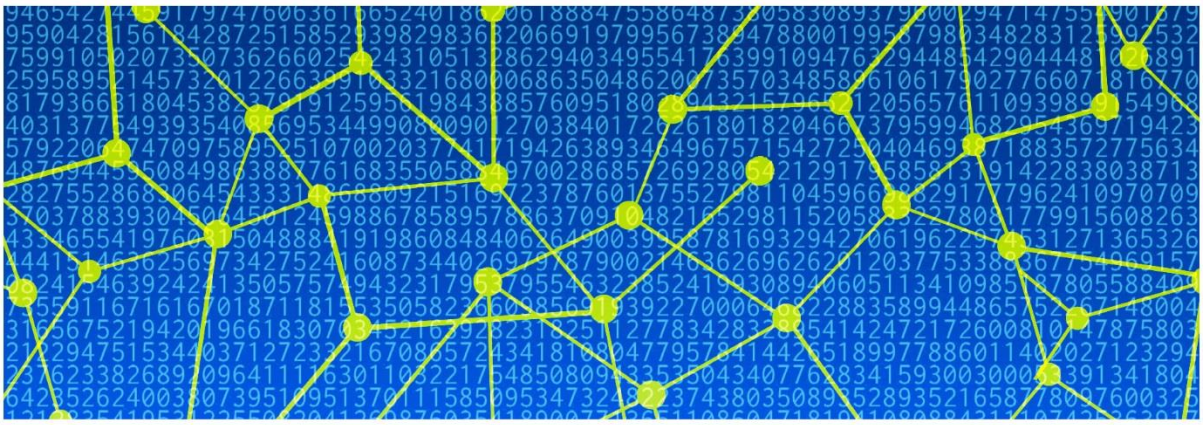

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 06/2016

Stellungnahme des EDSB zum zweiten Paket „Intelligente Grenzen“ der EU

Empfehlungen betreffend den überarbeiteten Vorschlag zur Einrichtung eines Einreise-/Ausreisesystems

EDPS

21. September 2016

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 der 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". Nach Auffassung des EDSB wird die Einhaltung der Datenschutzvorschriften über den Erfolg des überarbeiteten Pakets „Intelligente Grenzen" und des Informationsaustausches über Ein- und Ausreisen von Drittstaatsangehörigen über das Einreise-/Ausreisesystem entscheiden.

Zusammenfassung

Schon seit langem hat der EU-Gesetzgeber die Einrichtung eines Einreise-/Ausreisesystems (EES) zur Registrierung von Ein- und Ausreisen von Drittstaatsangehörigen im Hoheitsgebiet der Europäischen Union erwogen. Die Kommission verabschiedete drei Vorschläge als Teil des ersten Pakets „Intelligente Grenzen“ im Jahr 2013; die Mitgesetzgeber äußerten schwere Bedenken, und es konnte keine Einigung über das Paket erzielt werden. Daraufhin führte die Kommission aufgrund dieser Bedenken einen Konzeptnachweis durch und legte in diesem Jahr ein zweites Paket „Intelligente Grenzen“ vor, das nunmehr aus zwei überarbeiteten Vorschlägen besteht.

Der EDSB hat diese Vorschläge sorgfältig geprüft und als Hilfestellung für den Gesetzgeber Empfehlungen formuliert, mit denen sichergestellt werden soll, dass der Rechtsrahmen für die EES-Regelung vollkommen im Einklang mit dem Recht auf Privatsphäre und dem Datenschutzrecht in der EU, insbesondere mit den Artikeln 7 und 8 der EU-Charta der Grundrechte, steht.

Der EDSB räumt ein, dass Bedarf an kohärenten und wirksamen Informationssystemen für Grenzen und Sicherheit besteht. Diese Vorschläge werden zu einem kritischen Zeitpunkt vorgelegt, zu dem die EU in diesem Bereich vor ernstzunehmenden Herausforderungen steht. Der EDSB unterstreicht jedoch, dass die vorgeschlagene Verarbeitung personenbezogener Daten im Rahmen der EES-Regelung möglicherweise einen erheblichen Eingriff in die Privatsphäre darstellt und daher aus dem Blickwinkel sowohl von Artikel 7 als auch Artikel 8 der Charta zu prüfen ist. Notwendigkeit und Verhältnismäßigkeit der EES-Regelung sind sowohl insgesamt, unter Berücksichtigung der bereits in der EU bestehenden IT-Großsysteme, als auch spezifisch, für jeden Einzelfall dieser Drittstaatsangehörigen, zu bewerten, die ja rechtmäßige Besucher der EU sind. Der EDSB stellt fest, dass EES-Daten zu zwei verschiedenen Zwecken verarbeitet werden sollen, nämlich einerseits zu Zwecken des Grenzmanagements und der Erleichterung des Grenzübertritts und andererseits zu Strafverfolgungszwecken. Der EDSB empfiehlt nachdrücklich, schon im EES-Vorschlag von 2016 durchgängig zwischen diesen Zielsetzungen zu differenzieren, da sie unterschiedliche Auswirkungen auf das Recht auf Privatsphäre und auf Datenschutz haben.

Zwar begrüßt der EDSB, dass den früher geäußerten Bedenken bezüglich des Schutzes der Privatsphäre und des Datenschutzes Aufmerksamkeit geschenkt wird und die überarbeiteten Vorschläge besser geworden sind, doch hegt er schwere Bedenken bezüglich mehrerer Aspekte des EES-Vorschlags, die vom Gesetzgeber besser begründet oder sogar nochmals überdacht werden sollten; dazu gehören insbesondere folgende Elemente:

- die fünfjährige Speicherfrist für EES-Daten. Nach Ansicht des EDSB sollte die Notwendigkeit der Speicherung der Daten von Overstayern für fünf Jahre besser nachgewiesen werden und dürfte eine Speicherfrist von fünf Jahren für alle im EES gespeicherten personenbezogenen Daten unverhältnismäßig sein;

- die Speicherung des Gesichtsbilds von visumspflichtigen Reisenden, deren Gesichtsbild bereits im VIS gespeichert ist;

- die Notwendigkeit des Zugriffs von Gefahrenabwehr- und Strafverfolgungsbehörden auf EES-Daten, für die keine hinreichend überzeugenden Anhaltspunkte genannt werden;

- die Bedingung, der zufolge eine betroffene Person bei der Ausübung ihres Rechts auf Auskunft über ihre gespeicherten Daten und deren Berichtigung und/oder Löschung ihre Fingerabdrücke abnehmen lassen muss, woraus ein ernstzunehmendes Hindernis für die wirksame Ausübung dieser Rechte entstehen könnte.

In der Stellungnahme werden zudem weitere Empfehlungen für den Datenschutz und den Schutz der Privatsphäre formuliert, die im Gesetzgebungsverfahren aufgegriffen werden sollten und auch die Sicherheit des Systems betreffen.

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],

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[2], 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[3] –,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG UND HINTERGRUND

1. Zum ersten Mal kündigte die Kommission ihre Absicht, ein europäisches Einreise-/Ausreisesystem für die Kontrolle von Ein- und Ausreisen von Drittstaatsangehörigen im Hoheitsgebiet der Europäischen Union einzurichten, im Jahr 2008 an.[4] Seinerzeit gab der EDSB zunächst vorläufige Kommentare[5] zu dieser Absicht ab und ging dann in einer Stellungnahme vom Juli 2011[6] auf konkrete Einzelfragen ein. Die Kommission führte ihre Überlegungen näher in einer Mitteilung[7] mit dem Titel *„Intelligente Grenzen: Optionen und weiteres Vorgehen“* vom Oktober 2011 aus, zu der die Artikel 29-Datenschutzgruppe Kommentare abgab[8]. Auch der EDSB äußerte sich, und zwar in einer Diskussionsrunde mit verschiedenen Interessenträgern.[9]

2. Im Februar 2013 verabschiedete die Kommission drei Vorschläge als Teil des ersten Pakets „Intelligente Grenzen“, nämlich einen Vorschlag über ein Einreise-/Ausreisesystem[10] (nachstehend „EES-Vorschlag von 2013“), einen Vorschlag über ein Registrierungsprogramm für Reisende[11] (nachstehend „RTP-Vorschlag von 2013“) und einen Vorschlag zur Änderung des Schengener Grenzkodex[12] zur Einführung dieser Änderungen. Das Paket rief sofort Kritik von Seiten der beiden Mitgesetzgeber hervor, und zwar wegen technischer, operativer und die Kosten betreffender Bedenken, aber auch wegen erheblicher Datenschutzbedenken. Im gleichen Jahr formulierte der EDSB seine ersten konkreten Empfehlungen zu den drei Vorschlägen in Form einer Stellungnahme.[13] Auch die Artikel 29-Datenschutzgruppe legte eine Stellungnahme[14] vor, zu der der EDSB ebenfalls einen Beitrag leistete, und in der die Notwendigkeit eines Einreise-/Ausreisesystem als solchem hinterfragt wurde.

3. Anfang 2014 kündigte die Kommission als Reaktion auf diese Bedenken die Durchführung eines Konzeptnachweises in zwei Stufen an: Zunächst sollten eine Technische Studie[15] und eine Studie zu den Kosten[16] durchgeführt werden, um die passendsten Optionen

und Lösungen für die Einführung intelligenter Grenzen zu finden, auf die dann im Verlauf des Jahres 2015 ein Pilotprojekt[17] unter der Leitung der Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (nachstehend „eu-LISA“) folgen sollte, bei dem die ermittelten Optionen getestet werden sollten. Parallel hierzu leitete die Kommission im Juli 2015 eine dreimonatige öffentliche Konsultation[18] ein, mit der Ansichten und Meinungen von Bürgern und Organisationen eingeholt werden sollten, und an der sich auch der EDSB beteiligte[19].

4. Am 6. April 2016 legte die Kommission ein zweites Paket „Intelligente Grenzen“ vor.[20] Dieses Mal wird nur ein System vorgeschlagen, nämlich das Einreise-/Ausreisesystem (nachstehend „EES“). Die Kommission beschloss, ihren EES-Vorschlag von 2013 und den Vorschlag von 2013 zur Änderung des Schengener Grenzkodex zu überarbeiten, zog jedoch ihren RTP-Vorschlag von 2013 zurück. Das derzeitige Paket „Intelligente Grenzen“ setzt sich aus folgenden Bestandteilen zusammen:

- einer Mitteilung „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“[21];
- einem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten der Europäischen Union und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung der Verordnung (EG) Nr. 767/2008 und der Verordnung (EU) Nr. 10777/2011[22] (nachstehend „EES-Vorschlag von 2016“), und
- einem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 399/2016[23] in Bezug auf die Nutzung des Einreise-/Ausreisesystems[24] (nachstehend „Vorschlag von 2016 zur Änderung des Schengener Grenzkodex“).

5. Den beiden Vorschlägen beigefügt ist eine detaillierte Folgenabschätzung.[25]

6. Neue Impulse für das Paket „Intelligente Grenzen“ haben sich aus der aktuellen Migrationskrise und den jüngsten Terroranschlägen in Europa ergeben. Der niederländische und der slowakische Ratsvorsitz kündigten intensive Arbeiten an dem Paket mit dem Ziel an, bis Ende 2016 hierzu eine politische Einigung zu erzielen.[26]

7. Der EDSB begrüßt, dass er vor der Annahme der neuen Vorschläge von der Kommission informell konsultiert wurde. Ferner begrüßt er die gute Zusammenarbeit[27] zwischen der GD HOME und dem EDSB während der gesamten Überarbeitung des ersten Pakets „Intelligente Grenzen“.

2. ZIEL DER VORSCHLÄGE

8. Der Vorschlag für das EES kommt zu einem kritischen Zeitpunkt, an dem die EU im Hinblick auf ihre Grenzkontrollen und ihre Sicherheit vor ernstzunehmenden Herausforderungen steht. Das EES wird bereits existierende IT-Großsysteme der EU für Asylbewerber und Antragsteller auf ein Visum ergänzen. Vor diesem Hintergrund dient der **EES-Vorschlag von 2016** einer Verbesserung des Managements der EU-Außengrenzen und

einer Verringerung der irregulären Migration, indem gegen Überschreitungen der zulässigen Aufenthaltsdauer („Overstaying“) vorgegangen wird.[28] Ein Blick auf Stempel in Reisedokumenten ist derzeit die einzige den Grenzschutzbeamten und Einwanderungsbehörden zur Verfügung stehende Methode für die Berechnung der Aufenthaltsdauer von Drittstaatsangehörigen und zur Überprüfung der Frage, ob diese ihre zulässige Aufenthaltsdauer überzogen haben. Zu diesem Zweck findet der Vorschlag Anwendung auf legal in die EU eingereiste Drittstaatsangehörige. Nach dem Verständnis des EDSB bestimmen die Umstände der Einreise eines Drittstaatsangehörigen in die EU darüber, ob seine Daten im EES oder in der Eurodac-Datenbank gespeichert werden: Die Daten von Personen, die legal über eine offizielle Grenzübergangsstelle für einen Kurzaufenthalt (also höchsten 90 Tage innerhalb eines beliebigen Zeitraums von 180 Tagen) im Schengen-Raum einreisen, werden im EES gespeichert, während die Daten von Drittstaatsangehörigen, die Asyl beantragen oder illegal in die EU einreisen oder illegal eingereist sind und in der EU aufgefunden werden, in Eurodac gespeichert werden. Das EES erhebt ihre personenbezogenen Daten, einschließlich biometrischer Daten, und vermerkt Zeitpunkt und Ort ihrer Ein- und Ausreisen. Das System wird auch Einreiseverweigerungen erfassen.

9. Darüber hinaus soll das EES zur Verhütung, Aufdeckung und Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten beitragen und zur Identifizierung und Erkenntnisgewinnung dienen.

10. Zu den wichtigsten Änderungen, die im EES-Vorschlag von 2016 im Vergleich zum EES-Vorschlag von 2013 vorgenommen wurden, gehören eine längere Speicherfrist von fünf Jahren für *alle* EES-Daten, der Zugriff für Gefahrenabwehr- und Strafverfolgungsbehörden ab der Inbetriebnahme des Systems, die Spezifizierung der verwendeten biometrischen Identifikatoren und die Interoperabilität mit dem Visa-Informationssystem (nachstehend „VIS“) über einen direkten Kommunikationskanal zwischen beiden Datenbanken.

11. Mit dem **Vorschlag von 2016 zur Änderung des Schengener Grenzkodex** sollen die sich aus dem EES-Vorschlag von 2016 ergebenden technischen Änderungen in den Schengener Grenzkodex aufgenommen werden, insbesondere die Erfassung im EES von Einreiseverweigerungen für Drittstaatsangehörige, die Ausweichverfahren für das EES und die Interoperabilität zwischen EES und VIS. Der Vorschlag von 2016 sieht ferner die neue Möglichkeit für Mitgliedstaaten vor, freiwillig nationale Programme für Erleichterungen des Grenzübertritts einzuführen.

3. ANALYSE DER VORSCHLÄGE

I. Auswirkungen des EES auf Privatsphäre und Datenschutz

12. In Anbetracht der erheblichen Herausforderungen durch Migration, vor denen die EU steht, erkennt der EDSB die Notwendigkeit eines Tätigwerdens der EU an. Dieses Tätigwerden muss jedoch vollumfänglich unter Wahrung des EU-Rechtsrahmens geschehen. Die vorgeschlagene EES-Regelung findet Anwendung auf Drittstaatsangehörige, die legal als Besucher eingereist sind. Der Gesetzgeber hat unter anderem ihre in Artikel 7 und 8 der EU-Charta der Grundrechte (nachstehend „Charta“) verankerten Grundrechte auf Privatsphäre und Datenschutz zu wahren; es sind beide Artikel anzuwenden, da zur EES-Regelung auch die Erfassung, Speicherung und Verwendung sie betreffender personenbezogener Daten in erheblichem Umfang gehören.

13. Grundsätzlich ist eine solche Verarbeitung mit den durch die Charta geschützten Grundrechten vereinbar, sofern die in Artikel 52 Absatz 1 der Charta genannten Bedingungen erfüllt sind; Einschränkungen müssen

- gesetzlich vorgesehen sein,
- den Wesensgehalt des Rechts achten,
- den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen tatsächlich entsprechen und,
- sofern sie sich als erforderlich erweisen, dem Grundsatz der Verhältnismäßigkeit entsprechen.

14. Notwendigkeit und Verhältnismäßigkeit dieser Regelung sind sowohl insgesamt, unter Berücksichtigung der bereits in der EU bestehenden IT-Großsysteme, als auch spezifisch, für jeden Einzelfall dieser Drittstaatsangehörigen, zu bewerten, die rechtmäßig als Besucher in die EU einreisen. **Der EDSB möchte zunächst betonen, dass aus dem Blickwinkel der Artikel 7 und 8 der Charta die Verarbeitung personenbezogener Daten im Rahmen des EES einen erheblichen Eingriff bedeutet**, bedenkt man die Zahl der von dieser Regelung betroffenen Personen, die Art der verarbeiteten Informationen, die für die Verarbeitung dieser Informationen eingesetzten Mittel und die verschiedenen verfolgten Zwecke, wie weiter unten noch näher ausgeführt wird.

15. Erstens werden im EES *alle* Ein- und Ausreisen von Drittstaatsangehörigen[29] erfasst, die in das Hoheitsgebiet der EU einreisen oder es wieder verlassen; damit sind alljährlich Millionen von Menschen betroffen. Nach Angaben der Kommission selber ist zu erwarten, dass die Gesamtzahl regulärer Grenzübertritte bis 2025 auf 887 Millionen steigen wird, von denen rund ein Drittel auf Drittstaatsangehörige entfällt.[30] Allein das durch dieses System zu verarbeitende Volumen personenbezogener Daten dürfte das EES zu einer der größten europäischen Datenbanken machen. Diesbezüglich begrüßt der EDSB, dass der EES-Vorschlag von 2016 im Sinne des Grundsatzes der Datenminimierung eine Reduzierung der Menge verarbeiteter personenbezogener Daten anstrebt: Vermutlich werden im EES höchstens 26 Datenelemente pro Person erfasst[31] (und nicht mehr die im EES-Vorschlag von 2013 vorgesehenen 36 Datenelemente[32]).

16. Zweitens ist zu erwarten, dass das EES zur Abnahme der Fingerabdrücke von Drittstaatsangehörigen und der Aufnahme eines Gesichtsbilds bei der Einreise führen wird, womit die Menge der von der EU in bereits bestehenden Datenbanken wie Eurodac, Schengener Informationssystem (nachstehend „SIS“) und VIS gespeicherten biometrischen Daten signifikant steigen würde. Biometrische Daten sind von einer besonderen Art und gelten als sensibler als andere, da sie unwiderruflich mit einem Menschen verbunden sind, dessen Körper „lesbar“ gemacht wird.[33] Der EDSB nimmt zur Kenntnis, dass die Verwendung biometrischer Daten erforderlich ist, um die Identität von die EU-Grenzen überschreitenden Drittstaatsangehörigen besser bestimmen zu können. Dessen ungeachtet gilt, dass die Verarbeitung biometrischer Daten eben wegen des besonderen Charakters dieser Daten einen schwerer wiegenden Eingriff bedeutet und daher nach einem höheren Datenschutzniveau verlangt.

17. Drittens stellt der EDSB ebenfalls fest, dass im Nachgang zu dem von eu-Lisa geleiteten Pilotprojekt der EES-Vorschlag von 2016 nunmehr die Speicherung einer geringeren Anzahl biometrischer Daten vorsieht. Gestützt auf die Ergebnisse dieses Pilotprojekts regt der EES-

Vorschlag von 2016 an, die Erfassung von vier Fingerabdrücken und des Gesichtsbilds als für Überprüfungs- und Identifizierungszwecke ausreichend zu erachten (im EES-Vorschlag von 2013 waren es noch zehn Fingerabdrücke, dafür kein Gesichtsbild). Der EDSB weist allerdings darauf hin, dass eine geringere Zahl biometrischer Daten nicht unbedingt mit einem geringeren Eingriff gleichzusetzen ist, da der Vorschlag auch die Erfassung einer Kombination von zwei Arten biometrischer Daten vorsieht und damit den Einsatz sowohl von Software für den Abgleich von Fingerabdrücken als auch von Gesichtserkennungssoftware für eine schnelle Verarbeitung und ein schnelles Durchsuchen der gespeicherten Daten zulässt.

18. Schließlich wird das EES in zweifacher Hinsicht Wirkung zeigen, denn EES-Daten werden sowohl für Zwecke des Grenzmanagements und der Erleichterung des Grenzübertritts als auch für Gefahrenabwehr- und Strafverfolgungszwecke verarbeitet.

II. Ziele des EES

19. In der Begründung der Kommission zum EES-Vorschlag von 2016[34] heißt es, das EES verfolge drei allgemeine Ziele:

1) Reduzierung von Verzögerungen bei den Grenzübertrittskontrollen und Verbesserung der Qualität der Grenzübertrittskontrollen für Drittstaatsangehörige („Erleichterung"),
2) Gewährleistung einer systematischen und zuverlässigen Ermittlung von „Overstayern" („Grenzmanagement"),
3) Unterstützung der Bekämpfung von Terrorismus und schwerer Kriminalität und letztendlich Leistung eines Beitrags zur Stärkung der inneren Sicherheit („Gefahrenabwehr und Strafverfolgung").

20. Der EDSB merkt hierzu an, dass die Ziele 1) und 2) in der Folgenabschätzung zum EES-Vorschlag von 2016 häufig als *„die beiden primären Ziele des EES"*[35] bezeichnet werden, während der Zugriff auf das EES für Gefahrenabwehr- und Strafverfolgungsbehörden als *„sekundäres Ziel"*[36] der Regelung angesehen wird. Diese Unterscheidung hat jedoch keinen Niederschlag im Wortlaut des EES-Vorschlags von 2016 gefunden, weder in seinem verfügenden Teil, noch in seinen Erwägungsgründen. Ganz im Gegenteil: Im EES-Vorschlag von 2016 werden diese drei Ziele in Artikel 1 (Gegenstand) und in Artikel 5 des Vorschlags auf eine Stufe gestellt, in dem 12 konkrete Zwecke für die Erhebung, die Speicherung und den Abruf von EES-Daten aufgeführt sind. **Der EDSB empfiehlt nachdrücklich, im EES-Vorschlag von 2016 durchgängig zwischen den Zielen zu unterscheiden.**

21. Nach dem Verständnis des EDSB wird das EES vorrangig für Zwecke des Grenzmanagements und der Erleichterung des Grenzübertritts geschaffen und soll potenziell auch einen Zugriff auf EES-Daten für Zwecke der Gefahrenabwehr und Strafverfolgung ermöglichen. Daher wird in dieser Stellungnahme nacheinander auf die Einrichtung des EES für Zwecke des Grenzmanagements und der Erleichterung des Grenzübertritts als den beiden primären Zielen des Systems in Abschnitt III und dann auf den Zugriff für Gefahrenabwehr- und Strafverfolgungsbehörden zu diesem Instrument der Grenzkontrolle als einem sekundären Ziel in Abschnitt IV näher eingegangen.

III. Grenzmanagement und Erleichterung des Grenzübertritts

22. Der EDSB räumt ein, dass die EU derzeit vor zunehmend großen Herausforderungen durch Migration steht und hält fest, dass der EES-Vorschlag von 2016 Teil einer umfassenderen Politik der EU für Grenzkontrollen und Migrationsmanagement ist. Erforderlich ist eine Beurteilung der tatsächlichen Auswirkungen des EES auf diese Politik zusammen mit allen in diesem Bereich bereits vorhandenen relevanten IT-Großsystemen wie Eurodac, SIS und VIS, die in absehbarer Zukunft ebenfalls weiterentwickelt werden sollen.

23. Der EDSB begrüßt, dass die Kommission den mit Blick auf das EES früher geäußerten Bedenken wegen des Schutzes der Privatsphäre und des Datenschutzes Aufmerksamkeit geschenkt und sich die Zeit genommen hat, mehr Unterlagen zusammenzustellen und auszuarbeiten, die für die Schaffung dieses Systems und die politischen Weichenstellungen im zweiten Paket „Intelligente Grenzen" sprechen; dazu gehören das von eu-LISA geleitete Pilotprojekt, die FRA-Erhebung, die öffentliche Konsultation und eine sorgfältige Folgenabschätzung für die Vorschläge von 2016. Die Belege sind zwar nicht immer vollständig[37], doch scheinen ausreichend viele Faktoren die Einrichtung des EES für Zwecke des Grenzmanagements und der Erleichterung des Grenzübertritts durchaus zu rechtfertigen.

24. In Anbetracht der vielfältigen Auswirkungen der vorgeschlagenen EES-Regelung auf Privatsphäre und Datenschutz[38] kommt es darauf an, dass die künftige EES-Verordnung für den Fall, dass eine Überprüfung durch den EuGH stattfinden sollte, das in Artikel 52 Absatz 1 der Charta formulierte Erfordernis der Verhältnismäßigkeit in vollem Umfang erfüllt. Auch wenn das System als erforderlich gilt, sollte doch klarer nachgewiesen werden, dass die Vorteile eines Einreise-/Ausreisesystems schwerer wiegen als der Eingriff in die Privatsphäre *aller* Drittstaatsangehörigen. Eine Orientierungshilfe bot der EuGH im Urteil Digital Rights Ireland in den verbundenen Rechtssachen C-293/12 und C-594/12[39] (nachstehend „DRI-Urteil"). Der EDSB hat den von der Kommission in der Folgenabschätzung vorgenommenen Verhältnismäßigkeitstest zur Kenntnis genommen.[40]

25. Der EDSB kommentiert zwei Hauptaspekte des EES-Vorschlags von 2016, die unmittelbar mit der Verhältnismäßigkeit einer solchen Regelung für Zwecke des Grenzmanagements und der Erleichterung des Grenzübertritts zu tun haben (Abschnitte III.1 und III.2). Der EDSB spricht ferner weitere Empfehlungen betreffend einzelne Aspekte des EES-Vorschlags von 2016 aus (Abschnitt III.3), die er der Kommission zur Prüfung anheimstellt.

III.1 Datenspeicherung über fünf Jahre

26. Bei der Festlegung einer Datenspeicherfrist verlangen die EU-Datenschutzstandards einen möglichst kurzen Zeitraum. In Erwägungsgrund 25 des EES-Vorschlags von 2016 heißt es vollkommen zu Recht: *„Personenbezogene Daten sollten im EES nicht länger als für die Zwecke des EES erforderlich gespeichert werden"*. Nunmehr sieht der Vorschlag[41] eine längere Speicherfrist von fünf Jahren für *alle* Einträge zu Ein- und Ausreisen *aller* Drittstaatsangehörigen ab dem Datum des Ausreisedatensatzes vor (Artikel 31 Absatz 1), sowie fünf Jahre und einen Tag für Dossiers zu einer Person[42] *„nach dem Datum des letzten Ausreisedatensatzes [...], sofern innerhalb von fünf Jahren nach diesem letzten Ausreisedatensatz [...] kein Einreisedatensatz eingegeben wurde"* (Artikel 31 Absatz 2). Ferner sieht der EES-Vorschlag von 2016 in Artikel 31 Absatz 4 eine geringfügige Ausnahme

für Ein-/Ausreisedatensätze von Familienangehörigen von Drittstaatsangehörigen vor, die ein Jahr lang gespeichert werden, während ihre Dossiers ebenfalls fünf Jahre lang aufbewahrt werden sollen.

27. Der EDSB weist zunächst darauf hin, dass in Anbetracht des in Artikel 31 Absatz 2 festgelegten Datums, ab dem die Speicherfrist für Dossiers zu einer Person läuft, bei Drittstaatsangehörigen, die mindestens einmal alle fünf Jahre in die EU einreisen, die personenbezogenen Daten, einschließlich ihres Gesichtsbilds und vier ihrer Fingerabdrücke, im EES nicht nur für fünf Jahre, sondern praktisch ständig gespeichert bleiben. Wenn sie nämlich vor Ablauf der fünf Jahre erneut in die EU reisen, wird ihr Dossier nicht gelöscht, sondern nach ihrer Ausreise aus dem Hoheitsgebiet der EU erneut fünf Jahre lang gespeichert.

28. **Der EDSB möchte den Gesetzgeber darauf hinweisen**, dass mit Blick auf das Ziel einer Reduzierung von Verzögerungen bei den Grenzübertrittskontrollen und der Verbesserung der Qualität der Grenzübertrittskontrollen für Drittstaatsangehörige sowie der Ermittlung von Overstayern **die Verhältnismäßigkeit einer Speicherfrist von fünf Jahren für personenbezogene Daten eingehend zu begründen ist**.

29. **Der EES-Vorschlag von 2016 sollte also die vom Gerichtshof im DRI-Urteil formulierten Bedingungen erfüllen**. Diesbezüglich befand der Gerichtshof, dass *„[die] Festlegung [der Speicherfrist] auf objektiven Kriterien beruhen muss, die gewährleisten, dass sie auf das absolut Notwendige beschränkt wird“*.[43] Der EDSB nimmt zur Kenntnis, dass eine Frist von fünf Jahren der durchschnittlichen Gültigkeitsdauer eines von Drittländern ausgestellten Passes sowie der maximalen Gültigkeitsdauer von Mehrfachvisa entsprechen würde, wie in der Folgenabschätzung[44] zu den Vorschlägen ausgeführt wird. Allerdings macht die Tatsache, dass die ausgewählte Speicherfrist der in anderen bestehenden Systemen wie dem VIS angeglichen wurde, nicht per se die Verhältnismäßigkeit dieser Frist aus.

30. Der Vorschlag sieht gleichfalls die vorzeitige Löschung der Dossiers zu einer Person und der Ein- und Ausreisedatensätze vor Ablauf der gewählten Frist für den Fall vor, dass die betreffende Person die Staatsangehörigkeit oder einen Aufenthaltstitel eines Mitgliedstaats erworben hat[45] (Artikel 32 Absatz 6). Der EDSB begrüßt, dass in dem Vorschlag der für die Löschung verantwortliche Mitgliedstaat genannt wird und dass eine solche Löschung „unverzüglich“ erfolgen sollte. Der EDSB schlägt jedoch vor, den Ausdruck „unverzüglich“ im Zusammenhang mit der Löschung gespeicherter Daten, die überflüssig geworden sind und für die Zwecke des EES nicht länger benötigt werden, näher zu spezifizieren.

31. Im Sonderfall von Overstayern sieht Artikel 31 Absatz 3 des EES-Vorschlags von 2016 eine Datenspeicherfrist von fünf Jahren nach dem letzten Tag des zulässigen Aufenthalts vor (ähnlich wie der EES-Vorschlag von 2013[46]). Die Erwägungsgründe des aktuellen Vorschlags liefern jedoch im Vergleich zum älteren Vorschlag[47] keine weitere Begründung dieser Notwendigkeit, obwohl der EDSB in der Vergangenheit dem Gesetzgeber empfohlen hatte, in einem Erwägungsgrund des EES-Vorschlags genauer zu begründen, weshalb die Daten von Overstayern so lange gespeichert werden sollen, oder diesen Zeitraum deutlich zu verkürzen[48].

32. Des Weiteren sieht der EES-Vorschlag von 2016 vor, dass das künftige System die betroffenen Mitgliedstaaten drei Monate im Voraus über die geplante Löschung von Daten zu Overstayern informiert, damit sie geeignete Maßnahmen treffen können (Artikel 31 Absatz 3). Hierzu heißt es in der Begründung des EES-Vorschlags, dass Daten über Overstayer, die nach Ablauf der fünfjährigen Datenspeicherfrist noch nicht aufgespürt worden sind, als

Ausschreibung wegen Einreiseverweigerung auf der Grundlage einer nationalen Entscheidung in das SIS eingegeben werden können.[49] Geeignete Maßnahmen, darunter die Eingabe einer Ausschreibung in das SIS, könnten jedoch schon früher als fünf Jahre nach der Identifizierung eines Drittstaatsangehörigen als Overstayer ergriffen werden.

33. **Nach wie vor entzieht sich dem EDSB, warum für den Zweck einer Identifizierung als Overstayer diese Daten über einen so langen Zeitraum gespeichert werden müssen, und er fordert den Gesetzgeber auf, diesen Zeitraum zu begründen und/oder ihn zu verkürzen und so sicherzustellen, dass er auf das unbedingt notwendige Maß beschränkt ist.**

III.2 Erhobene Daten

34. Wie in den Artikeln 14 bis 18 geregelt, sieht der EES-Vorschlag von 2016 die Erhebung, Speicherung und Verwendung alphanumerischer Daten und biometrischer Daten von Drittstaatsangehörigen vor, die in die EU einreisen bzw. aus ihr ausreisen. Der EDSB begrüßt, dass der Vorschlag die Gesamtmenge personenbezogener Daten von 36 auf 26 Datenelemente pro Person sowie die Zahl der verarbeiteten Fingerabdrücke[50] von zehn auf vier für visumbefreite Drittstaatsangehörige reduziert hat (Artikel 15 Absatz 1). Bei visumpflichtigen Drittstaatsangehörigen wird das Gesichtsbild der einzige biometrische Identifikator sein, der in das EES eingegeben wird (Artikel 14 Absatz 1), da ihre zehn Fingerabdrücke bereits im VIS gespeichert sind. Die Erfassung von zehn Fingerabdrücken wäre in der Regel mit Zwecken der Gefahrenabwehr und Strafverfolgung verbunden.

35. Der EDSB stellt allerdings die Notwendigkeit der Speicherung von Gesichtsbildern von visumpflichtigen Drittstaatsangehörigen im EES in Frage, denn ihre Gesichtsbilder sind bereits im VIS gespeichert. Der EDSB nimmt die Aussage in der Folgenabschätzung zur Kenntnis, der zufolge bisher *„ein Visuminhaber im VIS nicht auf der Grundlage seines Bildes gesucht werden kann“*[51], stellt aber die Frage, weshalb das VIS nicht in vollem Umfang sowohl für Funktionalitäten sowohl des EES als auch des VIS genutzt werden kann. **Der EDSB bittet um eine Begründung der Notwendigkeit, Gesichtsbilder von visumpflichtigen Drittstaatsangehörigen im EES zu speichern. Dieses Erfordernis hat zur Folge, dass das Gesichtsbild von visumpflichtigen Drittstaatsangehörigen doppelt in zwei verschiedenen, miteinander verbundenen Datenbanken gespeichert ist. In Ermangelung einer überzeugenden Begründung für die Speicherung der Gesichtsbilder in zwei verschiedenen Datenbanken empfiehlt der EDSB, das Gesichtsbild aus Artikel 14 Absatz 1 des Vorschlags herauszunehmen, so dass sich das EES bei visumpflichtigen Drittstaatsangehörigen sowohl auf die Fingerabdrücke als auch das Gesichtsbild berufen kann, die bereits im VIS gespeichert sind, und so eine Doppelerfassung biometrischer Daten in IT-Systemen der EU vermieden und die Erhebung und Speicherung von Daten im EES auf das unbedingt erforderliche Maß beschränkt wird.**

36. Schließlich sind in Artikel 15 des EES-Vorschlags von 2016 mehrere Fälle geregelt, in denen aus rechtlichen Gründen (weil z. B. die Person unter 12 Jahre alt ist) oder aus faktischen Gründen (weil z. B. eine Hand fehlt oder Finger fehlen oder die Fingerkuppen beschädigt sind) die Fingerabdrücke eines Drittstaatsangehörigen nicht abgenommen werden können. Artikel 15 Absatz 3 befasst sich mit Situationen, in denen Drittstaatsangehörigen aus physischen Gründen keine Fingerabdrücke abgenommen werden können. Einige dieser Situationen können vorübergehender Art sein und sind dann normalerweise auf einen

medizinischen Grund zurückzuführen. Das in Artikel 15 Absatz 3 beschriebene Verfahren gibt den Grenzbehörden die Befugnis, nähere Angaben zu den Gründen der vorübergehenden Unmöglichkeit der Abnahme von Fingerabdrücken zu erfragen. Es findet sich jedoch dort keine nähere Erläuterung dazu, was mit den erhobenen Daten geschieht, auch nicht dazu, wo, wie und wie lange sie gespeichert werden, und ferner nicht dazu, wie diese Daten möglicherweise verwendet und wie sie geschützt werden. **Der EDSB empfiehlt, Artikel 15 Absatz 3 dahingehend zu ändern, dass genau spezifiziert wird, welche Daten von den Grenzbehörden erhoben, gespeichert und verwendet werden dürfen.**

III.3 Weitere Empfehlungen zu den Vorschlägen

a) Biometrische Daten

37. Der EES-Vorschlag von 2016 sieht für die Erhebung, Speicherung und Verwendung biometrischer Daten von Drittstaatsangehörigen vor: das Gesichtsbild nur bei visumpflichtigen Reisenden (Artikel 14 Absatz 1) und eine Kombination von vier Fingerabdrücken plus Gesichtsbild bei visumbefreiten Reisenden (Artikel 15 Absatz 1). Der EDSB begrüßt die Begründung der spezifischen Verwendung biometrischer Daten in Erwägungsgrund 10 des EES-Vorschlags von 2016 sowie durchgängig in der Folgenabschätzung zum Vorschlag.[52] Der EDSB hat wiederholt eingeräumt, dass biometrische Daten Vorteile bieten können, hat aber auch stets unterstrichen, dass diese Vorteile aufgrund der ureigensten Natur der Daten von der Anwendung strengerer Garantien abhängen würden.[53] Jeder Systemfehler könnte erhebliche nachteilige Folgen[54] für Drittstaatsangehörige haben, deren Daten im System gespeichert sind.

38. In jedem vorgeschlagenen System, das die Verarbeitung biometrischer Daten verlangt, sollte es ausreichende Garantien und Schutzvorkehrungen geben, mit denen der wirksame Schutz der gespeicherten Daten vor Missbrauch, Irrtum, rechtswidrigem Zugriff und rechtswidriger Verwendung dieser Daten gewährleistet ist. Diese Garantien und Schutzvorkehrungen lassen das Pendel in Richtung größerer Verhältnismäßigkeit schwingen. Der EDSB hat bereits die Einführung einer nicht erschöpfenden Liste von Garantien für die automatische Verarbeitung biometrischer Daten über das EES empfohlen, mit der vermieden werden könnte, dass Drittstaatsangehörige unter den Mängeln des Systems zu leiden haben, z. B. bei Nichterfassung der Fingerabdrücke oder einem Systemfehler bei der Verwendung biometrischer Daten.[55]

39. Der EDSB begrüßt die von der Kommission vorgenommene Folgenabschätzung betreffend Grundrechte[56], in deren Mittelpunkt die Auswirkungen des künftigen EES auf Artikel 7 und 8 der Charta stehen, und die sich mit der Relevanz biometrischer Daten in diesem Zusammenhang und mit den Gründen für die Wahl der biometrischen Identifikatoren im Vorschlag befasst. Der EDSB bedauert allerdings, dass dieses Dokument keine Analyse der Auswirkungen von Fehlern und Ausfällen der Technologie zum Abgleich biometrischer Daten auf Drittstaatsangehörige enthält.

40. Artikel 33 des EES-Vorschlags von 2016 besagt vollkommen zu Recht, dass die Fingerabdrücke von sehr guter Qualität sein müssen. Nicht eingegangen wird jedoch auf die Qualität von Gesichtsbildern, die nicht elektronischen maschinenlesbaren Reisedokumenten (eMRTD) (also Pässen) entnommen wurden, obwohl die Qualität von Gesichtsbildern von allergrößter Bedeutung ist. **Der EDSB empfiehlt, in Artikel 14 eine Bestimmung aufzunehmen, der zufolge in Fällen, in denen Gesichtsbilder vor Ort aufgenommen werden, diese Bilder Mindestanforderungen an ihre Qualität genügen müssen. Zudem**

sollte in Artikel 33 spezifiziert werden, dass die Kommission im Wege einer Durchführungsmaßnahme detailliert regeln wird, wie diese erforderliche Qualität bei vor Ort aufgenommenen Gesichtsbildern zu erreichen ist.

41. Der EDSB begrüßt, dass Artikel 19 des EES-Vorschlags von 2016 Ausweichverfahren für den Fall vorsieht, dass die Eingabe von Daten in das Zentralsystem technisch nicht möglich ist oder das System ausfällt.

b) Sicherheit des Systems

42. Die Sicherheit eines Systems wie des in Artikel 6 des EES-Vorschlags beschriebenen, das sich auf eine Vielzahl von Komponenten verteilt (ein bei eu-LISA angesiedeltes Zentralsystem und eine einheitliche nationale Schnittstelle (NUI) in jedem Mitgliedstaat), lässt sich nur mit einem ganzheitlichen Blick auf das System erreichen, bei dem nicht nur die Sicherheit des Zentralsystems im Mittelpunkt steht, sondern auch alle anderen Teile des Systems und alle Nutzer des Systems berücksichtigt werden. Einfluss auf die Sicherheit des vorgeschlagenen EES wird darüber hinaus die Sicherheit anderer, mit ihm verbundener Systeme wie der nationalen Grenzinfrastruktur der einzelnen Mitgliedstaaten haben.

43. Die am System (Zentralsystem und NUI) ergriffenen Sicherheitsvorkehrungen, einschließlich der Verpflichtungen der Nutzer in den Mitgliedstaaten, müssen aneinander angepasst werden, da eine Sicherheitsschwachstelle in irgendeinem Teil des Systems die Sicherheit des Systems in seiner Gesamtheit beeinträchtigen würde. So kann beispielsweise ein Sicherheitszwischenfall in einem Teil einer an eine NUI angeschlossenen nationalen Grenzinfrastruktur die Sicherheit des Zentralsystems des EES berühren.

44. Zwar sind in Artikel 39 des EES-Vorschlags von 2016 die Sicherheitsverantwortlichkeiten für eu-LISA und die Mitgliedstaaten festgelegt, doch wird dort nicht die Notwendigkeit erwähnt, diese Angleichung von Sicherheitsbemühungen generell zu gewährleisten. **Der EDSB empfiehlt, in Artikel 39 diese ausgeprägte Notwendigkeit einer Koordinierung zwischen eu-LISA und den Mitgliedstaaten bei der Gewährleistung der Sicherheit hervorzuheben. Grundlage für diese Angleichung der Sicherheit sollte ein geeignetes Verfahren für das Risikomanagement der Informationssicherheit sein, das alle Bestandteile des neuen Systems abdeckt, also auch Teile, die der Verantwortung der Mitgliedstaaten unterstehen.**

45. In Artikel 6 Absatz 1 Buchstabe c ist von der Notwendigkeit eines *„sicheren Kommunikationskanals zwischen dem Zentralsystem des EES und dem Zentralsystem des VIS“* die Rede, doch ist dann in Artikel 6 Absatz 1 Buchstabe d nicht gesondert die Rede von der Sicherheit der *„Kommunikationsinfrastruktur zwischen dem Zentralsystem und den einheitlichen nationalen Schnittstellen“*. **Der EDSB empfiehlt, den Wortlaut von Artikel 6 Absatz 1 Buchstabe d zu ändern in *„einer sicheren Kommunikationsinfrastruktur zwischen dem Zentralsystem und den einheitlichen nationalen Schnittstellen“*.**

46. Gegenstand von Artikel 34 sind die Zuständigkeiten für die Entwicklung und das Betriebsmanagement des Zentralsystems, der einheitlichen nationalen Schnittstellen, der Kommunikationsinfrastruktur sowie des sicheren Kommunikationskanals zwischen dem Zentralsystem des EES und dem Zentralsystem des VIS. Mit der Sicherheit befasst sich Artikel 34 jedoch nicht. Er beschäftigt sich auch nicht mit dem Schutz der Privatsphäre. Der

EDSB gibt zu bedenken, dass ein neues System und jedwede größere Änderung an einem bestehenden System (in diesem Fall am VIS) professionell nur erreicht werden kann,

- wenn ein fundierter Sicherheitsprozess mit einer detaillierten Risikoanalyse durchgeführt wird, und
- wenn die Grundsätze des eingebauten Datenschutzes (privacy by design) und datenschutzfreundlicher Voreinstellungen eingehalten werden.

47. **Der EDSB empfiehlt, in Artikel 34 folgende Anforderungen aufzunehmen:**

- Durchführung einer Risikobewertung als Teil der Entwicklung dieses neuen Systems;
- Einhaltung der Grundsätze des eingebauten Datenschutzes und datenschutzfreundlicher Voreinstellungen während des gesamten Lebenszyklus der Systementwicklung;
- Aktualisierung der Risikobewertung für das VIS, um der neuen Verbindung mit dem künftigen EES Rechnung zu tragen, und später Durchführung der zusätzlichen Sicherheitsvorkehrungen, auf die in der aktualisierten Risikobewertung hingewiesen wurde.

c) Sicherheit des Web-Dienstes

48. Der EDSB sieht die Notwendigkeit, Drittstaatsangehörigen Informationen bereitzustellen, damit sie *„jederzeit die verbleibende zulässige Aufenthaltsdauer überprüfen können“*, und auch, dass Beförderungsunternehmer die Möglichkeit benötigen, *„zu überprüfen, ob Drittstaatsangehörige, die im Besitz eines Visums für die ein- beziehungsweise zweimalige Einreise sind, das betreffende Visum bereits verwendet haben“*. Gemäß Artikel 12 des EES-Vorschlags von 2016 soll dies über einen sogenannten sicheren Internetzugang zu einem bei eu-LISA angesiedelten Web-Dienst geschehen. Aus dem Blickwinkel der Sicherheit betrachtet gibt der EES-Vorschlag von 2016 nur unzureichend Auskunft über die konkreten Maßnahmen, mit denen die Sicherheit der bei diesem Web-Dienst befindlichen personenbezogenen Daten gewährleistet werden soll, und über die genauen Zuständigkeiten für die Sicherheit der personenbezogenen Daten in diesem Web-Dienst, auch in Fällen, in denen die personenbezogenen Daten von Beförderungsunternehmern extrahiert und gespeichert worden sind.

49. **Nach dem Verständnis des EDSB wird eu-LISA für die Sicherheit des Web-Dienstes, die Sicherheit der darin enthaltenen personenbezogenen Daten und für das Verfahren verantwortlich sein, mit dem die personenbezogenen Daten aus dem Zentralsystem in den Web-Dienst eingespeist werden, und sollte daher in diesen Fragen als für die Verarbeitung Verantwortlicher gelten. Der EDSB empfiehlt, diese Verantwortlichkeiten im EES-Vorschlag von 2016 genau zu spezifizieren.** Der spezifische Sicherheitsbedarf sollte das Ergebnis einer von eu-LISA vorgenommenen Risikobewertung der Informationssicherheit sein. Diese Risikobewertung der Informationssicherheit sollte regelmäßig auf den neuesten Stand gebracht werden. Eu-LISA sollte ferner für die ordnungsgemäße Durchführung und Überwachung von Sicherheitskontrollen verantwortlich sein, die im Zuge der Risikobewertung festgelegt wurden.

50. Bedenken hegt der EDSB ferner bezüglich der Sicherheit der personenbezogenen Daten, sobald die Beförderungsunternehmer sie aus dem Web-Dienst extrahiert haben, weil es keinerlei Hinweise auf ihre Verantwortung für die Sicherheit dieser Daten gibt. In Artikel 33

Absatz 1 Buchstabe g ist die Rede von Durchführungsmaßnahmen, die die Kommission im Vorfeld der Entwicklung des neuen Systems für diesen Web-Dienst annehmen müsste; diese Durchführungsmaßnahmen könnten eine Möglichkeit bieten, ein gewisses Sicherheitsniveau für personenbezogene Daten nach ihrer Extraktion durch die Beförderungsunternehmer vorzugeben.

51. Ein weiterer Sicherheitsaspekt dieses Web-Dienstes berührt die Frage, wie sich Drittstaatsangehörige und Beförderungsunternehmer gegenüber dem Web-Dienst authentifizieren, wenn sie Informationen abrufen wollen. Die Authentifizierung gegenüber dem Web-Dienst ließe sich folgendermaßen bewerkstelligen:

- für Drittstaatsangehörige: Eingabe der in Artikel 14 Absatz 1 Buchstabe b genannten Daten, also Art und Nummer des Reisedokuments oder der Reisedokumente und des aus drei Buchstaben bestehender Codes des ausstellenden Staates (Artikel 12 Absatz 1);

- für Beförderungsunternehmer: gegebenenfalls Eingabe der in Artikel 14 Absatz 1 Buchstabe d genannten Daten, also Nummer der Visummarke des Visums für einen kurzfristigen Aufenthalt mit dem aus drei Buchstaben bestehenden Code des ausstellenden Mitgliedstaats, Art des Visums, Enddatum der maximalen Dauer des aufgrund des Visums zulässigen Aufenthalts, das bei jeder Einreise aktualisiert werden muss, und Datum des Ablaufs der Gültigkeitsdauer des Visums (Artikel 12 Absatz 2).

52. Bei Drittstaatsangehörigen kann die Authentifizierung gegenüber dem Web-Dienst (lediglich Angabe von Art und Nummer des Reisedokuments oder der Reisedokumente und des aus drei Buchstaben bestehenden Codes des ausstellenden Staates) eine Schwachstelle sein; ein Dritter könnte einfach versuchen, vorschriftsmäßig formatierte Daten in den Web-Dienst in der Hoffnung einzugeben, dass die Verbindung zwischen einem interessanten Drittstaatsangehörigen und seinen Angaben in Reisedokumenten bestätigt wird, und könnte dann etwas über die zulässige Aufenthaltsdauer des Drittstaatsangehörigen in Erfahrung bringen. Es sollten von dem den Web-Dienst nutzenden Drittstaatsangehörigen weitere Angaben verlangt werden, um diese Art von Angriffen auf den Web-Dienst zu erschweren; gleichzeitig wäre damit eher gewährleistet, dass die Person, die einen bestimmten Datensatz abrufen will, tatsächlich der betreffende Drittstaatsangehörige ist. Eine Möglichkeit wäre beispielsweise die Abfrage des Geburtsdatums zusätzlich zu Art und Nummer des Reisedokuments oder der Reisedokumente und des aus drei Buchstaben bestehenden Codes des ausstellenden Staates. Genauen Aufschluss über die weiteren Angaben, die für eine korrekte Authentifizierung eines Drittstaatsangehörigen zu machen wären, sollten unter anderem die Ergebnisse der weiter oben unter Punkt 49 empfohlenen Risikobewertung geben.

53. Da Beförderungsunternehmer Zugriff auf Daten einer Vielzahl von Drittstaatsangehörigen hätten, muss dafür gesorgt werden, dass nur befugte Mitarbeiter von Beförderungsunternehmern Zugang zum Web-Dienst erhalten. Es sollte daher eine solide Authentifizierungsregelung gefunden werden, die nicht an die Daten von Drittstaatsangehörigen gekoppelt ist (z. B. mit Login und Passwort, Token). Das angemessene Authentifizierungsniveau sollte auf der Grundlage der bereits erwähnten Risikobewertung festgelegt werden. Des Weiteren sollte eine angemessene Rückverfolgbarkeit von Abfragen des Web-Dienstes durch Beförderungsunternehmer (Protokollierung) vorgesehen werden, damit sie zur Rechenschaft gezogen werden können, sollte ein Missbrauch des Web-Dienstes aufgedeckt werden.

d) Interoperabilität zwischen EES und VIS

54. Der EES-Vorschlag von 2016 sieht „Interoperabilität" zwischen EES und VIS von Anfang an vor, oder eher eine „Vernetzung" zwischen den beiden Systemen. Nach Auffassung der Kommission ist die Vernetzung von Informationssystemen einer der Aspekte der Interoperabilität, und sie definiert sie als die Tatsache, dass *„verschiedene Systeme oder Datenbanken technisch miteinander kommunizieren können"*".[57] Eine Vernetzung zwischen dem künftigen EES und den bestehenden VIS ist ein erster Schritt hin zu einem langfristigen Ziel der Kommission, das in der Mitteilung „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit", die zum zweiten Paket „Intelligente Grenzen" gehört, angekündigt wurde: bessere Interoperabilität zwischen bestehenden und künftigen EU-Informationssystemen für Grenzmanagement und Sicherheit.

55. Der EES-Vorschlag von 2016 überträgt eu-LISA die Aufgabe, einen direkten Kommunikationskanal zwischen den Zentralsystemen der beiden Datenbanken einzurichten, so dass direkte Abfragen zwischen diesen beiden Systemen erfolgen können (Artikel 7). EES und VIS haben die gleichen technischen Merkmale und verfügen über ein gemeinsames System für den Abgleich biometrischer Daten. Das hat zur Folge, dass das EES verwendende Grenzbehörden zu in Artikel 7 Absatz 2 des EES-Vorschlags von 2016 festgelegten konkreten Zwecken Abfragen im VIS durchführen können, während das VIS verwendende Visumbehörden zu in Artikel 7 Absatz 3 festgelegten konkreten Zwecken Abfragen im EES vornehmen können. Artikel 55 des EES-Vorschlags von 2016 sieht eine Änderung der VIS-Verordnung vor, um die Interoperabilität zwischen den beiden Systemen zu gewährleisten.

56. Die Kommission merkt hierzu an: *„Somit wird die Mehrfachverarbeitung personenbezogener Daten im Einklang mit dem Grundsatz des „eingebauten Datenschutzes" („privacy by design") verhindert"*.[58] Konkret bedeutet dies, dass bereits im VIS gespeicherte Fingerabdrücke von Visuminhabern nicht noch einmal im EES gespeichert werden, sondern dass stattdessen das EES Fingerabdrücke aus dem VIS für die Zwecke des EES wiederverwendet und so vermieden wird, dass Fingerabdrücke von Visuminhabern zweimal, nämlich in beiden Systemen, gespeichert werden. Der EDSB fragt sich, warum diese Vorgehensweise nicht auch bei den bereits im VIS gespeicherten Gesichtsbildern visumpflichtiger Drittstaatsangehöriger möglich ist.[59]

57. Der EDSB ist nicht grundsätzlich gegen die Interoperabilität von IT-Großsystemen der EU, solange die Grundrechte in vollem Umfang gewahrt werden. Er weist jedoch nachdrücklich darauf hin, dass ein solches Vorgehen die Gefahr von Verstößen gegen die Grundsätze des Datenschutzes und hier vor allem den Grundsatz der Zweckbindung möglicherweise erhöht. Was nun EES und VIS angeht, sollte die Vereinbarkeit der Wiederverwendung von im Zusammenhang mit dem VIS erhobenen Daten für die einzelnen Zwecke des EES (und umgekehrt) bewertet werden. Nach Auffassung des EDSB sind die primären Zwecke der beiden Systeme eng miteinander verknüpft und die betroffenen Daten bis zu einem gewissen Grad identisch. Damit wäre das Risiko eines Missbrauchs eingedämmt.

58. Über den EES-Vorschlag von 2016 hinausgehend wird sich der EDSB an anderer Stelle noch genauer mit den Auswirkungen des allgemeinen Ziels der Kommission befassen, mehr Interoperabilität anzustreben.

e) Nationale Erleichterungsprogramme

59. Die Kommission beschloss, ihren RTP-Vorschlag von 2013 aus dem zweiten Paket „Intelligente Grenzen“ herauszunehmen, legte aber stattdessen einen geänderten Vorschlag zur Änderung des Schengener Grenzkodex vor. Eine der Hauptänderungen im Vorschlag von 2016 zur Änderung des Schengener Grenzkodex ist ein neuer Artikel 8e, der jedem Mitgliedstaat die Möglichkeit gibt, ein nationales Programm für Drittstaatsangehörige einzurichten, die beim Übertritt der Außengrenzen Ausnahmeregelungen hinsichtlich der eingehenden Kontrolle in Anspruch nehmen können. Mitgliedstaaten, die sich freiwillig für diese Option entscheiden, sind verpflichtet, die Drittstaatsangehörigen, die die Aufnahme in das Programm beantragen, auf ihren Hintergrund zu überprüfen.

60. Der neue Artikel 8e verlangt ferner von der Kommission, vor Ablauf des dritten Jahres seiner Anwendung eine Bewertung seiner Umsetzung vorzunehmen. Auf der Grundlage dieser Bewertung können das Europäische Parlament oder der Rat die Kommission ersuchen, die Einrichtung eines *„Unionsprogramms für Vielreisende aus Drittstaaten vorzuschlagen, die auf ihren Hintergrund überprüft wurden“*. Der EDSB wird die weiteren Entwicklungen in dieser Angelegenheit sorgfältig beobachten.

61. Für nationale Erleichterungsprogramme müssen keine neuen Systeme entwickelt werden, da sie sich auf die im EES gespeicherten Daten stützen. Daher gewährt Artikel 23 des EES-Vorschlags von 2016 den in Artikel 8e genannten Behörden Zugang zu EES-Daten zum Zwecke der Prüfung von Anträgen auf Aufnahme in nationale Erleichterungsprogramme. Der EDSB empfiehlt, im Sinne der Kohärenz diesen Zweck in die Liste spezifischer Zwecke in Artikel 5 des EES-Vorschlags von 2016 aufzunehmen.

62. Abgesehen davon werden in dem neuen Artikel 8e keinerlei Sicherheitsvorkehrungen beschrieben und das Erfordernis der Sicherheit wird nicht einmal erwähnt. **Der EDSB empfiehlt eine klare Darstellung der Verantwortung für die Sicherheit in allen Phasen des Prozesses, auch für den Fall, dass freiwillige Programme aus verschiedenen Mitgliedstaaten an das EES angeschlossen werden. Ferner empfiehlt der EDSB, in dem neuen Artikel 8e des Schengener Grenzkodex zu bestimmen, dass die Sicherheit nach einer ordnungsgemäßen Risikobewertung der Informationssicherheit zu gewährleisten ist.**

f) Rechte der betroffenen Personen

63. Der EDSB begrüßt die Artikel 44 und 46 des EES-Vorschlags von 2016, in denen das Recht von Drittstaatsangehörigen auf Information sowie auf Auskunft über personenbezogene Daten und deren Berichtigung und Löschung geregelt ist.

64. Bedenken hegt der EDSB erstens bezüglich Artikel 46 Absatz 6 des Vorschlags, dem zufolge Ersuchen auf Auskunft, Berichtigung und Löschung personenbezogener Daten durch *alle* betroffenen Personen von der Abgabe ihrer Fingerabdrücke abhängig sind. Der EDSB sieht die Notwendigkeit, bei derartigen Ersuchen über personenbezogene Daten zu verfügen, die eine Identifizierung eines Drittstaatsangehörigen als der befugten betroffenen Person ermöglichen. Eine solche Bedingung könnte jedoch ein hohes Hindernis für die tatsächliche Ausübung des Auskunftsrechts darstellen, das für die betroffene Person eine wichtige Garantie

darstellt und sogar in Artikel 8 Absatz 2 der Charta erwähnt wird. **Der EDSB empfiehlt dem EU-Gesetzgeber, diese Bedingung für die Wahrnehmung des Auskunftsrechts noch einmal zu überdenken, beispielsweise indem die Verwendung von Fingerabdrücken auf Fälle beschränkt wird, in denen erhebliche Zweifel an der Identität des Antragstellers bestehen.**

65. Was das Recht auf Information angeht, begrüßt der EDSB die Tatsache, dass der EES-Vorschlag von 2016 nun ein gemeinsames Merkblatt und eine Website in mehreren Sprachen, möglicherweise mit zusätzlichen Informationen seitens der Mitgliedstaaten, zusätzlich zu den Informationen vorsieht, die Drittstaatsangehörige bereits zum Zeitpunkt der Anlage des Dossiers zu ihrer Person erhalten. Dessen ungeachtet **empfiehlt der EDSB, den in Artikel 44 Absatz 1 aufgelisteten Informationen noch folgende Punkte hinzuzufügen:**

1) eine Erläuterung bezüglich der Tatsache, dass die EES-Daten zu Zwecken des Grenzmanagements und der Erleichterung des Grenzübertritts abgerufen werden; den Hinweis, dass bei Überschreitung der zulässigen Aufenthaltsdauer die Daten der Person automatisch auf eine Liste gesetzt werden[60], sowie Angaben zu möglichen Konsequenzen der Überschreitung der zulässigen Aufenthaltsdauer;

2) die Datenspeicherfristen für Einreise- und Ausreisedatensätze und für Dossiers zu einer Person, und

3) das Recht von Overstayern auf Löschung ihrer personenbezogenen Daten, falls sie nachweisen können, dass sie die zulässige Aufenthaltsdauer wegen unvorhersehbarer, ernster Ereignisse überziehen mussten.[61]

66. Bezüglich des Rechts auf Auskunft **empfiehlt der EDSB die Festlegung einer streng harmonisierten Frist in Artikel 46 Absatz 1, die höchstens einige Monate für die Beantwortung von Ersuchen vorsieht**.[62] Die Wahrung des Rechts auf Auskunft, wie es in Artikel 8 der Charta garantiert ist, und die Bearbeitung von Auskunftsersuchen sind von großer Bedeutung, da betroffene Personen durch Ausübung dieses Rechts die Möglichkeit haben, die Verarbeitung ihrer personenbezogenen Daten zu kontrollieren und möglicherweise Fehler oder rechtswidrige Zugriffe auf ihre personenbezogenen Daten aufzudecken. Außerdem räumt Artikel 48 über „Rechtsbehelfe“ betroffenen Personen die Möglichkeit ein, eine Klage oder Beschwerde zu erheben, wenn das Recht auf Auskunft, Berichtigung und Löschung verweigert wird. Damit diese Rechte wirksam sind, sollte das Gleiche auch für Fälle gelten, in denen Ersuchen auf Ausübung dieser Rechte nicht streng fristgerecht beantwortet oder von dem für die Verarbeitung Verantwortlichen nie bearbeitet wurden.

67. Der EDSB begrüßt ferner Artikel 9 Absatz 2, der besagt, dass bei der Nutzung des EES Drittstaatsangehörige nicht aufgrund ihres Geschlechts, ihrer Rasse oder ethnischen Herkunft, ihrer Religion oder Weltanschauung, einer Behinderung, ihres Alters oder ihrer sexuellen Ausrichtung diskriminiert werden dürfen. Der EDSB begrüßt ebenfalls, dass der besonderen Situation von Kindern, älteren Menschen und Menschen mit Behinderungen ausdrücklich Rechnung getragen wird. Der Vorschlag enthält jedoch keine Aussagen dazu, mit welchen zusätzlichen Schutzvorkehrungen sichergestellt werden soll, dass der besonderen Situation von Kindern, älteren Menschen und Menschen mit Behinderungen tatsächlich Rechnung getragen wird. **Der EDSB empfiehlt, Artikel 9 Absatz 2 dahingehend zu ändern, dass er eine klare Beschreibung der Schutzvorkehrungen enthält, mit denen gewährleistet ist, dass**

Kindern, älteren Menschen und Menschen mit Behinderungen die angemessene Aufmerksamkeit geschenkt wird.

g) Statistiken

68. Der EDSB sieht durchaus die Notwendigkeit für dazu befugte Mitarbeiter der zuständigen Behörden der Mitgliedstaaten, der Kommission, von eu-LISA und Frontex, Berichte und Statistiken zu den Daten im EES zu erstellen. Anders als es in Artikel 57 Absatz 1 und Artikel 57 Absatz 2 heißt, könnte allerdings die Menge der abrufbaren Daten eine Identifizierung einzelner Personen ermöglichen. So kann beispielsweise die Kombination von Staatsangehörigkeit, Geschlecht und Geburtsdatum eines Drittstaatsangehörigen durchaus zu einer Identifizierung führen.

69. Da außerdem von eu-LISA die Extraktion dieser Daten und ihre Eingabe in ein Zentralregister verlangt wird, steigt das Risiko von Datenlecks spürbar an, zumal angemessene Sicherheitsvorkehrungen noch nicht erdacht wurden.

70. **Der EDSB empfiehlt daher eine Umformulierung von Artikel 57 „Verwendung von Daten zur Erstellung von Berichten und Statistiken“**, mit der eingeräumt wird, dass die in Artikel 57 Absatz 1 Buchstaben a bis i aufgelisteten Daten zu einer Identifizierung einzelner Personen führen können und daher ähnlich wie das Zentralregister des EES geschützt werden müssen. Das bedeutet, dass eine ordnungsgemäße Risikobewertung der Informationssicherheit durchgeführt werden muss und angemessene Sicherheitsvorkehrungen getroffen werden müssen, bevor dieses weitere Zentralregister bereitgestellt wird. Der EDSB warnt nachdrücklich davor, dass die derzeit in Artikel 57 vorgeschlagene Lösung eine große Belastung für eu-LISA darstellt, denn sie müsste ein zweites Register pflegen und angemessen sichern, aber auch für den EDSB, denn er müsste die Aufsicht über dieses zweite Register übernehmen. **Der EDSB würde eine Lösung bevorzugen, die kein weiteres Zentralregister erfordert, sondern eher von eu-LISA verlangt, Funktionalitäten zu entwickeln, die den Mitgliedstaaten, der Kommission, eu-LISA und Frontex die Möglichkeit gäben, die notwendigen Statistiken direkt aus dem EES-Zentralsystem zu extrahieren, ohne dass ein weiteres Register erforderlich wäre.**

h) Aufsicht durch den EDSB

71. In Artikel 50 des EES-Vorschlags von 2016 sind die Aufgaben des EDSB als Aufsichtsstelle des künftigen EES geregelt, zu denen gehört, dafür Sorge zu tragen, dass mindestens alle vier Jahre die Verarbeitung personenbezogener Daten durch eu-LISA in diesem neuen System geprüft wird.

72. Allerdings stattet der EES-Vorschlag von 2016 den EDSB nicht mit sachdienlichen Informationen dafür aus, dass der diese neuen Aufgaben wirksam und effizient wahrnehmen kann. Der EDSB sollte ebenfalls von eu-LISA von allen Berichten in Kenntnis gesetzt werden, die diese Agentur gemäß dem Vorschlag der Kommission, dem Rat oder dem Parlament vorzulegen hat. **Der EDSB empfiehlt daher Folgendes:**

- Artikel 36 Absatz 3 sollte besagen, dass der EDSB über die Maßnahmen unterrichtet wird, die eu-LISA gemäß Artikel 36 Absatz 2 ergreift, und zwar nicht nur bei der

Inbetriebnahme des EES, sondern während des gesamten Lebenszyklus des EES und seiner Daten;

- Artikel 64 Absatz 2 sollte besagen, dass der EDSB über die Berichte über den Stand der Entwicklung des Zentralsystems, der einheitlichen Schnittstellen und der Kommunikationsinfrastruktur zwischen dem Zentralsystem und den einheitlichen Schnittstellen informiert wird;

- Artikel 64 Absatz 4 sollte besagen, dass dem EDSB der Bericht über die technische Funktionsweise des EES alle zwei Jahre nach der Inbetriebnahme des Systems übergeben wird;

- Artikel 65 Absatz 5 sollte besagen, dass der EDSB den Bericht der Kommission über die Gesamtbewertung des EES erhält.

73. Des Weiteren **empfiehlt der EDSB, in Artikel 50 eine Artikel 49 Absatz 3 ähnliche Bestimmung aufzunehmen, damit der EDSB die Ressourcen erhält, die er für eine ordnungsgemäße Kontrolle dieses neuen Systems benötigt.**

IV. Zugang durch Gefahrenabwehr- und Strafverfolgungsbehörden

74. Der EES-Vorschlag von 2016 sieht vor, dass Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europol ab Inbetriebnahme des Systems Zugang zu ihm haben.[63] Das EES wird als Instrument für die Identifizierung von unbekannten Tatverdächtigen, Straftätern oder Opfern und als Instrument zur polizeilichen Erkenntnisgewinnung zur Abfrage von Daten zu bisherigen Reisen bekannter Tatverdächtiger dienen.

75. Der EDSB räumt ein, dass es für Gefahrenabwehr- und Strafverfolgungsbehörden wichtig ist, über die bestmöglichen Instrumente zum Auffinden von Terroristen oder anderen Schwerkriminellen zu verfügen. Dennoch erinnert der EDSB daran[64], dass bei der Gewährung des Zugangs zu EES-Daten für Gefahrenabwehr- und Strafverfolgungsbehörden zusätzlich das Recht von Drittstaatsangehörigen auf Privatsphäre und Datenschutz zu wahren ist und vorab ebenfalls die Notwendigkeit und Verhältnismäßigkeit zu prüfen sind.

76. Der EDSB erinnert daran[65], dass der Zugang zu EES-Daten für Gefahrenabwehr- und Strafverfolgungsbehörden zur steigenden Tendenz der Gewährung des Zugangs für diese Behörden zu personenbezogenen Daten von Drittstaatsangehörigen passt, die die EU-Grenzen übertreten[66], selbst wenn diese Reisenden grundsätzlich keines unrechtmäßigen Verhaltens verdächtigt werden oder sonstige Ermittlungen gegen sie laufen.

IV.1 Gefahrenabwehr und Strafverfolgung als sekundäres Ziel

77. Wie bereits erläutert[67], wird die EES-Datenbank in erster Linie für Zwecke des Grenzmanagements eingerichtet und Zugang zum EES kann dann Gefahrenabwehr- und Strafverfolgungsbehörden vorbehaltlich strenger Bedingungen und Garantien gewährt werden. **Nach Auffassung des EDSB wäre die Einrichtung des beschriebenen EES unmittelbar**

und primär für Strafverfolgungszwecke nicht hinnehmbar und das EES sollte ein Instrument für Grenzmanagement bleiben, das allein für diesen Zweck konzipiert wurde.

78. In Artikel 5 des EES-Vorschlags von 2016 werden jedoch 12 Zwecke für die *Erhebung*, die *Speicherung* und den Abruf von EES-Daten ausgeführt; die Zwecke j), k) und l) haben mit den sekundären Gefahrenabwehr- und Strafverfolgungszwecken des EES zu tun. **Der EDSB empfiehlt eine Änderung von Artikel 5, damit deutlich wird, dass das EES primäre und sekundäre Zwecke hat, sowie spezifische Zwecke im Zusammenhang mit Gefahrenabwehr und Strafverfolgung als sekundäre Zwecke in einer eigenständigen Bestimmung zu regeln, damit sie zumindest nicht gleichberechtigt neben den anderen Zwecken in den Bereichen Grenzmanagement und Erleichterung des Grenzübertritts aufgelistet werden.**

IV.2 Notwendigkeit des Zugangs für Gefahrenabwehr- und Strafverfolgungsbehörden

79. Der EDSB unterstreicht, dass allein die Tatsache, dass EES-Daten primär für bestimmte Zwecke erhoben wurden - und damit zur Verfügung stehen -, an sich nicht den Zugang zu diesen Daten und ihre Verwendung für andere Zwecke wie Gefahrenabwehr und Strafverfolgung rechtfertigt.[68] In diesem Zusammenhang hat der EDSB mehrfach empfohlen, die Notwendigkeit des Zugangs zu EES-Daten für Zwecke der Gefahrenabwehr und Strafverfolgung mit guten Argumenten zu begründen.[69]

80. Im aktuellen Vorschlag heißt es in Erwägungsgrund 16, dass es *„unerlässlich [ist], dass die Gefahrenabwehr- und Strafverfolgungsbehörden über die aktuellsten Informationen verfügen, um ihren Aufgaben gerecht werden zu können"*; und weiter ist dort die Rede von der bestehenden Möglichkeit des Zugriffs auf VIS-Daten zu Gefahrenabwehr- und Strafverfolgungszwecken, der *„sich bereits als zweckmäßig erwiesen [hat]."*[70] Der EDSB weist darauf hin, dass das, was als zweckmäßig gilt, nicht zwangsläufig auch aus Perspektive des Datenschutzes als notwendig betrachtet werden muss[71], und dass Aussagen zur Notwendigkeit mit eindeutigen Beweisen untermauert sein müssen.

81. In der Folgenabschätzung zum Vorschlag heißt es auch, dass das VIS tatsächlich von Gefahrenabwehr- und Strafverfolgungsbehörden genutzt wird (nämlich mit 14 000 Abfragen pro Monat in den ersten acht Monaten des Jahres 2015), und dass *„solche Abfragen zur Aufklärung schwerer Straftaten führen"*[72], ohne dass dies näher ausgeführt wird. Der EDSB stellt jedoch fest, dass nach Angaben in der Mitteilung der Kommission „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit" die Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten die Möglichkeit in Bezug auf den Zugang zum VIS in sehr unterschiedlichem Maße nutzen und überdies von praktischen Problemen bei den Verfahren berichten.[73] Und Europol hat zwar r*echtlich gesehen* seit Ende 2013 die Möglichkeit, auf das VIS zuzugreifen, doch ist es *de facto* nicht an die Datenbank angeschlossen und nutzt also diese Möglichkeit noch nicht.

82. **Der EDSB fordert die Kommission auf, weitere Informationen vorzulegen, wie beispielsweise verfügbare Berichte und/oder Statistiken zu den bisherigen Erfahrungen mit dem VIS (aber auch mit dem SIS und mit Eurodac), um diese Behauptungen zu stützen und um weitere objektive Nachweise zu erbringen, dass Gefahrenabwehr- und**

Strafverfolgungsbehörden, einschließlich Europols, wirklich den Zugriff auf EES-Daten benötigen.

IV.3 Bedingungen für den Zugang und Garantien

83. Sollte die Notwendigkeit dieses Zugangs festgestellt werden, wäre nachzuweisen, dass diese Weiterverarbeitung dem in Artikel 52 Absatz 1 der Charta verankerten Erfordernis der Verhältnismäßigkeit Genüge tut. Hierzu hat der EuGH Orientierungshilfe im DRI-Urteil[74] gegeben und dort ausgeführt, dass ein solcher Zugriff verhältnismäßig und eng gefasst sein muss und auf dem Verdacht gegen eine bestimmte Person beruhen muss. Dieser Zugriff darf nur unter strengen Bedingungen erfolgen, die den Zugriff auf bestimmte Fälle beschränken, und er muss mit angemessenen Garantien einhergehen.

84. Der EDSB begrüßt, dass in Artikel 29 des EES-Vorschlags von 2016 die Bedingungen für den Zugang von Gefahrenabwehr- und Strafverfolgungsbehörden zu EES-Daten über einen begründeten elektronischen Antrag festgelegt sind, und dass in Artikel 29 Absatz 2 weitere Bedingungen für den Zweck der Identifizierung von unbekannten Tatverdächtigen oder Straftätern und mutmaßlichen Opfern terroristischer oder sonstiger schwerer Straftaten genannt werden.

85. In Artikel 29 Absatz 2 heißt es, dass eine vorherige Suchabfrage nicht durchgeführt werden muss, wenn hinreichende Gründe für die Annahme vorliegen, dass ein Abgleich mit den Systemen der anderen Mitgliedstaaten nicht zur Verifizierung der Identität der betroffenen Person führen würde. Der EDSB kann nicht erkennen, wie eine benannte Behörde vorab, ohne Abfragen der Systeme der anderen Mitgliedstaaten durchgeführt zu haben, wissen kann, ob diese Systeme möglicherweise sachdienliche Daten enthalten. **Der EDSB fordert die Kommission auf, Artikel 29 Absatz 2 klarer zu formulieren.**

86. Der EDSB ist ferner der Ansicht, dass der Mechanismus zur Überprüfung der Einhaltung dieser Bedingungen für den Zugriff auf EES-Daten eine wichtige Vorkehrung zur Verhinderung unbefugten Zugriffs ist. Artikel 26 Absatz 3 des EES-Vorschlags überträgt die Verantwortung für die Überprüfung der Frage, ob die Zugangsbedingungen durch Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten eingehalten wurden, an benannte zentrale Zugangsstellen. Allerdings können benannte nationale Behörden, die um Zugriff auf EES-Daten ersuchen, und Prüfstellen, die diesen Zugriff gewähren, Teil der gleichen Behörden sein. In Artikel 26 Absatz 3 heißt es in der Tat: *„Die benannte Behörde und die zentrale Zugangsstelle können, wenn dies nach den nationalen Rechtsvorschriften zulässig ist, Teile der gleichen Organisation sein; die zentrale Zugangsstelle nimmt ihre Aufgaben gemäß dieser Verordnung jedoch unabhängig wahr“*; und weiter heißt es: *„Die zentrale Zugangsstelle ist von den benannten Behörden getrennt und nimmt bei der Wahrnehmung ihrer Prüftätigkeiten von diesen keine Anweisungen entgegen“*. **Der EDSB empfiehlt eine Änderung dieser Bestimmung dahingehend, dass vorgeschrieben wird, dass die benannten Behörden und die Prüfstelle nicht Teile der gleichen Organisation sein dürfen.** Die gleiche Empfehlung gilt für die Spezialeinheit aus Europol-Beamten, die von Europol gemäß Artikel 27 Absatz 2 als zentrale Zugangsstelle benannt wird. In Anbetracht der Besonderheiten von Europol sollte ein wirksamer Mechanismus gefunden werden, bei dem die vorherige Genehmigung zum Zugriff auf EES-Daten der Prüfung einer Stelle unterliegt, die von der benannten Behörde hinreichend unabhängig ist.[75]

87. Der EDSB betont, dass die Prüfstelle von der benannten Behörde tatsächlich unabhängig sein muss, um eine ordnungsgemäße Überprüfung der Einhaltung der Bedingungen vornehmen zu können. Diesbezüglich führte der EuGH im DRI-Urteil aus, der Zugang der zuständigen nationalen Behörden sollte *„einer vorherigen Kontrolle durch ein Gericht oder eine* unabhängige *Verwaltungsstelle [unterliegen], deren Entscheidung den Zugang zu den Daten und ihre Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll“*.[76]

88. Artikel 28 Absatz 2 regelt dringende Ausnahmefälle, bei denen erst nachträglich überprüft wird, ob alle Voraussetzungen gemäß Artikel 29 erfüllt sind. Nach Auffassung des EDSB sollten diese Ausnahmen so genau wie möglich geregelt werden. Im Vorschlag heißt es, dass die nachträgliche Überprüfung *„unverzüglich“* nach der Bearbeitung des Antrags durchgeführt wird. **Der EDSB empfiehlt, eine klare Frist für die Durchführung der Überprüfung festzulegen, die so bald wie möglich nach der Bearbeitung des Antrags beginnen sollte.**

89. Schließlich begrüßt der EDSB, dass in Artikel 44 Absatz 1 Buchstabe a dem Recht der betroffenen Person auf Information über den Zugriff von Gefahrenabwehr- und Strafverfolgungsbehörden besondere Aufmerksamkeit gewidmet wurde, denn dort heißt es, dass Drittstaatsangehörigen klar erläutert wird, dass die Möglichkeit des Zugriffs von Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und von Europol auf EES-Daten besteht.

4. SCHLUSSFOLGERUNG

90. Der EDSB begrüßt die im EES-Vorschlag von 2016 zum Ausdruck kommenden Bemühungen der Kommission, auf die im Zusammenhang mit dem Paket „Intelligente Grenzen“ von 2013 geäußerten Datenschutzbedenken einzugehen. Einige der Empfehlungen und Anmerkungen des EDSB aus seiner früheren Stellungnahme zu dem Paket wurden berücksichtigt, beispielsweise mit der Einführung von Ausweichverfahren bei technischen Problemen oder Systemausfall.

91. Der EDSB begrüßt die Bemühungen der Kommission um eine Rechtfertigung der Notwendigkeit der Einrichtung der EES-Regelung, spricht aber wichtige Empfehlungen aus, die unmittelbar mit deren Verhältnismäßigkeit zu tun haben, damit das EES in vollem Umfang der in Artikel 52 Absatz 1 der Charta formulierten wesentlichen Bedingung Genüge tut, nämlich sowohl erforderlich als auch verhältnismäßig zu sein. Er weist darauf hin, dass Notwendigkeit und Verhältnismäßigkeit der EES-Regelung sowohl insgesamt, unter Berücksichtigung der bereits in der EU bestehenden IT-Großsysteme, als auch spezifisch, für jeden Einzelfall dieser Drittstaatsangehörigen, zu bewerten sind, die rechtmäßige Besucher der EU sind. Seiner Ansicht nach sollte eine Speicherfrist von fünf Jahren für alle im EES gespeicherten personenbezogenen Daten besser begründet werden. Er unterstreicht ferner, dass die folgenden Aspekte des EES-Vorschlags von 2016 besser begründet und durch überzeugende Nachweise unterstützt werden sollten: die Erfassung von Gesichtsbildern von visumpflichtigen Reisenden, die fünfjährige Speicherfrist für Overstayer und die Notwendigkeit des Zugriffs auf EES-Daten durch Gefahrenabwehr- und Strafverfolgungsbehörden. Falls dies nicht geschieht, sollten diese Aspekte vom EU-Gesetzgeber erneut geprüft werden.

92. In Anbetracht der vielfältigen Eingriffe in die Grundrechte von Drittstaatsangehörigen auf Privatsphäre und Datenschutz vertritt der EDSB die Ansicht, dass das EES ein Instrument des Grenzmanagements bleiben sollte, das ausschließlich zu diesem Zweck konzipiert wurde. Daher sollte die Unterscheidung zwischen den erklärten Zielen des EES, also den primären Zielen des Grenzmanagements und der Erleichterung des Grenzübertritts und dem sekundären Ziel der Gefahrenabwehr und Strafverfolgung, im EES-Vorschlag von 2016 klar eingeführt und dort durchgängig aufrechterhalten werden, insbesondere mit Blick auf die Artikel 1 und 5.

93. Des Weiteren hegt der EDSB Bedenken bezüglich der für alle betroffenen Personen geltenden Bedingung, zur Einreichung eines Antrags auf Auskunft über ihre personenbezogenen Daten und deren Berichtigung und Löschung auf jeden Fall ihre Fingerabdrücke abnehmen zu lassen. Dies könnte ein hohes Hindernis für die tatsächliche Ausübung des Auskunftsrechts darstellen, das für die betroffene Person eine wichtige Garantie darstellt und in Artikel 8 Absatz 2 der EU-Charta erwähnt wird.

94. Weitere Empfehlungen des EDSB in dieser Stellungnahme betreffen die folgenden Aspekte und Artikel:

- Artikel 14 sollte dahingehend näher ausgeführt werden, dass in Fällen, in denen Gesichtsbilder von Drittstaatsangehörigen vor Ort aufgenommen werden, bei diesen Bildern eine Mindestqualität erreicht wird, und in Artikel 33 sollte festgelegt werden, dass die Kommission detaillierte Informationen dazu bereitstellt, wie die erforderliche Qualität bei den vor Ort aufgenommenen Gesichtsbildern zu erreichen ist.

- Artikel 15 Absatz 3 sollte so geändert werden, dass klar hervorgeht, welche Informationen von den Grenzbehörden erhoben, gespeichert und verwendet werden dürfen, wenn sie nähere Angaben zu den Gründen der vorübergehenden Unmöglichkeit der Abnahme von Fingerabdrücken erfragen.

- Artikel 39 sollte die klare Notwendigkeit einer Koordinierung zwischen eu-LISA und Mitgliedstaaten im Hinblick auf die Sicherheit des EES unterstreichen.

- Für den Fall eines Anschlusses nationaler Erleichterungsprogramme von Mitgliedstaaten an das EES sollten die Verantwortlichkeiten für die Sicherheit klar festgelegt werden. Im neuen Artikel 8e des Schengener Grenzkodex sollte festgelegt werden, dass Sicherheit nach einer ordnungsgemäßen Risikobewertung der Informationssicherheit gewährleistet werden muss, und es sollten die erforderlichen Sicherheitsvorkehrungen beschrieben werden.

- Der Vorschlag sollte eindeutig besagen, dass eu-LISA für die Sicherheit des Web-Dienstes, die Sicherheit der darin enthaltenen personenbezogenen Daten und das Verfahren verantwortlich ist, mit dem die personenbezogenen Daten aus dem Zentralsystem in den Web-Dienst eingespeist werden.

- Artikel 44 Absatz 1 sollte dahingehend geändert werden, dass er die den betroffenen Personen bereitgestellten Informationen enthält, also Angaben zur Speicherfrist für ihre Daten, den Hinweis auf das Recht von Overstayern auf Löschung ihrer personenbezogenen Daten, falls sie nachweisen können, dass sie die zulässige Aufenthaltsdauer wegen unvorhersehbarer, ernster Ereignisse überziehen mussten, und

eine Erläuterung bezüglich der Tatsache, dass die EES-Daten zu Zwecken des Grenzmanagements und der Erleichterung des Grenzübertritts abgerufen werden.

- In Artikel 46 Absatz 1 sollte eine streng harmonisierte Frist festgelegt werden, die höchstens einige Monate für die Beantwortung von Ersuchen vorsieht.

- Artikel 9 Absatz 2 sollte dahingehend geändert werden, dass er eine klare Beschreibung der Schutzvorkehrungen enthält, mit denen gewährleistet ist, dass Kindern, älteren Menschen und Menschen mit Behinderungen die angemessene Aufmerksamkeit geschenkt wird.

- Artikel 57 sollte geändert werden und von eu-LISA verlangen, Funktionalitäten zu entwickeln, die den Mitgliedstaaten, der Kommission, eu-LISA und Frontex die Möglichkeit gäben, die notwendigen Statistiken direkt aus dem EES-Zentralsystem zu extrahieren, ohne dass ein weiteres Register erforderlich wird.

- Der Vorschlag sollte den EDSB mit sachdienlichen Informationen und den Ressourcen dafür ausstatten, dass er seine neuen Aufgaben als Kontrolleur des künftigen EES wirksam und effizient wahrnehmen kann.

- Artikel 28 Absatz 2 sollte der Prüfstelle eine klare Frist für die Durchführung der nachträglichen Überprüfung der Bedingungen für den Zugriff auf EES-Daten für Zwecke der Gefahrenabwehr und Strafverfolgung im Notfall setzen.

- Artikel 28 Absatz 3 sollte dahingehend geändert werden, dass vorgeschrieben wird, dass benannte Behörden und Prüfstellen nicht Teile der gleichen Organisation sein dürfen.

95. Der EDSB unterstreicht nachdrücklich, dass alle diese Fragen aus einer Gesamtperspektive zu betrachten sind. Er ermutigt den Gesetzgeber, mit der Bestandsaufnahme bei den im Bereich Grenzen und Migration bestehenden Datenbanken fortzufahren, dabei die Systeme besser zu koordinieren, Überschneidungen zwischen ihnen zu vermeiden und in vollem Umfang die Datenschutznormen einzuhalten, auch in seinen Beziehungen mit Drittländern.

Brüssel, den 21. September 2016

(**gezeichnet)**

Giovanni BUTTARELLI
Europäischer Datenschutzbeauftragter

VERWEISE

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 8 vom 12.1.2001, S. 1.
[3] ABl. L 350 vom 30.12.2008, S. 60.
[4] Mitteilung der Kommission vom 13. Februar 2008 „Vorbereitung der nächsten Schritte für die Grenzverwaltung in der Europäischen Union“, KOM(2008) 69 endgültig.
[5] Vorläufige Kommentare des EDSB vom 3. März 2008 zu drei Mitteilungen zum Thema Grenzverwaltung.
[6] Stellungnahme des EDSB vom 7. Juli 2011 zu der Mitteilung zur Migration.
[7] Mitteilung der Kommission vom 25. Oktober 2011 „Intelligente Grenzen: Optionen und weiteres Vorgehen“, KOM(2011) 680 endgültig.
[8] Die Artikel 29-Datenschutzgruppe äußerte sich zu der Mitteilung der Kommission über Intelligente Grenzen in einem Schreiben an Kommissionsmitglied Malmström vom 12. Juni 2012.
[9] Runder Tisch des EDSB zum Paket „Intelligente Grenzen“ und den Auswirkungen auf den Datenschutz, Brüssel, 10. April 2013, siehe die Zusammenfassung unter: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/2013/13-04-10_Summary_smart_borders_final_EN.pdf
[10] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates für ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten der Europäischen Union, COM(2013) 95 final.
[11] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Registrierungsprogramm für Reisende, COM(2013) 97 final.
[12] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 562/2006 in Bezug auf die Nutzung des Einreise-/Ausreisesystems (EES) und des Programms für registrierte Reisende (RTP), COM(2013) 96 final.
[13] Stellungnahme des EDSB vom 18. Juli 2013 zu den Vorschlägen für eine Verordnung über ein Einreise-/Ausreisesystem (EES) und für eine Verordnung über ein Registrierungsprogramm für Reisende (RTP).
[14] Artikel 29-Datenschutzgruppe, Stellungnahme 05/2013 vom 6. Juni 2013 zu intelligenten Grenzen.
[15] Technische Studie zu „Intelligente Grenzen“ - Abschlussbericht, Oktober 2014, abrufbar unter: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_technical_study_en.pdf
[16] Technische Studie zu „Intelligente Grenzen“ - Kostenanalyse, Oktober 2014, abrufbar unter: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_study_en.pdf
[17] eu-LISA, Abschlussbericht über das Pilotprojekt „Intelligente Grenzen“, Dezember 2015, abrufbar unter: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm
[18] Öffentliche Konsultation der Kommission zu „Intelligente Grenzen“, abrufbar unter: http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/consulting_0030_en.htm
[19] Formelle Kommentare des EDSB vom 3. November 2015 zur öffentlichen Konsultation der Europäischen Kommission zum Thema „Intelligente Grenzen“.
[20] Siehe die Pressemitteilung, abrufbar unter: http://europa.eu/rapid/press-release_IP-16-1247_de.htm
[21] Mitteilung der Kommission vom 6. April 2016 „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“, COM(2016) 205 final.
[22] COM (2016) 194 final.
[23] Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex) (kodifizierter Text), ABl. L 77 vom 23.3.2016, S. 1.
[24] COM(2016) 196 final.
[25] Arbeitsunterlage der Kommissionsdienststellen vom 6. April 2016 „Folgenabschätzung der Einrichtung eines Einreise-/Ausreisesystems der EU zum EES-Vorschlag von 2016 und zum Vorschlag von 2016 zur Änderung des Schengener Grenzkodex“, SWD(2016) 115 final (nachstehend „Folgenabschätzung“).
[26] http://data.consilium.europa.eu/doc/document/ST-8485-2016-INIT/en/pdf
[27] 2015 fanden zwei Workshops von GD HOME und EDSB zu Aspekten intelligenter Grenzen statt: ein Workshop am 20. März, in dem es ganz konkret um die Vorbereitung der Vorschläge für „Intelligente Grenzen“ ging, und ein interaktiver Workshop am 21. September 2015 über Erwägungen zum Datenschutz und zum Schutz der Privatsphäre bei Maßnahmen im Bereich Migration und Inneres, in dessen Verlauf auch die Vorschläge zu

„Intelligente Grenzen“ von 2013 gestreift wurden; siehe das Protokoll des Workshops vom 20. März 2015 in Anhang 16 der Folgenabschätzung.

[28] In Artikel 3 Nummer 1 Ziffer 18 des EES-Vorschlags von 2016 ist ein „Overstayer“ definiert als *„ein [...] Drittstaatsangehöriger, der die Bedingungen für den Kurzaufenthalt im Hoheitsgebiet der Mitgliedstaaten nicht oder nicht mehr erfüllt“*.

[29] Der EES-Vorschlag von 2016 nimmt von seinem Anwendungsbereich Drittstaatsangehörige aus, die unter die Richtlinie 2004/38/EG fallen und im Besitz der entsprechenden Aufenthaltskarte sind, ferner Inhaber eines Aufenthaltstitels gemäß Artikel 2 Nummer 16 des kodifizierten Schengener Grenzkodex, Inhaber eines Visums für den längerfristigen Aufenthalt, Staatsangehörige von Andorra, Monaco und San Marino sowie Personen oder Personengruppen, die von der Erleichterung des Grenzübertritts gemäß dem Schengener Grenzkodex ausgenommen sind oder denen eine solche gewährt wird (Artikel 2 Absatz 3).

[30] Siehe S. 5 der Folgenabschätzung.

[31] In den Artikeln 14 bis 18 des EES-Vorschlags sind erschöpfend die personenbezogenen Daten aufgelistet, die im EES sowohl für visumpflichtige als auch visumbefreite Drittstaatsangehörige erhoben und gespeichert werden.

[32] Siehe S. 34 der Folgenabschätzung, der zufolge z. B. Geburtsname und Geburtsort im künftigen EES nicht länger erfasst werden sollen.

[33] Artikel 29-Datenschutzgruppe, Stellungnahme 03/2012 zu Entwicklungen im Bereich biometrischer Technologien; EGMR, S. und Marper gegen Vereinigtes Königreich, 4. Dezember 2008, Beschwerden Nrn. 30562/04 und 30566/04, Randrn. 84-85, in denen der Europäische Gerichtshof für Menschenrechte befand, dass Fingerabdrücke *„objektiv einzigartige Informationen über die betreffende Person enthalten, die unter den vielfältigsten Umständen ihre genaue Identifizierung ermöglichen“,* und dass die Speicherung solcher Daten aus dem Blickwinkel der Privatsphäre höchst bedenklich sein könnte.

[34] Siehe S. 2 und 3 der Begründung des EES-Vorschlags von 2016.

[35] Siehe S. 58 und S. 65 der Folgenabschätzung; Grenzmanagement und Erleichterung des Grenzübertritts werden auf S. 65 des Dokuments auch als *„der vorrangige Zweck des EES“* bezeichnet. Ebenso ist in Anhang 13 der Folgenabschätzung („Folgenabschätzung bezüglich der Grundrechte“) vom *„primären Ziel“* die Rede.

[36] Siehe S. 37 der Folgenabschätzung; Gefahrenabwehr und Strafverfolgung wird auch auf S. 38 und *S.* 65 des Dokuments als *„der sekundäre Zweck“* bezeichnet. Ebenso ist in Anhang 13 der Folgenabschätzung („Folgenabschätzung bezüglich der Grundrechte“) vom *„sekundären Ziel“* die Rede.

[37] Siehe weiter unten die Punkte 28, 35 und 82.

[38] Siehe weiter oben Abschnitt I „ Auswirkungen des EES auf Privatsphäre und Datenschutz“.

[39] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland (C-293/12) und Seitlinger (C-594/12), ECLI:EU:C:2014:238 (nachstehend „DRI-Urteil“).

[40] Siehe Anhang 13 der Folgenabschätzung („Folgenabschätzung bezüglich der Grundrechte“), S. 127.

[41] Der EES-Vorschlag von 2013 sah eine maximale Speicherfrist für die Daten von 180 Tagen vor (Artikel 20).

[42] Der Vorschlag unterscheidet zwischen sogenannten „Dossiers zu einer Person“, die „Identitätsdaten“ (z. B. Namen, Geburtsdatum usw.), Angaben zum Pass und biometrische Daten enthalten, und Ein-/Ausreisedatensätzen oder Einreiseverweigerungsdatensätzen, in denen Datum und Ort der Ein-/Ausreise oder Einreiseverweigerung erfasst sind.

[43] DRI-Urteil, Randnr. 64.

[44] Siehe S. 37 der Folgenabschätzung.

[45] Falls beispielsweise ein Drittstaatsangehöriger die Ehe mit einem EU-Bürger schließt.

[46] Siehe Artikel 20 Absatz 3 des EES-Vorschlags von 2013.

[47] Erwägungsgrund 27 des EES-Vorschlags von 2016 hält diese Speicherfrist für erforderlich, *„damit diese Personen leichter identifiziert und rückgeführt werden können“*.

[48] Stellungnahme des EDSB vom 18. Juli 2013, Punkt 76; formelle Kommentare des EDSB vom 3. November 2015, S. 9.

[49] Siehe S. 6 der Begründung des EES-Vorschlags von 2016 und Artikel 24 Absatz 3 der SIS II-Verordnung, wo es heißt: *„Eine Ausschreibung kann auch eingegeben werden, wenn die Entscheidung nach Absatz 1 darauf beruht, dass der Drittstaatsangehörige ausgewiesen, zurückgewiesen oder abgeschoben worden ist, wobei die Maßnahme nicht aufgehoben oder ausgesetzt worden sein darf, ein Verbot zur Einreise oder gegebenenfalls ein Verbot des Aufenthalts enthalten oder davon begleitet sein muss und auf der Nichtbeachtung der nationalen Rechtsvorschriften über die Einreise oder den Aufenthalt von Drittstaatsangehörigen beruhen muss“*.

[50] Siehe Artikel 10 und 11 des EES-Vorschlags von 2013.

[51] Siehe S. 30 der Folgenabschätzung.

[52] Siehe Anhang 13 der Folgenabschätzung („Folgenabschätzung bezüglich der Grundrechte“), S. 125.

[53] Stellungnahme des EDSB vom 18. Juli 2013, Punkt 64, und formelle Kommentare des EDSB vom 3. November 2015, S. 6.

[54] Die Ermittlung als Overstayer in der EU könnte beispielsweise zur Folge haben, dass später ein anderes Visum verweigert wird, wenn die Person irgendwann das Hoheitsgebiet der EU verlassen hat und dann zurückkehren

möchte, oder sie könnte auch ein Grund für die Rückführung des Drittstaatsangehörigen in sein Herkunftsland sein.

[55] Stellungnahme des EDSB vom 7. Juli 2013, Punkt 31, formelle Kommentare des EDSB vom 3. November 2015, S. 6, und Stellungnahme des EDSB vom 19. Oktober 2005 zu drei Vorschlägen betreffend das Schengener Informationssystem der zweiten Generation (SIS II), Abschnitt 4.1 über biometrische Daten.

[56] Anhang 13 der Folgenabschätzung („Folgenabschätzung bezüglich der Grundrechte").

[57] Mitteilung der Kommission vom 6. April 2016 „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit", COM(2016) 205 final, S. 17.

[58] Siehe S. 5 der Begründung des EES-Vorschlags von 2016.

[59] Siehe weiter oben Punkt 35.

[60] Siehe Artikel 11 des EES-Vorschlags von 2016.

[61] Siehe Artikel 32 Absatz 5 des EES-Vorschlags von 2016.

[62] Artikel 12 der Richtlinie 95/46/EG.

[63] Der EES-Vorschlag von 2013 sah einen solchen Zugang als mögliche Option an, die nach einer Bewertung des Systems zwei Jahre nach dessen Inbetriebnahme hätte realisiert werden können.

[64] Anhang 16 zur Folgenabschätzung „Vorbereitende Arbeiten mit dem Europäischen Datenschutzbeauftragten", S. 142.

[65] Stellungnahme des EDSB vom 18. Juli 2013, Punkt 68, und formelle Kommentare des EDSB vom 3. November 2015, S. 5.

[66] Diese Tendenz hat sich in den letzten Jahren abgezeichnet und dürfte in der allernächsten Zukunft im Zusammenhang mit der vorgeschlagenen ECRIS-Verordnung, mit der das bestehende System auf Strafregisterauszüge von Drittstaatsangehörigen ausgedehnt wird, und im Zusammenhang mit der vorgeschlagenen Neufassung 2016 der Eurodac-Verordnung noch deutlicher hervortreten, die die Zweckbestimmungen des Systems erweitern und damit auch die Datenmenge vergrößern wird, zu der nationale Gefahrenabwehr- und Strafverfolgungsbehörden möglicherweise Zugang haben.

[67] Siehe weiter oben Punkt 20.

[68] Artikel 29-Datenschutzgruppe, Stellungnahme 03/2013 zur Zweckbindung.

[69] Stellungnahme des EDSB vom 18. Juli 2013, Punkt 69, und formelle Kommentare des EDSB vom 3. November 2015, S. 4 und 10.

[70] Erwägungsgrund 16 des EES-Vorschlags von 2016.

[71] Der EGMR befand, dass der Begriff Notwendigkeit nicht so flexibel ist wie *„zulässig"*, *„normal"* oder *„hilfreich"*, dass er aber *„ein dringendes gesellschaftliches Bedürfnis impliziert"*; siehe EGMR, Handyside gegen Vereinigtes Königreich, 7. Dezember 1976, Beschwerde Nr. 5493/72, Randnr. 48.

[72] Siehe S. 67 der Folgenabschätzung.

[73] Mitteilung der Kommission vom 6. April 2016 „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit", COM(2016) 205 final, S. 10.

[74] DRI-Urteil, Randrn. 58-68.

[75] Zur gleichen Argumentation siehe Punkt 58 der Stellungnahme 7/2016 des EDSB vom 21. September 2016 zum ersten Reformpaket für das Gemeinsame Europäische Asylsystem.

[76] DRI-Urteil, Randnr. 62.