 Absatz 2 Buchstabe g der Verordnung 2016/679). Der für die Verarbeitung Verantwortliche sollte ferner geeignete mathematische oder statistische Verfahren für das Profiling verwenden, technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird, und personenbezogene Daten in einer Weise sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen wird und mit denen verhindert wird, dass es gegenüber natürlichen Personen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung zu diskriminierenden Wirkungen oder zu Maßnahmen kommt, die eine solche Wirkung haben.[38]

88 **Der EDSB ist** daher **der Auffassung, dass die Herstellung von Verknüpfungen zum Zweck der Aufdeckung von Mehrfachidentitäten eine automatisierte Entscheidungsfindung wäre**. **Folglich sollten in den Vorschlägen Transparenz gegenüber den betroffenen Personen und die erforderlichen Garantien für eine solche Verarbeitung vorgesehen werden.**

4.6.2 Manuelle Verifizierung

89 Die Vorschläge sehen die Einführung eines Detektors für Mehrfachidentitäten („MID“) vor, der angeben könnte, ob eine Person in den verschiedenen Informationssystemen (also SIS, VIS, ETIAS, ECRIS, EES oder Eurodac) unter unterschiedlichen Identitäten

erfasst ist. Der MID speichert Verknüpfungen zwischen in mehr als einem System erfassten Personen sowie einen Vermerk, aus welchem System die Daten stammen. Diese Verknüpfungen werden vier Kategorien zugeordnet: weiß, gelb, grün und rot.

- Eine weiße Verknüpfung bedeutet, dass die verschiedenen biografischen Identitäten derselben Person zuzuordnen sind.
- Eine gelbe Verknüpfung bedeutet, dass es sich möglicherweise um verschiedene biografische Identitäten derselben Person handelt.
- Eine grüne Verknüpfung bestätigt, das mehrere Personen zufällig dieselbe biografische Identität haben.
- Eine rote Verknüpfung bedeutet, dass der Verdacht besteht, dass sich dieselbe Person unrechtmäßig unterschiedlicher biografischer Identitäten bedient.

90 Artikel 28 Absatz 4 der Vorschläge sieht vor, dass eine gelbe Verknüpfung hergestellt wird, wenn eine Abfrage biometrischer Daten oder von Identitätsdaten einen oder mehrere Treffer ergibt und die Identitätsdaten der verknüpften Dateien nicht als ähnlich angesehen werden können. Artikel 30 Absatz 1 Buchstabe b der Vorschläge besagt jedoch, dass eine gelbe Verknüpfung hergestellt wird, wenn die verknüpften Daten unterschiedliche Identitätsdaten enthalten und keine manuelle Verifizierung verschiedener Identitäten vorgenommen wurde. Diese Definition ist ziemlich verwirrend, denn sie impliziert, dass zwischen allen unterschiedlichen Daten von zwei oder mehr Informationssystemen eine gelbe Verknüpfung hergestellt würde. Dies würde auch bedeuten, dass von der zuständigen Behörde keine grüne Verknüpfung hergestellt werden könnte, da zuvor keine gelbe Verknüpfung hergestellt wurde. **Der EDSB vermutet, dass nicht „unterschiedliche Daten", sondern „ähnliche Daten" gemeint sind, und empfiehlt eine entsprechende Änderung von Artikel 30. Im Sinne der Klarheit empfiehlt er ferner, in Artikel 28 Absatz 4 und Artikel 30 der Vorschläge eine einheitliche Definition von „gelber Verknüpfung" zu geben.**

91 Die Herstellung einer gelben Verknüpfung löst das in Artikel 29 der Vorschläge geregelte Verfahren der manuellen Verifizierung aus. Gemäß Artikel 29 Absatz 1 der Vorschläge sollte die manuelle Verifizierung von der Behörde vorgenommen werden, die das persönliche Dossier angelegt oder aktualisiert hat. Gemäß Artikel 29 Absatz 2 der Vorschläge hingegen ist ausschließlich das Sirene-Büro zuständig, wenn eine gelbe Verknüpfung auf eine SIS-Ausschreibung verweist. Da das Sirene-Büro nicht zwangsläufig in die Anlage oder Aktualisierung eines Dossiers im Sinne von Artikel 29 Absatz 1 der Vorschläge eingebunden ist, ist nicht klar, ob und wie das Sirene-Büro über seine Verantwortung für die Verifizierung der verschiedenen Identitäten informiert werden könnte. **Der EDSB empfiehlt, in Artikel 29 der Vorschläge aufzunehmen, dass das zuständige Sirene-Büro unverzüglich informiert wird, wenn von ihm eine gelbe Verknüpfung manuell zu verifizieren ist.**

92 In diesem Zusammenhang hat der EDSB festgestellt, dass Artikel 29 der Vorschläge vorsieht, dass die zuständigen Behörden die relevanten Verknüpfungen unverzüglich zu aktualisieren haben, doch gibt es keine Bestimmungen für den Fall, dass eine zuständige Behörde ihrer Verantwortung nicht nachkommt. **Der EDSB empfiehlt daher die Einführung eines festen Zeitrahmens mit konkreten Fristen und die Festlegung eines klaren Verfahrens, das eine rechtzeitige Verifizierung gewährleistet, da solche Verknüpfungen für die betreffende(n) Person(en) möglicherweise nachteilige Folgen haben**.

93 Gemäß Artikel 29 Absatz 3 der Vorschläge soll die zuständige Behörde für die Verifizierung der Identität einer Person Zugang zur entsprechenden Identitätsbestätigungsdatei im MID und im Einklang mit Artikel 21 der Vorschläge zu den im CIR verknüpften Daten erhalten. Bezüglich des CIR stellt Artikel 21 der Vorschläge klar, dass ein Zugang nur zu den mit einer gelben Verknüpfung verbundenen Identitätsdaten gewährt werden sollte. Die zuständige Behörde hat dann die verschiedenen Identitäten zu prüfen und zu entscheiden, ob die Verknüpfung als grün, rot oder weiß einzustufen ist. Entscheidet die zuständige Behörde, eine weiße oder rote Verknüpfung herzustellen, werden die Daten im Einklang mit Artikel 19 Absatz 2 der Vorschläge der individuellen Datei im CIR hinzugefügt.

94 Gemäß Artikel 27 Absatz 1 Buchstabe e der Vorschläge tritt der MID in Aktion, wenn im SIS eine Ausschreibung erstellt oder aktualisiert wird. Artikel 26 Absatz 1 Buchstabe e und Artikel 29 Absatz 1 Buchstabe e der Vorschläge sehen jedoch vor, dass das Sirene-Büro nur Zugang zum MID erhält, wenn es eine Ausschreibung aktualisiert, nicht jedoch, wenn es eine Ausschreibung erstellt. **Nach Ansicht des EDSB handelt es sich hier um einen redaktionellen Fehler; er empfiehlt, die Artikel 26 und 29 der Vorschläge entsprechend zu ändern.**

95 Des Weiteren stellt der EDSB fest, dass die Vorschläge häufig von unterschiedlichen Identitätsdaten sprechen, die legaler- oder illegalerweise eine Person bezeichnen (Artikel 32 Absatz 1 Buchstaben a und b). **Da in den Vorschlägen nicht näher ausgeführt wird, wann eine Identität legaler- oder illegalerweise eine Person bezeichnet, empfiehlt der EDSB, die Bedeutung dieser Begriffe in den einschlägigen Bestimmungen oder zumindest in einem Erwägungsgrund abzuklären.**

96 Schließlich stellt der EDSB fest, dass die Vorschläge für eine betroffene Person die Möglichkeit der Berichtigung einer faktisch nicht korrekten Verknüpfung vorsehen, aber keine Möglichkeit für die Mitgliedstaaten planen, selber solche Verknüpfungen zu berichtigen.[39] Nach Meinung des EDSB würde ein solcher Mechanismus die Datenqualität in den entsprechenden Systemen weiter verbessern und damit dem angestrebten Ziel der Interoperabilität dienen. **Er empfiehlt daher, in die Vorschläge einen entsprechenden Mechanismus aufzunehmen, mit dessen Hilfe die Mitgliedstaaten selber eine nicht korrekt hergestellte Verknüpfung berichtigen können.**

4.7 Zentraler Speicher für Berichte und Statistiken - CRRS

97 Gemäß Artikel 39 der Vorschläge soll eu-LISA einen zentralen Speicher für Berichte und Statistiken einrichten, implementieren und hosten. Der EDSB verweist in diesem Zusammenhang auf seine früheren Stellungnahmen zum EES[40], ETIAS[41], SIS[42] und zu eu-LISA[43]. In diesen Stellungnahmen warnt der EDSB nachdrücklich davor, dass die für die Erstellung von Statistiken vorgeschlagene Lösung eine große Belastung für eu-LISA und den EDSB darstellen würde, denn eu-LISA müsste ein zweites Register pflegen und sichern, während der EDSB die Aufsicht über dieses zweite Register übernehmen müsste.

98 Der EDSB würde daher eine Lösung bevorzugen, die keinen weiteren Zentralspeicher erfordert, sondern stattdessen von eu-LISA verlangt, Funktionalitäten zu entwickeln, die

den Mitgliedstaaten, der Kommission, eu-LISA sowie befugten Behörden die Möglichkeit geben, die notwendigen Statistiken automatisch direkt aus dem System zu extrahieren.

99 Diesbezüglich unterstreicht der EDSB, dass eu-LISA vor der Implementierung des CRRS eine gründliche Abschätzung der Gefahren für die Informationssicherheit vornehmen und sich ferner mit der Frage sicherer Zugangspunkte beschäftigen sollte. Es kommt darauf an, dass vor der Einrichtung des CRRS angemessene Sicherheitsvorkehrungen getroffen werden.

100 Der EDSB sieht ein, dass ordnungsgemäß ermächtigtes Personal der zuständigen Behörden der Mitgliedstaaten, die Kommission und eu-LISA für Berichte und Statistiken und die Europäische Agentur für die Grenz- und Küstenwache für Gefährdungsabschätzungen und Gefährdungsbeurteilungen Zugang zu den im CIR und im MID gespeicherten Daten benötigen. Es sei jedoch angemerkt, dass im Gegensatz zu der Formulierung in Artikel 56 Absätze 2 und 3 der Vorschläge die Kombination von Staatsangehörigkeit, Geschlecht und Geburtsdatum einer Person durchaus zur deren Identifizierung führen kann.

101 **Der EDSB empfiehlt daher eine Umformulierung von Artikel 56 Absätze 2 und 3 der Vorschläge dahingehend, dass eingeräumt wird, dass die in Artikel 56 Absatz 2 Buchstaben a bis d und Absatz 3 Buchstaben a bis c aufgelisteten Daten zu einer Identifizierung von Personen führen können und daher geschützt werden müssen. Das bedeutet erneut, dass eine gründliche Abschätzung der Gefahren für die Informationssicherheit durchgeführt werden muss und angemessene Sicherheitsvorkehrungen getroffen werden müssen, bevor dieses weitere Zentralregister bereitgestellt wird. Der EDSB empfiehlt ferner, dass bei der Konzeption des CRRS der Grundsatz des Datenschutzes durch Technikgestaltung angewandt werden sollte.**

4.8 Einstufung von eu-LISA als Auftragsverarbeiter

102 Der EDSB hat bei verschiedenen Gelegenheiten auf die Implikationen der Rollenverteilung auf die verschiedenen Akteure in EU-Großdatenbanken hingewiesen und empfohlen, dass dort, wo ein Akteur unabhängig Zwecke und Mittel der Verarbeitung festlegt, er eher als für die Verarbeitung Verantwortlicher denn als Auftragsverarbeiter betrachtet werden sollte.[44] Ebenso gilt, dass für den Fall, dass mehrere Stellen über die Zwecke und/oder Mittel der Verarbeitung entscheiden, wie in diesem Vorschlag für eine Verordnung vorgesehen, sie als gemeinsam für die Verarbeitung Verantwortliche gelten sollten.

103 In Artikel 4 Absatz 7 der Verordnung 2016/679 ist der Verantwortliche definiert als eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Artikel 26 der Verordnung 2016/679 befasst sich mit dem Begriff der gemeinsamen Verantwortung für die Verarbeitung und besagt: Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Diese gemeinsam Verantwortlichen legen klar fest, wer von ihnen wofür verantwortlich ist, sofern dies nicht schon im Gesetz geregelt ist.

104 Die Artikel 29-Datenschutzgruppe hat 2010 eine Stellungnahme zu den Begriffen „für die Verarbeitung Verantwortlicher“, „Auftragsverarbeiter“ sowie „gemeinsame Verantwortung“ herausgegeben.[45] In ihrer Stellungnahme führte die Artikel 29-Datenschutzgruppe aus, dass der Begriff „für die Verarbeitung Verantwortlicher“ eine eigene Prägung des EU-Datenschutzrechts ist, und dass er funktionell ist, da er die Verantwortung entsprechend dem tatsächlichen Einfluss und damit auf der Grundlage einer faktischen anstelle einer formalen Analyse zuweist.

105 Artikel 40 der Vorschläge besagt, dass die mitgliedstaatlichen Behörden, die für die Verarbeitungen in den jeweiligen Quellsystemen verantwortlich sind, auch für die Verarbeitungen im gemeinsamen BMS und im CIR verantwortlich sind. Was die Verarbeitung von Daten im MID angeht, gelten die Europäische Agentur für die Grenz- und Küstenwache und Behörden der Mitgliedstaaten, die Daten der Datenbestätigungsdatei hinzufügen oder sie ändern, als für die Verarbeitung Verantwortliche im Sinne der Verordnung (EU) 2016/679. Artikel 41 des Vorschlags für eine Verordnung besagt, dass eu-LISA bei der Verarbeitung personenbezogener Daten im CIR als Auftragsverarbeiter im Sinne der Verordnung (EG) Nr. 45/2001 gilt.

106 Gemäß Artikel 52 der Vorschläge ist eu-LISA für die Entwicklung der Interoperabilitätskomponenten sowie für jegliche Anpassungen verantwortlich, die erforderlich sind, um die Interoperabilität zwischen den Zentralsystemen und dem Europäischen Suchportal, dem gemeinsamen BMS, dem CIR und dem MID herzustellen. Darüber hinaus legt eu-LISA die Architektur einschließlich der technischen Spezifikationen fest, wohingegen Vertreter von Mitgliedstaaten in einem Programmverwaltungsrat für eine angemessene Durchführung der Konzeptions- und Entwicklungsphase sorgen (Artikel 52 Absatz 4). Die technische Verwaltung der zentralen Infrastruktur übernimmt eu-LISA, die auch dafür verantwortlich ist, die Sicherheit der Interoperabilitätskomponenten und der mit ihnen verbundenen Kommunikationsinfrastruktur sicherzustellen (Artikel 53 Absatz 1 und Artikel 42 Absatz 2). In Zusammenarbeit mit den Mitgliedstaaten gewährleistet eu-LISA, dass die beste verfügbare Technologie eingesetzt wird (Artikel 53 Absatz 1), während eu-LISA einen Mechanismus für die Qualitätskontrolle entwickelt (Artikel 53 Absatz 3). Das zeigt, dass eu-LISA eine wichtige Rolle bei der Festlegung der Mittel der Verarbeitung spielen wird, und zwar sowohl bei der Erstentwicklung als auch im Betrieb.

107 Wie bereits erläutert, stützt sich das Konzept der Verantwortung für die Verarbeitung auf eine faktische Analyse. Die Zuweisung der Rollen in dem Vorschlag für eine Verordnung führt zu einer Situation, in der Mitgliedstaaten für Dinge verantwortlich sind, über die sie keine Kontrolle haben (z. B. die Frage, wie eu-LISA an die Informationssicherheit und die sichere Übermittlung der Daten an die und von den Datenbanken herangeht). Außerdem erhält eu-LISA Aufgaben (Entwicklung des Systems, Gewährleistung seiner Sicherheit während des Betriebs usw.), für deren Wahrnehmung sie laut den Vorschlägen größere Autonomie erhält als die eines Auftragsverarbeiters. **Wir empfehlen** daher, **eu-LISA und die zuständigen Behörden der Mitgliedstaaten zu gemeinsam Verantwortlichen zu machen und ihnen jeweils klar umrissene Aufgaben und Verantwortlichkeiten zuzuweisen**.

4.9 Sicherheit

108 Der EDSB hält fest, dass durch die Vorschläge EU-Großdatenbanken mit sensiblen Daten zusammengebracht werden. Es ist daher unerlässlich, dass diese Daten gegen potenzielle Angreifer und Sicherheitsvorfälle geschützt werden. Der EDSB empfiehlt eu-LISA und den Mitgliedstaaten nachdrücklich, in der Entwicklungs- und Implementierungsphase jedes neuen Systems und jeder Interoperabilitätskomponente den Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung zu beherzigen und darüber hinaus ein umfassendes Risikomanagement für Informationssicherheit (ISRM) zu betreiben.

109 Der EDSB unterstreicht die Bedeutung eines angemessenen Informationssicherheits-Risikomanagements gemäß Artikel 22 der Verordnung (EG) Nr. 45/2001 sowie gemäß der Leitlinien des EDSB. Der EDSB empfiehlt, im Vorschlag nicht von Sicherheit oder Sicherheitsplänen zu sprechen, sondern statt dessen die Formulierung „Implementierung eines umfassenden Informationssicherheits-Risikomanagements (ISRM)“ zu verwenden.

110 Gemäß Artikel 37 der Vorschläge soll mit automatischen Datenqualitätskontrollen ein Mindestmaß an Datenqualität für alle in den Systemen gespeicherten Daten gewährleistet werden. Der EDSB begrüßt die Einführung solcher automatischen Datenqualitätskontrollen. Liest man jedoch die Absätze 1 und 3 von Artikel 53 der Vorschläge zusammen, wird klar, dass eu-LISA einen Mechanismus für die Durchführung solcher Qualitätskontrollen erst nach Inbetriebnahme der neuen Systeme entwickeln wird.

111 **Der EDSB empfiehlt nachdrücklich, automatische Datenqualitätskontrollen so bald wie möglich einzuführen und sie am besten bereits vor der Inbetriebnahme zu testen.**

112 Nach Meinung des EDSB sollte sich eu-LISA in der Entwicklungsphase der Interoperabilitätskomponenten auch mit dem Thema Sicherheitsgovernance beschäftigen, da auf diese Weise sichergestellt wird, dass die dem Stand der Technik entsprechenden Sicherheitsmaßnahmen ergriffen werden.

113 Artikel 42 der Vorschläge enthält Bestimmungen betreffend die Sicherheit der Verarbeitung sowohl für eu-LISA als auch die Mitgliedstaaten. Nach Ansicht des EDSB sollte die technische Verantwortung für die Sicherheit der Interoperabilitätskomponenten unter Berücksichtigung der spezifischen architektonischen Gestaltung des Systems zwischen eu-LISA und den Mitgliedstaaten aufgeteilt werden. **Die Behörden der Mitgliedstaaten können zwar nicht die Verantwortung für das Zentralsystem übernehmen, doch können sie für die Sicherheit an den Endpunkten im Hinblick auf den Zugang zu den Systemen verantwortlich sein (Sicherheit ihrer nationalen Kommunikationsleitungen, Zugangskontrollen, Genehmigungen, Datenverarbeitung usw.). Der EDSB empfiehlt, Artikel 42 Absatz 1 der Vorschläge so zu ändern, dass diese Unterscheidung deutlich wird.**

114 Der EDSB erinnert daran, dass ein angemessener Sicherheitsplan, wie in Artikel 42 Absatz 3 der Vorschläge festgelegt, das Ergebnis einer gründlichen Abschätzung der Gefahren für die Informationssicherheit sein sollte, weshalb in Artikel 42 Absatz 3 der Vorschläge ein entsprechender Verweis erfolgen sollte. In dem Sicherheitsplan sollten

ferner die Verantwortlichkeiten und Sicherheitsanforderungen für die einzelnen Beteiligten genau festgelegt werden. Es sei ganz allgemein daran erinnert, dass sich eine hohe Informationssicherheit nur durch eine gründliche Abschätzung der Gefahren für die Informationssicherheit erreichen lässt, denen ein Informationssystem ausgesetzt ist.

115 Wie in Artikel 42 Absatz 3 Buchstabe i der Vorschläge zum Ausdruck kommt, müssen die Sicherheitsmaßnahmen durch eu-LISA überwacht werden, die auch die erforderlichen organisatorischen Maßnahmen zu ergreifen hat. **Der EDSB schlägt vor, diese Bestimmung zu verstärken, damit ein Sicherheitsgovernance-System aufgebaut werden kann, das die angewandten Sicherheitsmaßnahmen auch unter Berücksichtigung technologischer Entwicklungen beurteilen kann.**

4.10 Rechte der betroffenen Person

116 Der EDSB nimmt zur Kenntnis, dass die Vorschläge im Hinblick auf die Rechte der betroffenen Person auf die Verordnung (EG) Nr. 45/2001 und die Verordnung (EU) 2016/679 verweisen. Allerdings sind das Hauptziel des ECRIS und teilweise des SIS die Strafverfolgung und die justizielle Zusammenarbeit, für die die Richtlinie 2016/680 anzuwenden ist. In diesem Zusammenhang empfiehlt der EDSB, in Artikel 46 der Vorschläge einen Verweis auf Artikel 13 der Richtlinie 2016/680 und in Artikel 47 der Vorschläge einen Verweis auf die Artikel 14 und 16 der Richtlinie 2016/680 aufzunehmen.

117 Artikel 46 der Vorschläge besagt, dass die zuständigen Behörden die betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten im gemeinsamen BMS, im CIR und im MID, ihren Zweck, die Identität und die Kontaktdaten des für die Verarbeitung Verantwortlichen, über die Verfahren für die Ausübung ihrer Datenschutzrechte sowie über die Kontaktdaten des EDSB und der nationalen Aufsichtsbehörde informieren sollten. Der EDSB begrüßt, dass betroffene Personen über das Vorliegen illegaler Mehrfachidentitäten in Kenntnis gesetzt werden (siehe Artikel 32 Absatz 4 der Vorschläge). Er nimmt allerdings zur Kenntnis, dass die vorgeschlagenen Einschränkungen des Rechts betroffener Personen auf Information nicht im Einklang mit Artikel 13 Absatz 3 der Richtlinie (EU) 680/2016 stehen. **Er empfiehlt daher eine Angleichung von Artikel 32 Absatz 4 der Vorschläge an Artikel 13 Absatz 3 der Richtlinie (EU) 680/2016.**

118 Nach Meinung des EDSB ist es zwingend erforderlich, dass betroffene Personen auch über die Speicherfrist ihrer Daten informiert werden, also darüber, dass die Speicherfrist in den einschlägigen Verordnungen geregelt ist, wie in Artikel 13 Absatz 2 Buchstabe a der Verordnung 2016/679 und Artikel 13 Absatz 2 Buchstabe b der Richtlinie 680/2016. Da der automatische Prozess der Herstellung von Verknüpfungen zum Zweck der Aufdeckung von Mehrfachidentitäten eine automatisierte Entscheidungsfindung ist, sollten betroffene Personen auch hierüber unterrichtet werden (siehe Artikel 13 Absatz 2 Buchstabe f der Verordnung 2016/679). Des Weiteren ist der EDSB der Meinung, dass betroffene Personen auch über die Empfänger ihrer Daten sowie im Einklang mit Artikel 48 der Vorschläge darüber informiert werden sollten, dass ihre in Interoperabilitätskomponenten gespeicherten oder von dort abgerufenen Daten nicht an Drittländer, internationale Organisationen oder private Stellen übermittelt oder diesen zur Verfügung gestellt werden; eine Ausnahme sind Übermittlungen an Interpol, wie in

Artikel 13 Absatz 1 Buchstabe f DSGVO und Artikel 13 Absatz 2 Buchstabe c der Richtlinie 680/2016 geregelt.

119 **Der EDSB empfiehlt daher, in Artikel 46 der Vorschläge aufzunehmen, dass die betroffenen Personen auch über die jeweiligen Speicherfristen, die automatisierte Entscheidungsfindung und die Tatsache informiert werden sollten, dass personenbezogene Daten (mit Ausnahme der Übermittlungen an Interpol) nicht an Drittländer, internationale Organisationen oder private Stellen übermittelt oder ihnen zur Verfügung gestellt werden.**

120 Der EDSB stellt fest, dass es in Artikel 47 Absatz 1 der Vorschläge zum Recht betroffener Personen auf Auskunft, Berichtigung und Löschung heißt, dass die betroffene Person ihren Antrag an irgendeinen Mitgliedstaat richten kann, der den Antrag prüft und beantwortet.

121 Hierzu merkt der EDSB an, dass für den Fall, dass eine Person einen Antrag bei irgendeinem Mitgliedstaat stellt, wie in Artikel 47 Absatz 1 der Vorschläge vorgesehen, dieser Mitgliedstaat dann prüfen müsste, welches der für die manuelle Verifizierung zuständige Mitgliedstaat ist. Da jedoch in Artikel 13 Absatz 2 und Artikel 18 Absatz 2 der Vorschläge nur von dem betreffenden System die Rede ist, nicht jedoch von dem zuständigen Mitgliedstaat, schränkt Artikel 26 Absatz 2 diesbezüglich den Zugang des Mitgliedstaats zur Identitätsbestätigungsdatei ein. Daher **empfiehlt der EDSB, in Artikel 13 Absatz 2 und Artikel 18 Absatz 2 der Vorschläge einen Verweis auf den zuständigen Mitgliedstaat und mit Blick auf Artikel 26 Absatz 2 der Vorschläge einen Verweis auf Artikel 34 Buchstabe d aufzunehmen. Auf diese Weise wäre sichergestellt, dass die betroffene Person ihre Rechte tatsächlich ausüben kann**.

122 Mit Blick auf Artikel 47 Absatz 3 der Vorschläge stellt der EDSB fest, dass in diesem Absatz zwar vom Recht auf Berichtigung und vom Recht auf Löschung die Rede ist, nicht hingegen vom Recht auf Auskunft. **Der EDSB empfiehlt, das Recht auf Auskunft in Artikel 47 Absatz 3 der Vorschläge aufzunehmen.**

123 Während in Artikel 47 Absatz 3 der Vorschläge vorgesehen ist, dass ein Antrag auf Berichtigung oder Löschung von einem Mitgliedstaat an den zuständigen Mitgliedstaat weitergeleitet werden sollte, gibt es keine entsprechende Bestimmung bezüglich des Rechts auf Auskunft. **Der EDSB empfiehlt, in Artikel 47 der Vorschläge einen Absatz aufzunehmen, in dem der Mitgliedstaat dazu verpflichtet wird, den Antrag auf Auskunft an den zuständigen Mitgliedstaat weiterzuleiten.**

124 Des Weiteren **empfiehlt der EDSB, in Artikel 47 der Vorschläge die Verpflichtung für die Mitgliedstaaten aufzunehmen, die betroffene Person darüber zu informieren, dass ihr Antrag weitergeleitet wurde und dabei die Kontaktdaten der in dem betreffenden Mitgliedstaat zuständigen Behörde anzugeben**. Auf diese Weise könnte die betroffene Person die zuständige Behörde leichter ermitteln und hätte die betroffene Person die Möglichkeit, weitere Anträge unmittelbar an die zuständige Behörde zu richten.

125 **Im Hinblick auf Artikel 47 Absatz 4 der Vorschläge empfiehlt der EDSB, die Verpflichtung für die Mitgliedstaaten vorzusehen, die betroffene Person unverzüglich von einer Berichtigung oder Löschung ihrer Daten zu unterrichten.**

126 Schließlich weist der EDSB darauf hin, dass die Interoperabilitätskomponenten in ihrer Anlaufphase im Wesentlichen Daten verarbeiten werden, die zu dem Zeitpunkt bereits in dem jeweiligen System gespeichert sind. Damit stellt sich die Frage, wie die für die Verarbeitung Verantwortlichen betroffenen Personen vor der Verarbeitung Informationen zukommen lassen können. **Der EDSB empfiehlt, in den Mitgliedstaaten und auf EU-Ebene eine angemessene Sensibilisierungskampagne durchzuführen, bevor die Interoperabilitätskomponenten implementiert werden und vollumfänglich in Betrieb gehen.**

4.11 Zugang durch Bedienstete von eu-LISA

127 Artikel 68 Absatz 3 der Vorschläge sieht vor, dass eu-LISA Zugang zu allen für technische Wartungszwecke erforderlichen Daten erhält. Da eu-LISA Systemanbieter und Administrator aller Systeme und der Interoperabilitätskomponenten ist, sieht der EDSB ein, dass eu-LISA Zugang zu in den Systemen gespeicherten personenbezogenen Daten haben muss.

128 **Der EDSB empfiehlt jedoch, in Artikel 68 Absatz 3 der Vorschläge zu betonen, dass eu-LISA nur unter strengen Garantien und für rechtmäßige und konkrete Zwecke Zugang zu personenbezogenen Daten erhalten sollte. Diesbezüglich sollten die Vorschläge klar einschlägige Situationen festlegen, in denen eu-LISA legal auf personenbezogene Daten zugreifen darf, wenn beispielsweise ein Mitgliedstaat eu-LISA um ein Eingreifen bei der Abstimmung von Daten (insbesondere bei biometrischen Daten) oder um Unterstützung usw. bittet. Der EDSB fordert daher eine nähere Erkundung dieser Umstände und – falls erforderlich – eine entsprechende Abänderung der Vorschläge.**

129 **Der EDSB unterstreicht ferner, dass jeder Zugriff durch eu-LISA protokolliert werden sollte, und empfiehlt nachdrücklich, eine entsprechende Bestimmung in die Vorschläge aufzunehmen.**

4.12 Übergangszeitraum

130 Nach dem Verständnis des EDSB werden gemäß den Erwägungsgründen 21 und 22 und Artikel 17 Absatz 2 der Vorschläge im CIR die personenbezogenen Daten (biografische und biometrische Daten) von Drittstaatsangehörigen aus dem EES, dem VIS, Eurodac, dem ETIAS und ECRIS-TCN gespeichert. Fest steht auch, dass diese Daten nicht in den genannten Systemen verbleiben würden, da das CIR *„eine zentrale Infrastruktur“* sein wird, *„die die Zentralsysteme ersetzt“*.

131 Den Plänen der Kommission und der Machbarkeitsstudie über das CIR zufolge würde für einen gewissen Zeitraum ein Hybridsystem bestehen. Es würden also im CIR gespeicherte Daten in den zugrunde liegenden Systemen verbleiben, um ein reibungsloses Funktionieren des neuen Systems zu gewährleisten. Das bedeutet, dass für einen nicht befristeten Zeitraum die Daten doppelt gespeichert würden.

132 **Der EDSB räumt ein, dass ein solcher Zeitraum notwendig ist, meint jedoch, dass die Hybridlösung in den Artikel über den Übergangszeitraum der Vorschläge**

eingehen sollte und dort deutlich gemacht werden sollte, dass diese Hybridlösung nur für einen begrenzten Zeitraum bestehen sollte.

4.13 Protokolle

133 Der EDSB begrüßt, dass die Interoperabilitätskomponenten für Zwecke des Datenschutzes und des Monitoring Protokolle speichern werden. **Er empfiehlt jedoch, in die Vorschläge auch Bestimmungen aufzunehmen, in denen geregelt wird, wer Zugang zu den Protokollen hat und wie dieser Zugang gewährt wird**, da der einschlägige Artikel 42 der Vorschläge keine näheren Informationen zur Verwaltung dieser Protokolle und zum Zugang zu ihnen enthält.

134 Der EDSB nimmt zur Kenntnis, dass gemäß Artikel 10 Absatz 1 und Artikel 16 Absatz 1 der Vorschläge Protokolle aller Verarbeitungsvorgänge im ESP und im gemeinsamen BMS zentral bei eu-LISA aufbewahrt werden. Dessen ungeachtet sind gemäß Artikel 45 der Vorschläge die für die Verarbeitung Verantwortlichen verpflichtet, die erforderlichen Maßnahmen zur Überwachung der Einhaltung der Vorschriften bei der Datenverarbeitung zu treffen und erforderlichenfalls mit den in den Artikeln 49 und 50 der Vorschläge genannten Aufsichtsbehörden zusammenzuarbeiten.

135 Da weder die Mitgliedstaaten als für die Verarbeitung Verantwortliche (siehe Artikel 40) noch die nationalen Aufsichtsbehörden Zugang zu den Protokollen des ESP und des gemeinsamen BMS haben, kommt der EDSB zu dem Schluss, dass eine angemessene Verifizierung oder Kontrolle des ESP und des gemeinsamen BMS nicht möglich ist.

136 **Der EDSB empfiehlt daher, die Protokolle des ESP und des gemeinsamen BMS auch auf nationaler Ebene zu speichern, so wie dies mit den Protokollen des CIR (Artikel 24 Absatz 5) und des MID (Artikel 36 Absatz 2) geschieht.**

4.14 Nationale Aufsichtsbehörden

137 Gemäß Artikel 49 der Vorschläge sollten die nationalen Aufsichtsbehörden gewährleisten, dass mindestens alle vier Jahre die Datenverarbeitungsvorgänge der zuständigen nationalen Behörden nach den einschlägigen internationalen Prüfungsstandards überprüft werden. Nicht vorgesehen in den Vorschlägen ist jedoch die Kontrolle der Rechtmäßigkeit der Verarbeitung personenbezogener Daten nach diesen Vorschlägen durch die nationalen Aufsichtsbehörden; vielmehr ist in Artikel 45 von einer Eigenkontrolle durch die für die Verarbeitung Verantwortlichen selber die Rede.

138 **Der EDSB empfiehlt nachdrücklich die Aufnahme einer Bestimmung, der zufolge jeder Mitgliedstaat zu gewährleisten hat, dass die gemäß Artikel 51 der Verordnung (EU) 2016/679 und Artikel 41 der Richtlinie (EU) 2016/680 benannten Aufsichtsbehörde(n) die Rechtmäßigkeit der Verarbeitung personenbezogener Daten im Einklang mit den vorgeschlagenen Verordnungen zu kontrollieren hat/haben.**

139 **Der EDSB empfiehlt, in Artikel 44 Absatz 3 der Vorschläge die nationale Aufsichtsbehörde hinzuzufügen.**

4.15 Rolle des EDSB

140 Der EDSB ist die für die Aufsicht über eu-LISA zuständige Datenschutzbehörde. Damit der EDSB im Rahmen seiner Zuständigkeiten eu-LISA wirksam beaufsichtigen kann, sollte er seiner Auffassung nach in die Liste der Empfänger der Berichte aufgenommen werden, die eu-LISA gemäß Artikel 68 Absätze 2 und 4 der Vorschläge zu veröffentlichen hat.

141 Ferner weist der EDSB erneut darauf hin, dass eine Aufsicht nur wirksam sein kann, wenn für sie angemessene Ressourcen bereitstehen. Zwar sieht Artikel 49 Absatz 2 der Vorschläge vor, dass die nationalen Aufsichtsbehörden über ausreichende Ressourcen zur Wahrnehmung ihrer Aufgaben verfügen sollten, die ihnen gemäß dieser Verordnung übertragen werden, doch **empfiehlt der EDSB, in Artikel 50 eine ähnliche Bestimmung aufzunehmen, damit für ihn angemessene Ressourcen zur Verfügung gestellt werden**.

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 Schwerkriminellen 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,

Giovanni BUTTARELLI

Endnoten

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 119 vom 4.5.2016, S. 1.
[3] ABl. L 8 vom 12.1.2001, S. 1.
[4] ABl. L 350 vom 30.12.2008, S. 60.
[5] ABl. L 119 vom 4.5.2016, S. 89.
[6] 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.
[7] a.a.O., S. 17.
[8] 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
[9] 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.
[10] 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.
[11] Schlussfolgerungen des Rates zum weiteren Vorgehen zur Verbesserung des 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.
[12]Öffentliche Konsultation und Folgenabschätzung sind abrufbar unter: https://ec.europa.eu/home-affairs/content/consultation-interoperability-eu-information-systems-borders-and-security_en.
[13] https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_de.pdf.
[14] Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (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, ABI. L 327 vom 9.12.2017, S. 20.
[15] 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.
[16] 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.
[17] 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.
[18] Erklärung des Europäischen Datenschutzbeauftragten zum Konzept der Interoperabilität im Bereich Migration, Asyl und Sicherheit, im Anhang zum Abschlussbericht der von der Europäischen Kommission eingesetzten hochrangigen Expertengruppe für Informationssysteme und Interoperabilität, 11. Mai 2017; abrufbar unter http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435
[19] Siehe beispielsweise den Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten, ABl. L 218 vom 13.8.2008, S. 129; die Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer

Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (Neufassung), ABl. L 180 vom 29.6.2013, S. 1.

[20] Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (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; Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts.

[21]Verordnung (EU) 2016/1624 des Europäischen Parlaments und des Rates vom 14. September 2016 über die Europäische Grenz- und Küstenwache und zur Änderung der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Verordnung (EG) Nr. 863/2007 des Europäischen Parlaments und des Rates, der Verordnung (EG) Nr. 2007/2004 des Rates und der Entscheidung des Rates 2005/267/EG.

[22] Eine Ausnahme bildet das ECRIS-TCN, das für Zwecke der justiziellen Zusammenarbeit eingerichtet wurde.

[23] Folgenabschätzung, S. 9f.

[24] Folgenabschätzung, S. 39.

[25] EuGH, *Digital Rights Ireland Ltd*, Rechtssache C-293/12, Urteil vom 8. April 2014, Rn. 60.

[26] EuGH, *Digital Rights Ireland Ltd*, Rechtssache C-293/12, Urteil vom 8. April 2014, Rn. 61.

[27] EuGH, *Digital Rights Ireland Ltd*, Rechtssache C-293/12, Urteil vom 8. April 2014, Rn. 61.

[28] Vorschlag für eine Verordnung 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) 0344 final.

[29] Siehe Folgenabschätzung, S. 39.

[30] Vorschlag für eine Verordnung 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) 0344 final.

[31] Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für einen Beschluss des Rates über den Zugang der für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Prävention, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten, (KOM(2005) 600 endg.), abrufbar unter https://edps.europa.eu/sites/edp/files/publication/06-01-20_access_vis_de.pdf, Stellungnahme des Europäischen Datenschutzbeauftragten zum geänderten Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von „EURODAC“ für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EG) Nr. (…/…) (zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist) und zum Vorschlag für einen Beschluss des Rates über die Beantragung eines Abgleichs mit EURODAC-Daten durch Strafverfolgungsbehörden der Mitgliedstaaten und Europol zu Strafverfolgungszwecken, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/09-10-07_access_eurodac_de.pdf; Stellungnahme 06/2016 zum zweiten Paket „Intelligente Grenzen“ der EU; Empfehlungen betreffend den überarbeiteten Vorschlag zur Einrichtung eines Einreise-/Ausreisesystems, S. 19-20, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_de.pdf, Stellungnahme 3/2017 zu dem Vorschlag für ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS), S. 13, abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_de.pdf.

[32] Folgenabschätzung, S. 25 und 43.

[33] Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität.

[34] Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität.

[35] 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, ABl. L 119 vom 4.5.2016, S. 1.

[36] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, COM(2017) 8 final.
[37] Siehe S. 12 der Begründung, COM(2016) 793 final.
[38] Siehe Erwägungsgrund 71 DSGVO.
[39] Siehe zum Beispiel Artikel 34 Absatz 3 der SIS II-Verordnung.
[40] https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_de.pdf.
[41] https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_de.pdf.
[42] https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_de.pdf.
[43] https://edps.europa.eu/sites/edp/files/publication/17-10-10_eu-lisa_opinion_de_0.pdf.
[44] EDSB, Stellungnahme 6/2016 zum zweiten Paket „Intelligente Grenzen“, Punkt 70, oder EDSB, Stellungnahme 11/2017 zu dem Vorschlag für eine Verordnung über ECRIS-TCN, Punkt 42.
[45] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf.