

Stellungnahme des Europäischen Datenschutzbeauftragten

zu den Vorschlägen für eine Verordnung über ein Einreise-/Ausreisensystem (EES) und für eine Verordnung über ein Registrierungsprogramm für Reisende (RTP)

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 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr¹,

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 Datenverkehr²,

gestützt auf ein Ersuchen um eine Stellungnahme gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

I.1. Konsultation des EDSB

1. Am 28. Februar 2013 nahm die Kommission folgende Vorschläge an („die Vorschläge“):
 - Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Einreise-/Ausreisensystem (EES) zur Erfassung der Ein- und Ausreisedaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten der Europäischen Union („EES-Vorschlag“)³;

¹ ABl. L 281 vom 23.11.1995, S. 31.

² ABl. L 8 vom 12.1.2001, S. 1.

³ COM(2013) 95 final.

- Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Registrierungsprogramm für Reisende („RTP-Vorschlag“)⁴;
 - 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-/Ausreisensystems (EES) und des Programms für registrierte Reisende (RTP) („Änderungsvorschlag“)⁵.
2. Noch am selben Tag wurden die Vorschläge dem EDSB zur Konsultation übermittelt. Noch vor der Annahme der Vorschläge hatte der EDSB Gelegenheit, der Kommission gegenüber informelle Kommentare abzugeben.
 3. Der EDSB begrüßt, dass seine Konsultation in der Präambel sowohl des EES-Vorschlags als auch des RTP-Vorschlags erwähnt wird.

I.2. Hintergrund

4. In ihrer Mitteilung aus dem Jahr 2008 „Vorbereitung der nächsten Schritte für die Grenzverwaltung in der Europäischen Union“ schlug die Kommission neue Instrumente für das künftige Management europäischer Grenzen vor, unter anderem ein Einreise-/Ausreisensystem („EES“) zur elektronischen Erfassung der Ein- und Ausreisedaten von Drittstaatsangehörigen und ein Programm für registrierte Reisende („RTP“), mit dem Bona-Fide-Reisenden der Grenzübertritt erleichtert werden soll. Ferner wurde die Einführung eines Systems zur elektronischen Erteilung von Reisebewilligungen (ESTA) für von der Visumpflicht befreite Drittstaatsangehörige erwogen.
5. Diese Vorschläge wurden vom Europäischen Rat vom Dezember 2009 im Stockholmer Programm⁶ gebilligt. In ihrer Mitteilung von 2011 über intelligente Grenzen⁷ kam die Kommission hingegen zu dem Schluss, dass die Idee der Einführung eines ESTA vorerst nicht weiter verfolgt werden sollte, weil „der potenzielle Sicherheitsgewinn für die Mitgliedstaaten weder eine derart umfangreiche Erhebung personenbezogener Daten noch die finanziellen Kosten und die zu erwartenden Auswirkungen auf die internationalen Beziehungen rechtfertigen würde.“⁸ Ferner kündigte sie für die erste Hälfte des Jahres 2012 die Vorlage von Vorschlägen für ein EES und ein RTP an.

⁴ COM(2013) 97 final.

⁵ COM(2013) 96 final.

⁶ „Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger“, ABl. C 115 vom 4.5.2010, S. 1.

⁷ Mitteilung der Kommission vom 25. Oktober 2011 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Intelligente Grenzen: Optionen und weiteres Vorgehen“, (KOM(2011) 680 endgültig).

⁸ Vorstehend zitierte Mitteilung der Kommission über intelligente Grenzen, S. 7.

6. Danach forderte der Europäische Rat vom Juni 2011 ein rasches Vorantreiben der Arbeiten an „intelligenten Grenzen“ und forderte die Einführung des EES und des RTP⁹.

⁹ EUCO 23/11.

7. Die Artikel 29-Datenschutzgruppe äußerte sich zu der Mitteilung der Kommission über intelligente Grenzen, die den Vorschlägen vorausging, in einem Schreiben an Kommissarin Malmström vom 12. Juni 2012¹⁰. Erst vor Kurzem, nämlich am 6. Juni 2013, nahm die Datenschutzgruppe eine Stellungnahme an, in der die Notwendigkeit des Pakets „Intelligente Grenzen“ in Frage gestellt wird¹¹.
8. Die vorliegende Stellungnahme baut auf diesen Positionen sowie einer früheren Stellungnahme des EDSB¹² zur Mitteilung der Kommission zur Migration aus dem Jahr 2011¹³ und auf den vorläufigen Kommentaren des EDSB¹⁴ zu drei Mitteilungen über Grenzverwaltung (2008) auf¹⁵. Ferner verwendet er Beiträge des Runden Tisches des EDSB zum Paket „Intelligente Grenzen“ und den Auswirkungen auf den Datenschutz¹⁶.

I.3. Ziel der Vorschläge

9. In Artikel 4 des EES-Vorschlags wird dessen Zweck beschrieben. Zweck des Vorschlags ist es, die Verwaltung der Außengrenzen der EU und die Bekämpfung der irregulären Zuwanderung, die Umsetzung einer integrierten Grenzverwaltungspolitik und die Zusammenarbeit und Konsultation zwischen den Grenz- und den Einwanderungsbehörden zu verbessern. Er sieht ein System vor, das folgenden Zwecken dient:

¹⁰ Die gemäß der Richtlinie 95/46/EG eingesetzte Artikel 29-Datenschutzgruppe besteht aus je einem Vertreter der nationalen Datenschutzbehörden, dem EDSB sowie einem Vertreter der Europäischen Kommission. Sie hat beratende Funktion und handelt unabhängig. Das Schreiben der Datenschutzgruppe vom 12. Juni 2012 an Frau Cecilia Malmström zum Thema „Intelligente Grenzen“ ist abrufbar unter:

http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120612_letter_to_malmstrom_smart-borders_en.pdf.

¹¹ Stellungnahme 05/2013 der Artikel 29-Datenschutzgruppe zu Intelligenten Grenzen.

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp206_en.pdf

¹² Stellungnahme des EDSB vom 7. Juli 2011, abrufbar unter http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/07.07.11_pharmacovigilance_DE.pdf.

¹³ Mitteilung der Kommission vom 4. Mai 2011 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zur Migration (KOM(2011) 248/3)

¹⁴ Vorläufige Kommentare des EDSB vom 3. März 2008, abrufbar unter http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf.

¹⁵ Mitteilungen der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Vorbereitung der nächsten Schritte für die Grenzverwaltung in der Europäischen Union“ (KOM(2008) 69 endgültig), „Prüfung der Schaffung eines Europäischen Grenzkontrollsystems (EUROSUR)“ (KOM(2008) 68 endgültig) und „Bericht über die Evaluierung und künftige Entwicklung der Agentur FRONTEX“ (KOM(2008) 67 endgültig).

¹⁶ Runder Tisch des EDSB zum Paket „Intelligente Grenzen“ und zu den Auswirkungen auf den Datenschutz, Brüssel, 10. April 2013, am Sitz des EDSB, Rue Montoyer 30, Brüssel. 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

- a. Verbesserung der Kontrollen an den Grenzübergangsstellen und Bekämpfung der irregulären Zuwanderung;
 - b. Berechnung und Überwachung der zulässigen Aufenthaltsdauer von Drittstaatsangehörigen bei Kurzaufenthalten;
 - c. Erleichterung der Identifizierung von Personen, die die Voraussetzungen für die Einreise in das Hoheitsgebiet der Mitgliedstaaten oder den dortigen Aufenthalt nicht beziehungsweise nicht mehr erfüllen;
 - d. Ermöglichung der Identifizierung von Overstayern und der Ergreifung der erforderlichen Maßnahmen durch die Behörden der Mitgliedstaaten;
 - e. Erfassung von Daten über die Ein- und Ausreise von Drittstaatsangehörigen zum Zweck der statistischen Analyse.
10. Das System soll durch die rasche Bereitstellung präziser Informationen für Grenzschutzbeamte und Reisende bei der Überwachung der zulässigen Aufenthaltsdauer helfen. Es würde das derzeitige System des manuellen Abstempeln von Reisepässen ablösen, das als schwerfällig und unzuverlässig gilt, und so effizientere Grenzkontrollen ermöglichen¹⁷.
 11. Weiter soll es durch die Speicherung biometrischer Daten bei der Identifizierung von Personen helfen, die die Voraussetzungen für die Einreise in die EU oder einen dortigen Aufenthalt nicht erfüllen, vor allem, wenn sie über keine Ausweispapiere verfügen. Das EES böte darüber hinaus präzise Informationen über die Reiseströme und die Zahl der Overstayer und würde damit faktengestützte politische Entscheidungen ermöglichen, beispielsweise über die Visumpflicht. Die in Artikel 4 erwähnten Statistiken werden für diesen zuletzt genannten Zweck verwendet.
 12. Das EES wäre die Grundlage für das RTP und diene der Erleichterung des Grenzübertritts für vorab überprüfte Vielreisende aus Drittländern. Ein registrierter Reisender soll einen Token mit einer ihm zugewiesenen Kennnummer erhalten, der bei der Ein- und Ausreise an der Grenze an einer automatischen Schleuse durchgezogen werden muss. Die Daten des Token, die Fingerabdrücke und gegebenenfalls die Nummer der Visummarke werden mit den im Zentralregister und anderen Datenbanken gespeicherten Informationen abgeglichen. Verlaufen alle Kontrollen positiv, kann der Reisende die automatische Schleuse passieren. Ansonsten hilft ein Grenzbeamter dem Reisenden.
 13. Der Änderungsvorschlag schließlich verfolgt den Zweck, die Verordnung (EG) Nr. 562/2006 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen („Schengener Grenzkodex“) an die neuen EES- und RTP-Vorschläge anzupassen.

¹⁷ Siehe die Begründung des EES-Vorschlags.

I.4. Hintergrund und Struktur der Stellungnahme

14. Das Projekt zur Entwicklung eines elektronischen Systems für die Überwachung der Einreise in das und der Ausreise aus dem Hoheitsgebiet der Europäischen Union ist nichts Neues, und mehrere vorstehend zitierte Mitteilungen der Kommission haben den nun hier zu prüfenden Vorschlägen den Weg bereitet. Das Paket „Intelligente Grenzen“ ist daher mit Blick auf diese Entwicklungen zu beurteilen. Dabei sind insbesondere folgende Elemente zu berücksichtigen.
15. Im Stockholmer Programm hat sich die Kommission für den strategischen Ansatz entschieden, gestützt auf eine Evaluierung des bestehenden Instrumentariums den Bedarf an der Entwicklung eines europäischen Modells für den Informationsaustausch zu analysieren. Zur Grundlage dieses Modells sollen unter anderem eine starke Datenschutzregelung, ein System der gezielten Datenerhebung und eine Straffung der verschiedenen Instrumente einschließlich der Annahme eines Geschäftsplans für IT-Großsysteme gehören. Im Stockholmer Programm wird auf die notwendige Kohärenz zwischen der Anwendung und Verwaltung der verschiedenen Informationsinstrumente und der Strategie für den Schutz personenbezogener Daten und dem Geschäftsplan für den Aufbau von IT-Großsystemen hingewiesen¹⁸.
16. Eine umfassende Analyse ist erst recht mit Blick auf die Existenz, Weiterentwicklung und Nutzung von IT-Großsystemen wie Eurodac¹⁹, VIS²⁰ und SIS II²¹ erforderlich. Ein System „Intelligente Grenzen“ ist ein weiteres Instrument, mit dem sich aus der Sicht der Grenzkontrolle große Mengen personenbezogener Daten erheben lassen. Dieser Gesamtansatz wurde kürzlich vom JI-Rat bestätigt, der die Notwendigkeit unterstrich, insbesondere mit Blick auf die Explosion der Kosten von den Erfahrungen mit SIS zu lernen²². Auch der EDSB führte aus, dass in Anbetracht der

¹⁸ Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, ABl. C 115 vom 3.3.2010, S. 1.

¹⁹ Siehe 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. 04/2013 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 Europol 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, ABl. L 180 vom 29.6.2013.

²⁰ Siehe Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung), ABl. L 218 vom 13.8.2008, S. 60.

²¹ Siehe Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 381 vom 28.12.2006, S. 4.

²² Siehe Dokument des Rates Nr. 8018/13, Vermerk des Vorsitzes an den Strategischen Ausschuss für Einwanderung, Grenzen und Asyl/Gemischter Ausschuss (EU-Island/Liechtenstein/Norwegen/Schweiz), 28. März 2013, zum Paket „Intelligente Grenzen“.
<http://www.statewatch.org/news/2013/apr/eu-council-smart-borders-8018-13.pdf>

beinahe grenzenlosen Möglichkeiten, die die neuen Technologien bieten, „ein europäisches Informationsmodell nicht allein auf technischen Überlegungen basieren darf“. Informationen sollten lediglich bei Vorliegen eines konkreten Bedarfs aus Sicherheitsgründen verarbeitet werden²³.

17. Die Analyse von EES und RTP aus dem Blickwinkel des Schutzes der Privatsphäre und des Datenschutzes hat vor dem Hintergrund der Charta der Grundrechte der Europäischen Union²⁴ („Charta“) und insbesondere deren Artikel 7 und 8 zu erfolgen. Artikel 7, der Artikel 8 der Europäischen Menschenrechtskonvention²⁵ (EMRK) ähnlich ist, sieht ein allgemeines Recht auf Achtung des Privat- und Familienlebens vor und schützt vor behördlichen Eingriffen, während Artikel 8 der Charta jeder Person das Recht zuspricht, dass ihre Daten nur unter bestimmten, genau festgelegten Bedingungen verarbeitet werden dürfen. Die beiden Konzepte unterscheiden und ergänzen sich. Das Paket „Intelligente Grenzen“ wird aus diesen beiden Blickwinkeln betrachtet.
18. Die vorliegende Stellungnahme hebt vorwiegend auf den EES-Vorschlag ab, der aus der Sicht des Schutzes der Privatsphäre und des Datenschutzes wohl der wichtigste ist, und ist folgendermaßen gegliedert:
 - Abschnitt II enthält eine allgemeine Bewertung des Einreise-/Ausreise-Systems und stellt die Einhaltung sowohl von Artikel 7 als auch von Artikel 8 der Charta in den Mittelpunkt;
 - Abschnitt III befasst sich mit konkreten Bestimmungen des EES-Vorschlags über die Verarbeitung biometrischer Daten und den Zugang für Strafverfolgungsbehörden;
 - Abschnitt IV enthält Anmerkungen zu anderen Fragen, die das EES aufwirft;
 - Abschnitt V befasst sich im Wesentlichen mit dem RTP;
 - Abschnitt VI geht auf den Bedarf an weiteren Datenschutzgarantien ein;
 - Abschnitt VII enthält die Schlussfolgerungen.

²³ Stellungnahme des EDSB vom 10. Juli 2009 zu der Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger“, ABl. C 276 vom 17.11.2009, S. 8.

²⁴ ABl. C 83 vom 30.3.2010, S. 389.

²⁵ Europarat, ETS Nr. 5, 4.11.1950.

II. ALLGEMEINE BEURTEILUNG DES EES

II.1. Artikel 7 der Charta: Achtung des Privat- und Familienlebens

19. Gemäß Artikel 7 der Charta hat „jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation“. Jede Einschränkung dieses Rechts (und dies gilt auch für Artikel 8) muss im Einklang mit Artikel 52 Absatz 1 der Charta stehen und daher gesetzlich vorgesehen sein, den Wesensgehalt der in der Charta anerkannten Rechte und Freiheiten achten, verhältnismäßig und erforderlich sein und „den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen“.
20. Artikel 7 der Charta ist in Verbindung mit Artikel 8 der EMRK zu lesen, der das Privat- und Familienleben mit fast derselben Formulierung schützt, und in dem es weiter heißt: „Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff *gesetzlich vorgesehen* und *in einer demokratischen Gesellschaft*“ für bestimmte Zwecke *„notwendig ist“*²⁶.
21. Der Grundsatz der Verhältnismäßigkeit ist eng mit dem Grundsatz der Notwendigkeit verknüpft. Nach Auffassung des Europäischen Gerichtshofs für Menschenrechte (EGMR) gilt ein solcher Eingriff in ein Recht als erforderlich, wenn er einem zwingendem gesellschaftlichen Bedürfnis entspricht, zu dem verfolgten Zweck in einem angemessenen Verhältnis steht, und wenn die von der Behörde angeführten Argumente zu seiner Begründung stichhaltig und ausreichend sind²⁷. Der Gerichtshof der Europäischen Union hat dem noch hinzugefügt, dass nachzuweisen ist, dass die gleichen Zwecke nicht auch mit weniger in die Privatsphäre eingreifenden Mitteln erreicht werden können²⁸.

Stellt das EES einen Eingriff dar? Und wenn ja, wie weit geht dieser?

22. Es liegt auf der Hand, dass bei der Routinespeicherung von Daten über die Ein- und Ausreise von Personen in das und aus dem Hoheitsgebiet der Europäischen Union häufig und auf unterschiedliche Art und Weise auch Informationen über ihr Privat- und Familienleben erfasst werden. In der Rechtsprechung des EGMR heißt es hierzu, dass „schon die Speicherung von Daten über das Privatleben einer Person einem Eingriff im Sinne von Artikel 8 der EMRK gleichkommt“²⁹. Zur Beurteilung des Ausmaßes des Eingriffs können mehrere Aspekte herangezogen werden, wie beispielsweise die Art der Daten, der Umfang der Datenerhebung, die weitere Verwendung und eine mögliche Änderung der Zweckbestimmung

²⁶ Nämlich „für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer“ (siehe Artikel 8 Absatz 2 EMRK).

²⁷ Siehe EGMR, Marper gegen Vereinigtes Königreich, 4. Dezember 2008, Klagen Nr. 30562/04 und 30566/04

²⁸ Siehe EuGH, C-92/09 Volker und Markus Schecke GbR gegen Land Hessen und C-93/09 Eifert gegen Land Hessen und Bundesanstalt für Landwirtschaft und Ernährung, 9.11.2010.

²⁹ a.a.O., Randnr. 67.

(z. B. die Speicherung von Telekommunikationsdaten für kommerzielle Zwecke und deren weitere Verwendung durch Strafverfolgungsbehörden), die Übermittlung an Drittländer (z. B. die systematische Übermittlung von Fluggastdatensätzen) oder der geheime Charakter der Erhebung und Verarbeitung (siehe z. B. die Schlussfolgerungen des EGMR in den Rechtssachen Amann und Rotaru³⁰).

23. Ein zentrales Element, das zu berücksichtigen ist, ist die Art der personenbezogenen Daten und deren Schutzbedürftigkeit. Die Erhebung biometrischer Daten stellt beispielsweise einen eindeutigen Eingriff dar, wie der EGMR in der Rechtssache Marper³¹ feststellte, der völlig unabhängig von der allgemeinen Frage von Informationen über das Privat- und Familienleben einer Person zu betrachten ist. Die Tatsache, dass die erhobenen Daten nicht Personen betreffen, die eines rechtswidrigen Verhaltens verdächtigt werden oder gegen die ansonsten ermittelt wird, spricht ebenfalls für einen Eingriff.
24. Zum EES merkt der EDSB an, dass hier eine Verarbeitung in großem Maßstab stattfindet, da von ihr alle Kurzzeitbesucher der EU betroffen sind, die unverdächtige Reisende sind, und da sie auch die Erhebung von Identifizierungsdaten einschließlich biometrischer Daten (10 Fingerabdrücke) umfasst. Die Möglichkeit des Zugangs für Strafverfolgungsbehörden ist ebenfalls vorgesehen; das System ist entsprechend ausgelegt. Es muss daher gefolgert werden, dass die Vorschläge einen Eingriff in das Recht auf Achtung des Privat- und Familienlebens mit möglicherweise weit reichenden Implikationen für die betroffenen Personen bedeuten.

Gibt es für den Eingriff eine eindeutige Rechtsgrundlage?

25. Die Rechtsvorschriften müssen so klar formuliert sein, dass Eingriffe vorhersehbar sind. Die Umstände, unter denen das Recht auf Achtung des Privat- und Familienlebens, der Wohnung oder Korrespondenz eingeschränkt werden darf, sind in der Rechtsgrundlage genau anzugeben³².
26. Genau darum geht es in dem EES-Vorschlag, der einen klaren Rahmen für die Erhebung, Verwendung und Speicherung von Daten von Drittstaatsangehörigen sowie für ihr Recht auf Information, Auskunft und Berichtigung abstecken soll. Wie nachstehend noch näher ausgeführt, sollten allerdings die Zweckbestimmungen des Vorschlags besser definiert und weitere Garantien vorgesehen werden.

³⁰ Siehe EGMR, Rotaru gegen Rumänien, 4. Mai 2000, Klage Nr. 28341/95; und Amann gegen Schweiz, 16. Februar 2000, Klage Nr. 27798/95.

³¹ a.a.O.

³² Siehe EGMR, Kruslin gegen Frankreich, Klage Nr. 11801/85, Randnr. 30 – 3.

Ist die Maßnahme in einer demokratischen Gesellschaft für einen der in Artikel 8 Absatz 2 EMRK oder Artikel 52 Absatz 1 der Charta aufgeführten Zwecke³³ notwendig und verhältnismäßig?

27. Punkt 9 der vorliegenden Stellungnahme macht deutlich, dass der Vorschlag andere, nicht genau definierte, auf jeden Fall aber eng miteinander verknüpfte Zwecke verfolgt, deren Schwerpunkt in der Grenzverwaltung und in einer besseren Bewältigung des Problems sich illegal aufhaltender Personen besteht. Bei der Beurteilung gemäß Artikel 7 sollte diesen Zwecken Rechnung getragen werden.
28. Der EDSB ist erstens der Auffassung, dass Großdatenbanken grundsätzlich zur Unterstützung einer im Unionsrecht verankerten EU-Politik geschaffen werden. Im vorliegenden Fall scheint die Datenbank jedoch aufgebaut zu werden, ohne dass bereits eine entsprechende umfassende Politik formuliert wurde, bzw. sogar erst, um herauszufinden, ob eine solche EU-Politik überhaupt formuliert werden muss. Dies ist besonders bedenklich, da das EES mit dem Ziel geschaffen wird, Overstayer zu identifizieren, ohne dass es eindeutige europäische politische Vorgaben für den Umgang mit Overstayers gibt.
29. Der Vorschlag besagt, das EES werde die Berechnung der Aufenthaltsdauer und damit die Identifizierung von Overstayers erleichtern (die mit Hilfe von Stempeln zwar bereits möglich, aber wohl schwieriger ist³⁴). Kann der Overstayer identifiziert werden, hat dies im Wesentlichen zur Folge, dass *ein neues Visum verweigert* wird, wenn die Person das Hoheitsgebiet der EU irgendwann verlässt und später zurückkehrt. Wurde der Overstayer im Hoheitsgebiet der EU gefunden und identifiziert, soll dies aber angeblich auch die *Rückführung* in den Herkunftsstaat erleichtern. Das EES mag zwar die *Identifizierung* von Overstayers erleichtern, doch trägt es nicht zu ihrer *eigentlichen Ortung im Hoheitsgebiet der EU* und zu den Voraussetzungen für eine *Rückführung* in ihr Herkunftsland bei³⁵. *Unklar* bleibt auch, ob das System in einem Gebiet mit *Landgrenzen* funktioniert³⁶. Nach Auffassung des EDSB hätten diese Fragen unbedingt im Vorfeld der Entwicklung dieser umfassenden Grenzkontrollregelung geklärt werden müssen.

³³ Nämlich „für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer“.

³⁴ Die Reisedokumente von Drittstaatsangehörigen werden bei der Ein- und Ausreise systematisch abgestempelt. Trägt ein Reisedokument keinen Einreisestempel, kann davon ausgegangen werden, dass sein Inhaber die Voraussetzungen für einen Aufenthalt nicht oder nicht mehr erfüllt.

³⁵ Zur Frage, ob die Übermittlung von Identifizierungsdaten an das Herkunftsland der Schlüssel zur Lösung von Rückführungsproblemen ist, insbesondere bei fehlender Kooperation des Drittlandes, siehe den Vermerk der Meijers-Ausschusses vom 3. Mai 2013 zu den Vorschlägen „Intelligente Grenzen“, S. 2.

³⁶ Siehe Folgenabschätzung des Vorschlags, S. 14f., und die Anmerkungen in der Stellungnahme der Artikel 29-Datenschutzgruppe, S. 6.

30. Ein zweiter, eigenständiger Zweck scheint die Erleichterung der Berechnung von unzulässig langen Aufenthalten und der Erstellung von Statistiken zu sein. Dieser Zweck kann allenfalls mittelbar mit den in Artikel 8 Absatz 2 EMRK aufgeführten Zwecken in Verbindung gebracht werden und dürfte kaum einen Eingriff in das Recht auf Achtung des Privatlebens rechtfertigen. Der EDSB stellt daher die Notwendigkeit und Verhältnismäßigkeit der Eingriffe in das Recht auf Schutz der Privatsphäre in Frage, wie sie im Vorschlag zum Zweck der Erleichterung der Berechnung und der Erstellung von Statistiken vorgesehen sind.
31. In diesem Zusammenhang hinterfragt der EDSB die Notwendigkeit identifizierbarer Informationen und vertritt die Ansicht, dass anonyme statistische Daten zum gleichen Ergebnis führen³⁷ und sogar ein besseres Kosten-Nutzen-Verhältnis aufweisen könnten. Bestehende diesbezügliche Möglichkeiten lassen sich im Schengener Grenzkodex finden³⁸. Dieses Ziel der Migrationssteuerung sollte auch mit bereits bestehenden migrationspolitischen Maßnahmen in Übereinstimmung gebracht werden, worauf die Artikel 29-Datenschutzgruppe mit Blick auf den „Gesamtansatz für Migration und Mobilität“ zu Recht hingewiesen hat³⁹.
32. Drittens sollte die Frage der Notwendigkeit auch vor dem breiteren Hintergrund von IT-Großsystemen geprüft werden. In den letzten Jahren wurde eine ganze Reihe solcher Systeme [http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/80 - Large scale](http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/80_Large_scale) entwickelt (Eurodac, VIS und jüngst SIS II als Ersatz für die erste Generation von SIS)⁴⁰, um eine wirksamere Kontrolle an den Außengrenzen zu gewährleisten, nachdem die Binnengrenzen für Personen, die innerhalb des Hoheitsgebietes der Europäischen Union reisen, abgeschafft worden sind. Diese Informationssysteme weisen Gemeinsamkeiten auf. Im Regelfall bestehen sie aus nationalen Systemen und einem Zentralsystem, und die Kontrolle der Datenverarbeitung wird gemeinsam durch die nationalen Datenschutzbehörden und den EDSB ausgeübt.

³⁷ Siehe EuGH, C-92/09, a.a.O.

³⁸ Siehe Artikel 11 Absatz 2 und Artikel 13 Absatz 5 des Schengener Grenzkodex, in denen die Mitgliedstaaten aufgefordert werden, sich gegenseitig sowie die Kommission und das Generalsekretariat des Rates über ihre nationalen Praktiken bezüglich der Annahme eines legalen Aufenthalts und ihrer Widerlegung gemäß Artikel 11 zu unterrichten, und in denen die Mitgliedstaaten aufgefordert werden, statistische Daten über die Anzahl der Personen, denen sie die Einreise verweigern, die Gründe für die Einreiseverweigerung, die Staatsangehörigkeit der betreffenden Personen und die Art der Grenze (Land-, Luft- oder Seegrenze), an der ihnen die Einreise verweigert wurde, zu erheben. Die Mitgliedstaaten übermitteln diese Statistiken einmal pro Jahr der Kommission. Die Kommission veröffentlicht alle zwei Jahre eine Übersicht über die von den Mitgliedstaaten vorgelegten Statistiken.

³⁹ Ausgeführt in der Stellungnahme der Artikel 29-Datenschutzgruppe, S. 10. Siehe KOM(2011) 743 endgültig.

⁴⁰ Das VIS ging teilweise 2011 in Betrieb und wird derzeit in verschiedenen Teilen der Welt eingeführt. Am 9. April 2013 nahm die zweite Generation des Schengener Informationssystems (SIS II) ihren Betrieb auf.

Der EDSB verweist auf die Ergebnisse seiner VIS-Inspektion im Jahr 2011, bei der mehrere der festgestellten Probleme erhebliche Risiken für die Sicherheit des Betriebs von VIS bargen.

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/VIS/12-06-01_VIS_security_audit_report_summ_EN.pdf

33. Wie bereits erwähnt, hat sich der EDSB unterstützend zu den Schlussfolgerungen des Stockholmer Programms geäußert und dabei dazu aufgefordert, solche Systeme gründlich zu überdenken und die Kosten für den Schutz der Privatsphäre und den Datenschutz sowie die Wirksamkeit für Grenzkontrollen und öffentliche Sicherheit angemessen zu berücksichtigen. Dort heißt es insbesondere: *„Der vollständigen und wirksamen Umsetzung, Durchsetzung und Bewertung der bestehenden Instrumente ist in den kommenden Jahren verstärkte Aufmerksamkeit zu widmen“*.⁴¹ Im vorliegenden Zusammenhang sollte die Analyse vorgeschlagene Instrumente wie EES und RTP, aber auch die Instrumente umfassen, die bereits umgesetzt werden.
34. Der EDSB nimmt die von der Kommission in der Folgenabschätzung für das EES vorgenommene Analyse zur Kenntnis⁴², in der es um die Vereinbarkeit des EES mit anderen IT-Großsystemen geht, und auch ihre Schlussfolgerung, der zufolge keines dieser Systeme die administrativen Anforderungen für die Verwaltung des Aufenthaltsrechts in der EU und für die Feststellung und Verhütung der illegalen Migration insbesondere im Hinblick auf Overstayer erfüllt. Es sei jedoch auf einige verbleibende Unklarheiten hingewiesen.
35. Wenn auch bestehende Systeme vielleicht nicht alle Ziele des „Intelligente Grenzen“-Pakets erreichen helfen, so können sie doch zum Erreichen einiger dieser Ziele beitragen und auch weiter entwickelt werden, um in Zukunft weitere anzustreben. Eines der Hauptziele der VIS-Verordnung⁴³ besteht beispielsweise darin, bei der Identifizierung von Personen zu helfen, die die Voraussetzungen für die Einreise in die Hoheitsgebiete der Mitgliedstaaten, den Aufenthalt oder die Wohnsitznahme dort nicht erfüllen. Gemäß Artikel 24 der SIS II-Verordnung kann auch eine Ausschreibung eingegeben werden⁴⁴.

⁴¹ Stockholmer Programm, Punkt 1.2.2.

⁴² Siehe S. 20 und S. 69-74 EES Folgenabschätzung.

⁴³ Das VIS sollte der Erleichterung der Betrugsbekämpfung und der Kontrollen an den Grenzkontrollstellen an den Außengrenzen und im Hoheitsgebiet der Mitgliedstaaten dienen. Weiter sollte das VIS der Identifizierung von Personen dienen, die die Voraussetzungen für die Einreise in das Hoheitsgebiet der Mitgliedstaaten, den Aufenthalt oder die Wohnsitznahme dort nicht oder nicht mehr erfüllen, und es sollte die Anwendung der Verordnung (EG) Nr. 343/2003 des Rates vom 18. Februar 2003 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen in einem Mitgliedstaat gestellten Asylantrags zuständig ist, erleichtern und zur Vermeidung von Bedrohungen der inneren Sicherheit aller Mitgliedstaaten beitragen.

⁴⁴ Siehe Artikel 24 Absatz 3 der SIS II-Verordnung, Voraussetzungen für Ausschreibungen zur Einreise- oder Aufenthaltsverweigerung:

„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“.

36. Das Hauptproblem besteht im Mangel an ausreichender Erfahrung mit der Funktionsweise dieser Systeme; es lassen sich noch keine nützlichen Schlussfolgerungen ziehen. Die Erfahrungen mit VIS und anderen bestehenden Systemen (Eurodac, SIS II) sind begrenzt: Vor allem VIS⁴⁵ ist noch nicht voll einsetzbar, da auf der Ebene des Zentralsystems noch Datenschutzprobleme zu lösen sind⁴⁶.
37. Der EDSB bezweifelt daher, ob es angebracht ist, ein neues Grenzkontrollsystem in Erwägung zu ziehen, bevor tatsächlich eine gründliche Evaluierung bestehender Systeme durchgeführt werden konnte; es sollte für Kohärenz und dafür gesorgt werden, dass sich bereits in der Vergangenheit aufgetretene Schwierigkeiten nicht wiederholen.
38. Schlussfolgernd gilt Folgendes: Selbst wenn das angestrebte *Ziel* als in einer demokratischen Gesellschaft legitim und notwendig angesehen werden kann, stehen die bestehenden *Rechtsvorschriften* nicht im Einklang mit den Anforderungen von Artikel 8 Absatz 2 EMRK bezüglich Notwendigkeit und Verhältnismäßigkeit. Der EDSB ist daher der Auffassung, dass ohne eine weitere Prüfung durch die Gesetzgeber
- a. ohne eine klare Politik der EU für den Umgang mit Overstayern kein EES für den Zweck der Identifizierung von Overstayern eingerichtet werden sollte;
 - b. zur Erleichterung der Berechnung unzulässig langer Aufenthalte und zur Erstellung von Statistiken keine Großdatenbank mit personenbezogenen Daten aufgebaut werden sollte;
 - c. vor einer tatsächlichen gründlichen Evaluierung bestehender Systeme kein EES geschaffen werden sollte, um Kohärenz sicherzustellen und die Wiederholung bereits in der Vergangenheit aufgetretener Schwierigkeiten zu vermeiden.
39. Als zweites muss die Regelung mit den spezifischen Garantien von Artikel 8 der Charta in Einklang stehen.

II.2. Artikel 8 der Charta: Schutz personenbezogener Daten

40. Diese Bestimmung besagt: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten“. Weiter heißt es dort, dass Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden dürfen, und dass jede Person das Recht hat, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Die Einhaltung dieser

⁴⁵ „Ende 2011 wurden folgende Risiken als am kritischsten eingestuft: a) vorzeitige Ausschöpfung der Systemkapazität, nachdem Mitgliedstaaten das System früher als geplant auch in anderen Regionen eingeführt hatten, b) Übergabe des zentralen VIS von C.SIS an die EU-Agentur für das Management von IT-Großsystemen sowie c) Fingerabdruckqualität während des Systembetriebs“.

Siehe S. 11 im Bericht der Kommission an das Europäische Parlament und den Rat über die Entwicklung des Visa-Informationssystems (VIS) im Jahr 2011 (vorgelegt gemäß Artikel 6 der Entscheidung 2004/512/EG des Rates).

⁴⁶ Siehe ferner Fußnote 24.

Vorschriften wird von einer unabhängigen Behörde überwacht. Dies sind die grundlegenden Anforderungen an die Verarbeitung personenbezogener Daten, die in den verschiedenen Datenschutzrechtsakten näher ausgeführt werden.

Verarbeitung nach Treu und Glauben

41. Zu der Spanne von Maßnahmen, die eine Verarbeitung nach Treu und Glauben gewährleisten, gehören allgemeine Transparenz, Minimierung der erhobenen Daten sowie Schritte zur Vermeidung von Diskriminierung. Der EDSB begrüßt, dass mit mehreren Bestimmungen des Vorschlags gewährleistet werden soll, dass Daten nicht im Übermaß erhoben werden (unbeschadet der Bewertung der Verwendung biometrischer Daten, auf die in einem späteren Kapitel gesondert eingegangen wird), und dass Sensibilisierungsmaßnahmen insbesondere für Bedienstete vorgesehen sind, die die Daten verarbeiten⁴⁷.
42. Dessen ungeachtet weist der EDSB auf die Risiken im Zusammenhang mit der automatisierten Berechnung von Daten und mit Entscheidungen hin, die gegen die betreffende Person auf der Grundlage einer solchen automatisierten Verarbeitung ergehen könnten. Wie nachstehend ausgeführt, sind die Bedingungen, unter denen eine Person darüber unterrichtet wird, dass sie (unangemessenerweise) als Overstayer registriert wird, sind nach wie vor nicht zufriedenstellend.

Festgelegter Zweck

43. Der Zweck/die Zwecke einer Maßnahme, die auf die Verarbeitung personenbezogener Daten abhebt, muss klar und präzise genug umrissen sein, damit für die von der Maßnahme Betroffenen Transparenz gegeben ist. Bei der Genauigkeit sind Umfang und Auswirkung der Datenverarbeitung zu berücksichtigen. Je weiter sie in die Privatsphäre eingreift, desto genauer muss die Beschreibung sein. Artikel 4 des Vorschlags enthält eine Auflistung miteinander verbundener Zwecke sowie Angaben zu weiteren Konsequenzen, die die Regelung ebenfalls erreichen möchte.
44. Diese Zwecke sind zwar in dieser Stellungnahme bereits erwähnt worden, doch sollen sie hier noch einmal in Erinnerung gerufen werden:
 - Die Hauptzwecke werden allgemein beschrieben, wie Verbesserung der Verwaltung der Außengrenzen und Bekämpfung der irregulären Zuwanderung, Umsetzung einer integrierten Grenzverwaltungspolitik und Zusammenarbeit und Konsultation zwischen den Grenz- und den Einwanderungsbehörden.
 - Erreicht werden sollen diese Zwecke durch die Gewährung von Zugang zu den Ein- und Ausreiseinformationen über Drittstaatsangehörige.

⁴⁷ Siehe insbesondere Artikel 8 zur allgemeinen Nutzung des EES und zur Vorbeugung von Diskriminierung, Artikel 11 und 12 mit der Auflistung der zu erhebenden Daten, die unter Berücksichtigung der Anmerkungen des EDSB teilweise gekürzt wurde, Artikel 25 über die Schulung der Bediensteten und Artikel 33 über die Information betroffener Personen.

- Als weitere Ziele werden genannt die Verbesserung der Kontrollen an den Grenzübergangsstellen, die Berechnung und Überwachung der zulässigen Aufenthaltsdauer, die Erleichterung der Identifizierung von Overstayern und der Ergreifung der erforderlichen Maßnahmen sowie die Erstellung von Statistiken.
45. Zu den Einzelheiten dieser Zwecke hat der EDSB keine weiteren Anmerkungen. Die Tatsache allerdings, dass die Zwecke genau aufzuführen sind, bedeutet auch, dass Daten nicht ohne Zusammenhang mit diesen Zwecken verarbeitet werden dürfen. Dies wirft ein besonderes Problem bezüglich der Wiederverwendung von Daten für Strafverfolgungszwecke auf. Solche Zwecke werden als zukünftige Möglichkeiten genannt, nach einer Evaluierung des Systems. In seinen Kommentaren zum Stockholmer Programm hatte der EDSB zu besonderer Aufmerksamkeit im Hinblick auf eine solche Wiederverwendung personenbezogener Daten aufgerufen und gefordert, die Notwendigkeit streng zu prüfen und enge Voraussetzungen für den Zugriff auf die Daten vorzusehen. Hierauf wird in Abschnitt III näher eingegangen.

Legitime Grundlage

46. Da das EES natürlich nicht auf der freiwilligen und in Sachkenntnis erteilten Einwilligung der betroffenen Personen beruht, steht die Notwendigkeit einer gesetzlich geregelten legitimen Grundlage im Wesentlichen mit der Frage im Zusammenhang, ob die vorgeschlagene Regelung im Einklang mit Artikel 7 der Charta und mit Artikel 8 EMRK steht, wie bereits in Abschnitt II.1 erörtert und in den Schlussfolgerungen unter Punkt 38 festgehalten. Es sei jedoch unterstrichen, dass die allgemeinen Grundsätze des Datenschutzes ebenfalls verlangen, dass die Verarbeitung personenbezogener Daten erforderlich ist und zu den möglicherweise betroffenen legitimen Zwecken in einem angemessenen Verhältnis steht.

Rechte der betroffenen Person

47. Der EDSB verweist nachdrücklich auf die Notwendigkeit, den möglichen rechtlichen Folgen der automatisierten Verarbeitung personenbezogener Daten besondere Aufmerksamkeit zu widmen. Wird die Faktenlage nicht ausreichend berücksichtigt, können sich für die betroffene Person besonders nachteilige Auswirkungen ergeben.
48. Vor allem Artikel 9 des EES-Vorschlags verdient besondere Aufmerksamkeit, denn er sieht zur Erleichterung der Berechnung der Aufenthaltsdauer vor, dass das System automatisch berechnet, für welche Einreiseeinträge keine Ausreisedaten unmittelbar nach Ablauf der zulässigen Aufenthaltsdauer vorliegen, und die zuständigen Behörde in Kenntnis setzt. Dies wirft die Frage auf, wie sich Fehler aufgrund einer automatisierten Entscheidung vermeiden lassen, bei der aus unterschiedlichen Gründen (dualer Status des Drittstaatsangehörigen – z. B. Einreise mit einem normalen Reisepass und Ausreise mit einem Diplomatenpass –, medizinische Gründe oder technische Probleme des Systems) Ausreisen nicht registriert werden.

49. Außerdem müssten die betroffenen Personen rechtzeitig umfassend über jede Entscheidung in Kenntnis gesetzt werden, damit sie ihre Rechte angemessen ausüben können. Dies ist umso nötiger, als immer mehr Datenbanken im Bereich der Grenzverwaltung entstehen, was den betroffenen Personen die Ausübung ihrer Rechte zunehmend erschwert. Nach Auffassung des EDSB könnten die folgenden Bestimmungen zur Stärkung der Rechte der betroffenen Personen geändert werden.

Recht auf Löschung (Artikel 21 Absatz 2)

50. Der EDSB begrüßt die Verpflichtung für die Mitgliedstaaten, personenbezogene Daten von Overstayern unverzüglich zu löschen, wenn der Drittstaatsangehörige einen Nachweis darüber vorlegt, dass er durch ein unvorhersehbares, ernstes Ereignis gezwungen war, die zulässige Aufenthaltsdauer zu überziehen. Allerdings sollte seiner Auffassung nach klargestellt werden, dass die betroffenen Personen über dieses Recht in Kenntnis zu setzen sind und bei Nichtachtung dieses Rechts Rechtsbehelfe einlegen können (siehe die Empfehlungen weiter unten).

Informationspflicht gegenüber der betroffenen Person (Artikel 33)

51. Der EDSB schlägt vor, in Artikel 33 Absatz 1 hinzuzufügen, dass Overstayer „von dem **für die Eingabe ihrer Daten verantwortlichen Mitgliedstaat informiert werden**“. Ohne diesen Zusatz würden die Kriterien für die Bestimmung des verantwortlichen Mitgliedstaats unklar bleiben.
52. Ferner schlägt der EDSB vor, Angaben aufzunehmen über
- die automatisierte Verarbeitung von Daten zur Berechnung der Aufenthaltsdauer;
 - die Tatsache, dass ein unzulässig langer Aufenthalt zur Folge hat, dass die personenbezogenen Daten der Person auf einer Overstayer-Liste veröffentlicht werden;
 - die Kategorien von Empfängern dieser Liste;
 - das Recht auf Löschung personenbezogener Daten, wenn ein Nachweis darüber vorliegt, dass der unzulässig lange Aufenthalt auf ein unvorhersehbares, ernstes Ereignis zurückzuführen ist;
 - das Recht, Informationen über die Verfahren für die Ausübung von Rechten und über mögliche Rechtsbehelfe zu erhalten, einschließlich der Regelungen, die der betroffenen Person die Möglichkeit einräumen, seine Ansicht zum automatisierten Charakter der Datenverarbeitung zu äußern.
53. Der EDSB begrüßt weiter, dass die Informationen schriftlich mitgeteilt werden (Artikel 33 Absatz 2), empfiehlt jedoch, Folgendes hinzuzufügen: „in verständlicher Form unter Verwendung einer klaren, einfachen und adressatengerechten Sprache“, wie es in Artikel 11 Absatz 2 der

vorgeschlagenen Allgemeinen Datenschutzverordnung⁴⁸ vorgesehen ist. Für Drittstaatsangehörige, die die Sprache des verantwortlichen Mitgliedstaats nicht verstehen, sollten Übersetzungen dieser Informationen zur Verfügung gestellt werden.

Rechtsbehelfe (Artikel 36)

54. Artikel 36 sieht Rechtsbehelfe vor, wenn das in Artikel 35 geregelte Recht auf Auskunft, Löschung und/oder Berichtigung verweigert wird. Es wird jedoch nicht klar, ob auch die in Artikel 21 Absatz 2 erwähnte Löschung von Daten unter diese Bestimmung fällt. Der EDSB empfiehlt daher, Artikel 35 (oder Artikel 36) dahingehend zu ändern, dass Rechtsbehelfe auch für die in Artikel 21 Absatz 2 genannte Situation gelten.

Kontrolle durch unabhängige Behörden (Artikel 37 bis 39)

55. Der EDSB begrüßt die Bestimmungen über die Überwachung der Datenverarbeitung. Dabei wird den Verantwortlichkeiten auf nationaler und auf EU-Ebene angemessen Rechnung getragen, und es wird ein System für die Koordinierung aller beteiligten Datenschutzbehörden vorgesehen, das auf Erfahrung und auf bestehenden, erprobten und vertrauten Mechanismen beruht. Der EDSB ist bereit, seinen Pflichten bezüglich des EES (und des RTP) nachzukommen.
56. Der EDSB nimmt die Verantwortlichkeiten der verschiedenen Akteure im Bereich „Intelligente Grenzen“ zur Kenntnis, also von Kommission, EU-Lisa und Mitgliedstaaten. Parallel dazu entstehen auch Verantwortlichkeiten bei den Datenschutzbehörden auf europäischer und nationaler Ebene.
57. Eine solche Kompetenzverteilung macht eine Zusammenarbeit auf mehreren Ebenen erforderlich, nämlich zwischen Datenschutzbeauftragten, zwischen Datenschutzbehörden und zwischen Behörden und Beauftragten, damit mögliche Grauzonen vermieden werden.
58. Der EDSB begrüßt das in Artikel 39 des Vorschlags vorgesehene koordinierte Aufsichtsmodell, mit dem eine kohärente Auslegung und Anwendung der Verordnung sichergestellt werden soll. Seiner Auffassung nach sollte dieser Ansatz durch eine klare Verteilung der Kompetenzen auf nationaler Ebene ergänzt werden, damit betroffene Personen ihre Rechte gegenüber der zuständigen Behörde wahrnehmen können. Wie bereits unter Punkt 51 ausgeführt, sollte die Bestimmung des verantwortlichen Mitgliedstaats in diesem Sinne klargestellt und für die Öffentlichkeit transparent gemacht werden.

⁴⁸ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Allgemeine Datenschutzverordnung), COM(2012) 11 final.

III. SPEZIFISCHE ANMERKUNGEN ZUM EES

III.1. Biometrische Daten

59. Die Vorschläge beruhen auf der Verwendung biometrischer Elemente (Fingerabdrücke). Der EDSB stellt fest, dass die Kommission im Einklang mit den in der Folgenabschätzung⁴⁹ herausgearbeiteten Optionen plant, drei Jahre nach dem Anlaufen des EES automatisch Fingerabdrücke hinzuzufügen.
60. Der EDSB weist darauf hin, dass nachgewiesen werden muss, dass die Verwendung biometrischer Daten in diesem Zusammenhang, die einen eigenständigen Eingriff in das Recht auf Achtung des Privatlebens darstellt, „in einer demokratischen Gesellschaft notwendig“ ist, und dass andere, weniger in die Privatsphäre eingreifende Mittel, nicht zur Verfügung stehen. In der Rechtssache S. und Marper befand der EGMR, dass Fingerabdrücke und Lichtbilder einzigartige Informationen enthalten, die „das Privatleben einer Person berühren können“, und dass die Speicherung dieser Informationen ohne Einwilligung der betroffenen Person „nicht als neutral oder unbedeutend betrachtet werden kann“⁵⁰. Darüber hinaus sollte die Verarbeitung solcher Daten nur mit strengen Garantien erfolgen und sollte das Fehlerrisiko berücksichtigt werden.
61. Der EDSB hätte es daher vorgezogen, wenn eine Ex ante-Bewertung vorgenommen worden wäre, auch im Hinblick auf die Aufnahme möglicher Garantien, und wenn nicht schon jetzt eine endgültige Entscheidung über die Aufnahme biometrischer Daten in das System gefallen wäre. Der EDSB schlägt eine Änderung des Wortlauts des Vorschlags in diesem Sinne vor. Genauer gesagt sollte die Kommission eine gezielte Folgenabschätzung im Hinblick auf die biometrischen Daten (Fingerabdrücke) vornehmen und diese nicht, wie derzeit im Vorschlag (Artikel 12) vorgesehen, automatisch in das System aufnehmen. Der EDSB schlägt vor, dies als verbindliche Vorgabe in Artikel 12 Absatz 5 des EES-Vorschlags aufzunehmen.
62. In Unterstützung dieser Empfehlung nimmt der EDSB Entwicklungen in den Vereinigten Staaten zur Kenntnis, wo vor kurzem ein vorläufiger Bericht des *Government Accountability Office* erschienen ist, der sich mit den Problemen bei der Planung einer „biometric exit capability“ (Möglichkeit der Überprüfung biometrischer Daten bei der Ausreise) befasst⁵¹. Es geht dort um so wichtige Fragen wie die Wirksamkeit der derzeitigen „biographic air exit processes“ (Verfahren zur Überprüfung biografischer Daten bei der Ausreise auf dem Luftweg), Fehlerraten bei

⁴⁹ Siehe S. 26 bis 39 der EES-Folgenabschätzung.

⁵⁰ Weiter heißt es dort, dass eine pauschale und unterschiedslose Speicherung von „Fingerabdrücken, Zellproben und DNA-Profilen“ von Personen, die nicht wegen einer Straftat verurteilt wurden, nicht „zu einem ausgewogenen Verhältnis zwischen miteinander konkurrierenden öffentlichen und privaten Interessen führen kann“; EGMR, S. und Marper gegen Vereinigtes Königreich, a.a.O. Randnr. 125.

⁵¹ Preliminary Observations on DHS's Overstay Enforcement Efforts (Vorbemerkungen zu Durchsetzungsbemühungen des *Department of Homeland Security* bei Overstayern), abrufbar unter <http://www.gao.gov/assets/660/654752.pdf>.

der Erfassung oder dem Abgleich von Daten, den Mehrwert der Überprüfung biometrischer Daten im Vergleich zum derzeitigen Verfahren der Überprüfung biografischer Daten bei der Ausreise auf dem Luftweg und um den Gesamtwert und die Gesamtkosten einer „biometric air exit capability“. Dieses Vorhaben der Vereinigten Staaten zur Entwicklung eines biometrischen Ausreisensystems wird derzeit noch geprüft.

63. Der EDSB weist ferner auf die „Australian Movement Reconstruction Database“ (Australische Datenbank zur Bewegungsrekonstruktion) hin, die eine Alternative in Form eines ähnlichen Systems darstellen könnte, das allein mit alphanumerischen Daten arbeitet⁵². Diese „Bewegungsaufzeichnungen“ können den Namen des Reisenden, sein Geburtsdatum, Geschlecht und Familienstand, sein Geburtsland, das Datum von Ankunft und/oder Abreise, die Nummer des Reisedokuments, den Hafencode und Angaben zum Flug/Schiff, die Visumsunterklasse und das Ablaufdatum des Visums sowie die Anzahl der Bewegungen umfassen.
64. Der EDSB hat wiederholt eingeräumt, dass die Verwendung biometrischer Daten Vorteile bietet, er hat aber auch unterstrichen, dass diese Vorteile von der Anwendung strenger Garantien abhängen.
65. In seiner Stellungnahme zu SIS II⁵³ hat der EDSB vorgeschlagen, eine nicht erschöpfende Liste gemeinsamer Verpflichtungen oder Anforderungen zu erarbeiten, die bei der Verwendung biometrischer Daten in einem System einzuhalten wären, einschließlich gezielter Folgenabschätzung, verstärkter Beachtung des Erfassungsverfahrens, Schwerpunkt Genauigkeitsgrad und Ausweichverfahren. Diese Elemente sollen dazu beitragen, dass dem Drittstaatsangehörigen die Mängel des Systems aufgebürdet werden, wie z. B. die Folgen einer falschen Identifizierung oder einer Nichterfassung der Fingerabdrücke. In diesem Zusammenhang begrüßt der EDSB Artikel 12 Absatz 3 des EES-Vorschlags zu Personen, bei denen aus physischen Gründen keine Fingerabdrücke abgenommen werden können.
66. Der EDSB weist ferner darauf hin, dass zehn und nicht nur zwei oder vier Fingerabdrücke genommen werden sollen, die für Überprüfungszwecke auf jeden Fall ausreichen würden. Die Abnahme von zehn Fingerabdrücken von vornherein wäre nur erforderlich, wenn damit ein anderer Zweck verfolgt würde, nämlich die Identifizierung von Spuren im Strafverfolgungskontext. Nach Auffassung des EDSB sollte eine solche umfassende Abnahme von Fingerabdrücken von Anfang an nicht vorgesehen werden, da die Bewertung eines möglichen Zugangs für

⁵² Einzelheiten unter:

<http://www.immi.gov.au/managing-australias-borders/border-security/systems/movement-records.htm>.

⁵³ Stellungnahme vom 19. Oktober 2005 zu drei Vorschlägen betreffend das Schengener Informationssystem der zweiten Generation (SIS II) (KOM(2005) 230 endgültig, KOM(2005) 236 endgültig und KOM(2005) 237 endgültig), ABl. C 91 vom 19.4.2006, S. 38.

Strafverfolgungsbehörden wohl frühestens zwei Jahre nach dem Inkrafttreten des Systems erfolgen wird.

III.2. Zugang für Strafverfolgungsbehörden

67. Der EDSB stellt fest, dass der EES-Vorschlag einen Zugang von Strafverfolgungsbehörden zum EES grundsätzlich nicht gestattet, sondern erst nach einer Phase der Evaluierung. Der Vorschlag sieht vor, dass sich eine erste Evaluierung des EES ausdrücklich mit der Frage des Zugangs zu Strafverfolgungszwecken einschließlich Zugangsbedingungen, Speicherfrist und Zugang für Behörden von Drittländern befassen soll.
68. Ein Zugang zum EES würde dem allgemeinen Trend folgen, Strafverfolgungsbehörden Zugang zu diversen Informations- und Identifizierungsgroßsystemen einzuräumen (siehe beispielsweise den Zugang zu Eurodac⁵⁴), und wäre auch ein Aufgreifen des Trends, Strafverfolgungsbehörden Zugang zu Daten von Personen zu geben, die eigentlich keiner Straftat verdächtigt werden.
69. Nach Auffassung des EDSB sollte die Möglichkeit eines Zugangs zum EES für Strafverfolgungsbehörden – der ein eigenständiger Eingriff in das Recht auf Achtung des Privatlebens sowie ein Verstoß gegen den Grundsatz der Zweckbindung, einen Kerngrundsatz des Datenschutzrechts wäre – erst nach einer angemessenen Evaluierung vorgesehen werden, die klar belegt, dass ein solcher Zugang erforderlich ist. Es sollte insbesondere der genaue Mehrwert eines solchen Zugangs im Vergleich zum Zugang zu bereits bestehenden biometrischen Datenbanken herausgearbeitet werden, und es sollte nachgewiesen werden, dass die Notwendigkeit des Zugangs mehr Gewicht als der Eingriff in das Privatleben von Personen hat. Der EDSB erinnert daran, dass die Personen, deren Daten im EES gespeichert werden, grundsätzlich keiner Straftat verdächtigt werden und daher auch nicht als Verdächtige behandelt werden sollten, da das System in erster Linie darauf angelegt ist, als Instrument für die Berechnung der Aufenthaltsdauer von Drittstaatsangehörigen zu dienen.
70. Sollte ein Zugang erforderlich sein, sind strenge Bedingungen wie z. B die notwendig, dass Datenabfragen verhältnismäßig, sehr gezielt und auf Verdachtsmomente gegen eine bestimmte Person gegründet sein sollten.

⁵⁴ Siehe 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 Europol 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, ABl. L 180 vom 29.6.2013, S. 1.

III.3. Datenübermittlungen an Drittländer

71. Nach Auffassung des EDSB sollten die Gründe, aus denen die Übermittlung von EES-Daten an Drittländer für die Rückführung von Drittstaatsangehörigen erforderlich ist, näher ausgeführt werden.
72. Der EDSB begrüßt, dass Übermittlungen grundsätzlich untersagt sind und dass Artikel 27 Absatz 2 eine Reihe von Bedingungen für Ausnahmefälle enthält. Seiner Ansicht nach ist allerdings der Wortlaut über die Übermittlung im EES gespeicherter personenbezogener Daten an Drittländer, internationale Organisationen und private Stellen⁵⁵ für den allgemeinen Zweck des Nachweises der Identität von Drittstaatsangehörigen und für den Zweck der Rückführung zu breit gefasst. Der EDSB räumt ein, dass es erforderlich sein kann, einige Daten mit einem Drittland auszutauschen, wenn es um die Rückführung der betreffenden Person geht. Aus dem Vorschlag geht jedoch nicht hervor, unter welchen Voraussetzungen und für welche Zwecke Drittländer einen Nachweis der Identität eines Drittstaatsangehörigen anfordern können.
73. Da sich eine ähnliche Bestimmung auch in der VIS-Verordnung⁵⁶, findet, empfiehlt der EDSB dem EU-Gesetzgeber, zunächst einen Bericht darüber abzuwarten, wie die VIS-Bestimmung in der Praxis angewandt wird, und dann die Möglichkeit der jetzt in Artikel 27 Absatz 2 aufgeführten Ausnahmen auch auf das EES anzuwenden.

IV. SONSTIGE ANMERKUNGEN ZUM EES

Definition des Overstayers

74. In Artikel 5 Absatz 13 ist ein „Overstayer“ definiert als ein Drittstaatsangehöriger, der die Bedingungen für den Kurzaufenthalt im Hoheitsgebiet der Mitgliedstaaten nicht oder nicht mehr erfüllt. Es ist nicht genau zu erkennen, ob diese Definition nur den Fall abdeckt, in dem ein Drittstaatsangehöriger rechtmäßig in das Hoheitsgebiet der EU eingereist ist und seine Aufenthaltsdauer überzogen hat, oder ob auch die Situation erfasst wird, in der ein Drittstaatsangehöriger die im Schengener Grenzkodex niedergelegten Bedingungen nicht eingehalten hat (gültiges Visum und gültige Reisedokumente, ausreichende Mittel zur Bestreitung des Lebensunterhalts usw.)⁵⁷. Daraus können sich zum einen für Personen, die die Dauer ihres rechtmäßigen Aufenthalts in der EU überschritten haben, und zum anderen für Personen, die die Bedingungen für eine legale Einreise in das Hoheitsgebiet der EU nicht eingehalten haben, aber innerhalb eines Zeitraums von 180 Tagen sich nicht länger als die

⁵⁵ Siehe Artikel 27 Absatz 2.

⁵⁶ Siehe Artikel 30 Absatz 2 der Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung).

⁵⁷ Siehe Artikel 5 Absatz 1 der Verordnung (EG) Nr. 562/2006 des Europäischen Parlaments und des Rates vom 15. März 2006 über einen Gemeinschaftskodex für das Überschreiten von Grenzen durch Personen (Schengener Grenzkodex), ABl. L 105 vom 13.4.2006, S. 1.

gesetzmäßigen 90 Tage dort aufgehalten haben, unterschiedliche rechtliche Konsequenzen ergeben. Der EDSB schlägt der Kommission eine Klarstellung dieser Begriffsbestimmung vor.

Überprüfung der Identität

75. Artikel 18 Absatz 1 erlaubt den Zugang zu Daten zum Zweck der Überprüfung der Identität des Drittstaatsangehörigen und/oder der Erfüllung der Voraussetzungen für eine Einreise in das Hoheitsgebiet der Mitgliedstaaten und den dortigen Aufenthalt. Der Wortlaut dieser Bestimmung ist zu weit gefasst. Vor allem das Wort „oder“ könnte bedeuten, dass personenbezogene Daten für die Überprüfung der Identität verwendet werden dürfen, unabhängig von der Überprüfung der Erfüllung der Voraussetzungen für Einreise oder Aufenthalt. Um zu vermeiden, dass irgendwelche Behörden, die nicht für Einwanderungsfragen zuständig sind, für beliebige Zwecke Zugang zu den Daten erhalten, empfiehlt der EDSB dem EU-Gesetzgeber, das Wort „oder“ zu streichen und beide Bedingungen (Überprüfung der Identität und Aufenthaltsbedingungen) ausdrücklich miteinander zu verknüpfen.

Datenspeicherung für Overstayer

76. Der EDSB begrüßt die in Artikel 20 festgelegte Höchstfrist von sechs Monaten für die Speicherung der Daten im EES. Die Speicherfrist von fünf Jahren für Daten von Overstayern wird weder in der Folgenabschätzung noch im Vorschlag begründet und dürfte in keinem Verhältnis zum angestrebten Zweck stehen. Der EDSB empfiehlt dem EU-Gesetzgeber, in einem Erwägungsgrund besser zu begründen, weshalb die Daten von Overstayern so lange gespeichert werden sollen, oder diese Frist deutlich zu begrenzen.

Anonyme Statistiken

77. Artikel 40 erlaubt den zuständigen Behörden, zur Erstellung von Berichten und Statistiken einige Datenkategorien abzufragen, „die eine Identifizierung nicht ermöglichen“. Die Formulierung „die eine Identifizierung nicht zulassen“ ist irreführend, da einige der abfragbaren Datenkategorien eine – zumindest indirekte – Identifizierung der Personen zulassen, insbesondere, wenn Daten miteinander kombiniert werden. Der in Artikel 40 erwähnte Ausdruck „Berichte“ sollte klargestellt werden (was muss berichtet werden, wer hat wem Bericht zu erstatten und wie oft). Der EDSB empfiehlt daher dem EU-Gesetzgeber, folgenden Wortlaut hinzuzufügen: „zur Erstellung von Berichten und *anonymen* Statistiken“, und die Bedeutung von „Berichte“ in einem Erwägungsgrund zu definieren.

V. ANMERKUNGEN ZUM RTP-VORSCHLAG

Ziel des Vorschlags und Rolle der Einwilligung

78. Das RTP dient der Beschleunigung des Grenzübertritts für vorab geprüfte Reisende. Grundlage des Systems sind automatisierte Identitätskontrollen und Sicherheitsschleusen an den Grenzen, mit denen Grenzbeamte weniger oder gar keine Reisedokumente mehr prüfen müssen. Dem RTP-Vorschlag ist entnehmen, dass das System auf Freiwilligkeit beruhen und Vielreisenden die Möglichkeit bieten soll, einen schnelleren Grenzübertritt zu beantragen⁵⁸.
79. Die Einwilligung des Reisenden wird als Legitimation der Verarbeitung personenbezogener Daten angeführt. Damit eine Einwilligung gültig ist, muss sie „ohne Zwang, in Kenntnis der Sachlage und für den konkreten Fall erteilt worden sein“⁵⁹. Wie es in der Stellungnahme 15/2011 der Artikel 29-Datenschutzgruppe⁶⁰, heißt, kann eine Einwilligung nur dann gültig sein, wenn die betroffene Person eine tatsächliche Wahlmöglichkeit hat und kein Risiko einer Einschüchterung oder beträchtlicher negativer Folgen besteht, wenn sie die Einwilligung nicht erteilt. Wenn die Folgen einer Einwilligung die Wahlfreiheit einer natürlichen Person einschränken, wäre die Einwilligung nicht ohne Zwang.
80. Die Einführung der EES-Regelung und die vollständige Umsetzung des VIS⁶¹ dürften die bei Grenzkontrollen verbrachte Zeit verlängern und somit das RTP zur bevorzugten Option für Vielreisende machen. In diesem Zusammenhang sollte dafür gesorgt werden, dass die Einwilligung tatsächlich eine gültige Rechtsgrundlage für die Verarbeitung darstellt. Die Tatsache im Übrigen, dass es sich um ein freiwilliges System handelt, greift noch nicht der Bewertung der Notwendigkeit und Verhältnismäßigkeit des Systems sowie der Tatsache vor, dass seine Entwicklung und seine Funktionsweise von einem anderen System abhängen, nämlich dem EES.
81. Es könnte ferner sein, dass das RTP für Vielreisende zumindest bei der Erfassung einen erheblichen Zeit- und Verwaltungsaufwand bedeutet, denn sie müssen sich erneut für einen anderen Zweck die Fingerabdrücke abnehmen lassen und erneut die in Artikel 9 des RTP-Vorschlags verlangten Unterlagen vorlegen. Außerdem werden ihre alphanumerischen und biometrischen Daten fünf Jahre im System gespeichert, damit das Reiseverhalten personenbezogen kontrolliert werden kann. Noch steht nicht fest, wie effizient das RTP in der Praxis funktionieren wird.

⁵⁸ a.a.O. S. 5.

⁵⁹ Siehe Artikel 2 Buchstabe h der Richtlinie 95/46/EG.

⁶⁰Stellungnahme 15/2011 der Artikel 29-Datenschutzgruppe zur Definition von Einwilligung, angenommen am 13. Juli 2011.

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_de.pdf

⁶¹ Ibid., S. 16.

RTP und mögliche Diskriminierungsrisiken

82. Das RTP verlangt, dass alle Teilnehmer vorab auf Identität und Hintergrund überprüft werden. Den Prüfkriterien kommt daher entscheidende Bedeutung zu. Dies wird auch in der Begründung unterstrichen, wo es heißt: „*Absatz 2 (von Artikel 12) kommt entscheidende Bedeutung zu, weil dort die Kriterien für die Prüfung registrierter Reisender festgelegt werden*“⁶². Ein Blick auf die vom Antragsteller vorzulegenden Unterlagen und die von Visum- oder Grenzbehörden zu prüfenden Voraussetzungen zeigt, dass die Prüfkriterien für RTP an die Kriterien für die Prüfung von Anträgen auf Mehrfachvisa angepasst wurden⁶³. Der EDSB begrüßt, dass die Kriterien für beide Instrumente einander angepasst wurden.
83. Wie es jedoch in Artikel 2 des Vorschlags heißt, besteht sein Zweck darin, „vorab überprüften Vielreisenden aus Drittländern den Grenzübertritt an den Außengrenzen der EU zu erleichtern“. Es mag ein gewisses Diskriminierungsrisiko bestehen⁶⁴, da nur die Reisenden, die ein bestimmtes Registrierungsverfahren durchlaufen und detaillierte Angaben machen, als Reisende eingestuft würden, die ein „geringes Risiko“ darstellen, während die überwiegende Mehrzahl von Reisenden, die nicht häufig genug reisen, um sich registrieren zu lassen, oder deren Fingerabdrücke nicht lesbar sind⁶⁵, stillschweigend in die Kategorie von Reisenden eingeordnet würden, die ein „höheres Risiko“ darstellen.
84. In der Folgenabschätzung heißt es, dass ein potenzielles Diskriminierungsrisiko vor allem dann besteht, wenn die Überprüfung zu streng ausfällt. Dieses Thema sollte daher in das Schulungsprogramm über Grundrechte aufgenommen werden, das Frontex für Grenzbeamte organisiert. Es sollte deutlich gemacht werden, wie es auch in der Folgenabschätzung heißt, dass Personen, die keine automatisierten Grenzkontrollsysteme benutzen, nicht als mit einem größeren Risiko behaftete Reisende gelten⁶⁶. Zur Sensibilisierung der breiten Öffentlichkeit sollte dieses Thema auch in der Informationskampagne vor der Inbetriebnahme des RTP angesprochen werden. In den Faltblättern und auf den Plakaten muss deutlich zum Ausdruck gebracht werden, dass es den Reisenden frei steht, einen RTP-Antrag zu stellen und automatisierte Grenzkontrollsysteme zu benutzen. Nach Auffassung des

⁶² S. 10.

⁶³ Siehe Artikel 14, 21 und 24 des Visumskodex.

⁶⁴ Siehe die vorläufigen Kommentare des EDSB zu drei Mitteilungen der Kommission über Grenzverwaltung KOM(2008) 69, KOM(2008) 68 und KOM(2008) 67, 3. März 2008, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf;

Stellungnahme vom 7. Juli 2011 zu der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zur Migration, ABl. C 34/02 vom 8.2.2012, S. 18.

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-07-07_Migration_DE.pdf

⁶⁵ Siehe Artikel 8 und die Begründung des Vorschlags, wonach eine Befreiung von der Erhebung biometrischer Daten nicht zulässig ist.

⁶⁶ Siehe S. 39 der Folgenabschätzung.

EDSB könnten derartige Initiativen in gewissem Umfang das Risiko der Stigmatisierung vermeiden helfen.

Subjektive Beurteilungskriterien

85. Sowohl in Artikel 5 als auch in Artikel 9 wird das Kriterium der „Integrität und Zuverlässigkeit“ des Antragstellers erwähnt. Im Sinne von Rechtssicherheit und Gleichbehandlung sollten subjektive Kriterien wie „wenn der Antragsteller für seine Integrität und Zuverlässigkeit bekannt ist“ gestrichen oder durch objektivere Kriterien ersetzt werden, die sich überall in der EU gleichermaßen anwenden lassen.

Zu erhebende Datenkategorien

86. Artikel 12 und Artikel 15 des Vorschlags besagen, dass Visum- oder Grenzbehörden zu überprüfen haben, ob der Antragsteller nicht als Gefahr für die öffentliche Ordnung, die innere Sicherheit, die öffentliche Gesundheit oder die internationalen Beziehungen eines Mitgliedstaats eingestuft ist, insbesondere dass er nicht in den nationalen Datenbanken der Mitgliedstaaten zur Einreiseverweigerung aus denselben Gründen ausgeschrieben worden ist (Artikel 12 Absatz 2 Buchstabe h) und Artikel 15 Absatz 1 Buchstabe d)). Der EDSB empfiehlt, klarer darzustellen, wie eine solche Überprüfung stattfinden sollte, welche Art von Informationen Visum- oder Grenzbehörden berücksichtigen sollten, mit oder ohne Verknüpfung von Datenbanken, und welche Auswirkungen eine solche Verarbeitung hat.
87. Der Vorschlag sollte ferner einen Mechanismus für die Erfassung von Anträgen und Ersuchen natürlicher Personen vorsehen, damit nicht eine Person gleichzeitig Anträge in mehreren Mitgliedstaaten stellen kann, die möglicherweise unterschiedlich beschieden werden. Das für Anträge gemäß Artikel 24 verwendete Zentralregister könnte darauf überprüft werden, ob es nicht zur Vermeidung von Mehrfachanträgen herangezogen werden könnte.

Verbot internationaler Übermittlungen

88. Der EDSB begrüßt Artikel 42, der ausdrücklich besagt, dass Daten, die im Zentralregister oder während der Prüfung von Anträgen verarbeitet werden, in keinem Fall Drittstaaten oder internationalen Organisationen übermittelt oder zur Verfügung gestellt werden.

VI. SICHERHEITSEMPFEHLUNGEN FÜR EES UND RTP

89. Gemäß Artikel 23 des EES-Vorschlags und Artikel 37 des RTP-Vorschlags beschließt die Kommission die für die Entwicklung und technische Umsetzung der Systeme notwendigen Maßnahmen. EU-Lisa, die Agentur für IT-Großsysteme, ist für die restliche Entwicklung dieser Systeme verantwortlich.
90. Die Entwicklung von Systemen wie EES und RTP ist häufig sehr komplex und erfordert das Befolgen einer fundierten Methodik, damit am Ende ein hochwertiges Produkt steht. Bevor Teile eines solchen Systems entworfen und umgesetzt werden, wird bei fundierten Entwicklungsmethoden in der Regel zunächst der Bedarf ermittelt, damit alle Anforderungen berücksichtigt werden können. Sie können dann mit funktionellen, Datenschutz-, Sicherheits- und anderen Bedürfnissen verknüpft werden und müssen so identifiziert, sorgfältig beschrieben und dokumentiert werden, dass sie nach dem bestmöglichen kosteneffizienten Ansatz umgesetzt werden. Die Analyse-Phase ist auch der Augenblick, an dem Datenschutz durch Technik⁶⁷ und Datenschutz durch datenschutzfreundliche Voreinstellungen⁶⁸ berücksichtigt werden müssen. Eine gründliche Analyse zeigt ferner, wie die Anforderungen zueinander passen und gewährleistet, dass sich die verschiedenen Anforderungen nicht irgendwie beeinträchtigen.
91. Der EDSB empfiehlt, in den Vorschlägen sicherzustellen, dass vor dem Entwerfen und der Umsetzung von Teilen des Systems eine gründliche Bedarfsanalyse vorgenommen wird. Diese Analyse könnte gemeinsam von Kommission und Agentur durchgeführt werden, um zu gewährleisten, dass alle Anforderungen Berücksichtigung finden und nicht miteinander kollidieren.

Entwicklung und Betriebsmanagement

92. Gemäß Artikel 24 des EES-Vorschlags und Artikel 38 des RTP-Vorschlags ist die Agentur für die Entwicklung der verschiedenen Bestandteile des Systems verantwortlich. Die Entwicklung umfasst gemäß Artikel 24 Absatz 1 EES und Artikel 38 Absatz 1 RTP „die Ausarbeitung und Anwendung der technischen Spezifikationen, die Erprobung und die Projektgesamtkoordination“.
93. In den Testphasen der Entwicklung eines jeden Systems müssen zur Aufdeckung von Entwicklungsfehlern einige Daten (so genannte „Testdaten“) zur Beantwortung der Frage verwendet werden, ob sich die neu entwickelte Software erwartungsgemäß verhält. Die Testdaten sollten also ähnliche Merkmale wie die „echten“ Daten (personenbezogene Daten betroffener Personen, die im EES verarbeitet werden) aufweisen. Üblicherweise werden zu diesem Zweck die „echten“ Daten untersucht

⁶⁷ Berücksichtigung des Datenschutzes in allen Elementen ab den allerersten Anfängen des Einsatzes eines Systems.

⁶⁸ Möglichst datenschutzfreundliche Gestaltung der Aktivitäten als Standardeinstellung.

und es wird dann ein Testdatensatz zusammengestellt, der diesen ähnlich ist, aber keine personenbezogenen Daten offenlegt.

94. In Artikel 24 Absatz 1 EES und Artikel 38 Absatz 1 RTP ist jedoch nicht geregelt, was die Agentur mit den „echten“ Daten bei der Entwicklung des Systems macht, beispielsweise bei Tests, Überprüfungen, der Validierung oder der Testmigration zu neuen Versionen des Systems. Es sollte in diesen Bestimmungen klar zum Ausdruck gebracht werden, dass für keine dieser Funktionen personenbezogene Daten verwendet werden dürfen.
95. In Artikel 24 Absatz 2 EES und Artikel 38 Absatz 2 RTP wird die Betriebsbereitschaft der Plattform mit 24 Stunden am Tag und 7 Tagen in der Woche angegeben; das zeigt, dass diese Systeme von kritischer Bedeutung sind und ununterbrochen funktionieren müssen. Beim Aufbau von Systemen ist ein Notfallplan erforderlich, in dem genau festgelegt ist, wie die Organisation auf Zwischenfälle reagieren sollte, damit auch bei schwersten Störungen der Betrieb unter Kontrolle bleibt. Das Erfordernis eines Notfallplans sollte daher in Artikel 24 Absatz 2 EES und Artikel 38 Absatz 2 RTP aufgenommen werden, und für die Durchführungsmaßnahmen mit den Modalitäten eines solchen Plans sollte eine Rechtsgrundlage vorgesehen werden.

Nationale Zuständigkeiten

96. Die vorstehenden Anregungen gelten für die Mitgliedstaaten bei der Entwicklung ihrer nationalen Systeme gleichermaßen. In Artikel 25 EES und Artikel 39 RTP sollte klargestellt werden, dass weder für Tests, Überprüfungen und Validierung noch für Testmigrationen zu neuen Versionen der nationalen Systeme personenbezogene Daten verwendet werden dürfen.

Datensicherheit

97. Der EDSB begrüßt, dass Artikel 28 EES und Artikel 43 RTP ein ausreichendes Sicherheitsniveau zum Schutz von EES- und RTP-Daten gegen Bedrohungen anstreben. Die Festlegung von Maßnahmen sollte allerdings auf der Grundlage einer kontinuierlichen Verwaltung und Überwachung von Informationsrisiken erfolgen. Das Ziel dieses kontinuierlichen Prozesses, der häufig als Informationssicherheitsrisikomanagement bezeichnet wird, besteht darin, Risiken für die Informationen der Organisation zu ermitteln, zu beurteilen und in eine Rangfolge zu bringen, und Sicherheitsmaßnahmen festzulegen und umzusetzen, um die Risiken auf ein Niveau zu senken, das im Einklang mit den Bedürfnissen steht und für die Agentur und die Mitgliedstaaten annehmbar ist. Das Informationssicherheitsrisikomanagement sorgt auch dafür, dass der Kontext, in dem Daten verarbeitet und Anlagen genutzt werden, verständlich gemacht wird (auch mit Blick auf den Datenschutzbedarf); damit können kosteneffiziente Sicherheitskontrollen ausgewählt und angewandt werden, mit denen sich das angemessene Sicherheitsniveau erreichen lässt.

98. Der EDSB empfiehlt daher, in Artikel 28 EES und in Artikel 43 RTP klarzustellen, dass mit Hilfe von Maßnahmen des Informationssicherheitsrisikomanagements die angemessenen technischen und organisatorischen Maßnahmen bestimmt werden sollten, mit denen unter Berücksichtigung des gesamten Datenschutzbedarfs alle relevanten Daten geschützt werden können. Es sollte die Verpflichtung aufgenommen werden, Sicherheit durch geeignete Maßnahmen des Informationssicherheitsrisikomanagements zu schaffen, die sich stützen auf
- anerkannte internationale Standards,
 - regelmäßige Überprüfungen aller in diesem Zusammenhang vorgenommenen Analysen,
 - Überwachung und Überprüfung aller in diesem Zusammenhang durchgeführten technischen und organisatorischen Maßnahmen und
 - eine enge Zusammenarbeit zwischen der Agentur und den Mitgliedstaaten, um Sicherheitsrisiken über Informationssystemgrenzen hinweg bewältigen zu können.
99. Zu den in Artikel 28 EES und Artikel 43 RTP aufgeführten konkreten Maßnahmen Folgendes:
- In Artikel 28 Absatz 2 Buchstabe a) EES und Artikel 43 Absatz 2 Buchstabe a) RTP sollte „kritisch“ durch „relevant“ ersetzt werden.
 - In Artikel 28 Absatz 2 Buchstabe f) EES und Artikel 43 Absatz 2 Buchstabe f) RTP sollte der Ausdruck „vertrauliche Zugriffsverfahren“ näher erläutert werden.
 - In Artikel 28 Absatz 2 Buchstabe g) EES und Artikel 43 Absatz 2 Buchstabe g) RTP sollte hinzugefügt werden: „ihre Profile und andere relevante Informationen zur Verfügung stellen, die die Behörden zur Wahrnehmung der Aufsichtspflicht benötigen“.
 - In Artikel 28 Absatz 2 Buchstabe i) EES und in Artikel 43 Absatz 2 Buchstabe i) RTP sollte sichergestellt werden, dass die Protokolle sowie die dazu gehörenden Daten geschützt sind.
 - Zur Überwachung der Wirksamkeit der Sicherheitsmaßnahmen sollten in Artikel 28 Absatz 2 Buchstabe k) EES und Artikel 43 Absatz 2 Buchstabe k) RTP nicht nur Audits (also der Überblick über die Situation zu einem bestimmten Zeitpunkt), sondern auch eine Beobachtung des Systems mit Hilfe besonderer Instrumente fast in Echtzeit aufgenommen werden. Beide Bestimmungen sollten umformuliert werden, damit klar zwischen diesen beiden Konzepten unterschieden werden kann und sie richtig angewandt werden können.
 - Artikel 28 Absatz 3 EES und Artikel 43 Absatz 3 RTP sollten auch von der Agentur zu ergreifende Maßnahmen enthalten, mit denen die in Artikel 24 EES und Artikel 38 RTP beschriebene Verfügbarkeit und die Backups gewährleistet werden.
 - In Artikel 28 Absatz 3 EES und Artikel 43 Absatz 3 RTP sollte ferner der Notfallplan erwähnt werden (siehe oben).

100. Im Hinblick auf Sicherheitszwischenfälle sollten Artikel 28 EES und Artikel 43 RTP ferner Folgendes enthalten:

- Die Vorgabe für die Agentur und die Mitgliedstaaten, ein gemeinsames Bewertungssystem für Sicherheitszwischenfälle auszuarbeiten;
- die Vorgabe für die Agentur und die Mitgliedstaaten, Sicherheitszwischenfälle nach einem dokumentierten Prozess zu managen, sowie Aufzeichnungen über alle Sicherheitszwischenfälle und deren Beilegung zu führen;
- die Vorgabe für die Mitgliedstaaten, ihre nationalen Aufsichtsbehörden und die Agentur über in ihrem System festgestellte Sicherheitszwischenfälle zu unterrichten;
- die Vorgabe, dass während eines Sicherheitszwischenfalls alle Beteiligten zusammenzuarbeiten haben;
- die Vorgabe für die Agentur, bei einem schwerwiegenden Sicherheitszwischenfall die betroffenen Mitgliedstaaten, die entsprechende(n) nationale(n) Aufsichtsbehörde(n) und den EDSB zu unterrichten.

Führen von Aufzeichnungen

101. Zu Artikel 30 Absatz 2 EES und Artikel 45 RTP sei angemerkt, dass es Unterschiede zwischen i) den für die Datensicherheit verwendeten Protokollen und ii) den Protokollen gibt, mit denen überwacht, geprüft und kontrolliert wird, ob die Datenverarbeitung vorschriftsgemäß war. Der EDSB empfiehlt eine Unterteilung dieser Aufzeichnungen in zwei Kategorien (wobei eine Kategorie eine Unterkategorie der anderen sein kann), um zu vermeiden, dass im System gespeicherte personenbezogene Daten Sicherheitsbediensteten zur Kenntnis gelangen. Diese Aufzeichnungen sollten außerdem gegen unbefugten Zugriff und unbefugte Änderung geschützt werden.

VII. SCHLUSSFOLGERUNGEN

102. Ziel des Pakets „Intelligente Grenzen“ ist der Aufbau eines neuen IT-Großsystems als Ergänzung der bestehenden Grenzkontrollmechanismen. Die Rechtmäßigkeit dieses Systems muss vor dem Hintergrund der Grundsätze der Charta und hier vor allem von Artikel 7 über das Recht auf Achtung des Privat- und Familienlebens und von Artikel 8 über den Schutz personenbezogener Daten mit dem Ziel analysiert werden, nicht nur die Eingriffe des neuen Systems in Grundrechte, sondern auch die in den Vorschlägen formulierten Datenschutzgarantien zu bewerten.

103. In diesem Zusammenhang bekräftigt der EDSB, dass das vorgeschlagene EES einen Eingriff in das Recht auf Achtung des Privat- und Familienlebens darstellt. Er begrüßt zwar die Garantien in den Vorschlägen und erkennt an, dass sich die Kommission in diesem Sinne bemüht hat, kommt aber zu dem Schluss, dass das Hauptproblem nach wie vor die Notwendigkeit ist: Es geht um die Kosten bzw. den Nutzen des Systems, nicht nur finanziell betrachtet, sondern auch im Hinblick auf

Grundrechte, gesehen vor dem Gesamthintergrund bestehender Systeme und der bestehenden Grenzpolitik.

104. Bezüglich des EES spricht der EDSB folgende Empfehlungen aus:

- Die Notwendigkeit und Verhältnismäßigkeit des Systems kann erst dann im Einklang mit Artikel 7 der Charta positiv nachgewiesen werden, wenn eine eindeutige europäische Politik für den Umgang mit Overstayern formuliert und das System vor dem Gesamthintergrund bestehender IT-Großsysteme evaluiert worden ist.
- Die Datenschutzgrundsätze sollten im Einklang mit Artikel 8 folgendermaßen verbessert werden:
 - Es sollte eine Zweckbegrenzung vorgenommen und bei der Gestaltung des Systems der künftigen Evaluierung eines etwaigen Zugangs zu EES-Daten für Strafverfolgungsbehörden nicht vorgegriffen werden.
 - Die Rechte betroffener Personen sollten gestärkt werden, insbesondere das Recht auf Information und das Recht auf Rechtsbehelfe, wobei der Bedarf an spezifischen Garantien bei automatisierten Entscheidungen im Zusammenhang mit der Berechnung der Aufenthaltsdauer zu berücksichtigen ist.
 - Die Aufsicht sollte durch einen klaren Überblick über die Verteilung der Kompetenzen auf nationaler Ebene ergänzt werden, damit betroffene Personen ihre Rechte gegenüber der zuständigen Behörde wahrnehmen können.
 - Die Verwendung biometrischer Daten sollte Gegenstand einer gezielten Folgenabschätzung werden, und bei Bedarf sollte es bei der Verarbeitung dieser Daten besondere Garantien für die Erfassung, den Genauigkeitsgrad und die Notwendigkeit eines Ausweichverfahrens geben. Der EDSB stellt übrigens nachdrücklich in Frage, ob wirklich zehn und nicht nur zwei oder vier Fingerabdrücke genommen werden müssen, die für Überprüfungszwecke auf jeden Fall ausreichen würden.
 - Die Gründe, aus denen die Übermittlung von EES-Daten an Drittländer für die Rückführung von Drittstaatsangehörigen erforderlich ist, sollten näher ausgeführt werden.

105. Das RTP wirft zwar nicht die gleichen substanziellen Fragen im Hinblick auf Eingriffe in Grundrechte wie das EES auf, doch weist der EDSB den Gesetzgeber trotzdem auf folgende Aspekte hin:

- Das System beruht zugegebenermaßen auf Freiwilligkeit, doch sollte eine Einwilligung nur dann als gültige Rechtsgrundlage für die Verarbeitung der Daten angesehen werden, wenn sie ohne Zwang erteilt wird, wenn also das RTP nicht die einzige Alternative zu langen Warteschlangen und Verwaltungsaufwand ist.
- Diskriminierungsrisiken sollten ausgeräumt werden: Die überwiegende Mehrheit der Reisenden, die nicht häufig genug reisen, um sich registrieren zu lassen, oder deren Fingerabdrücke unlesbar sind, sollte

nicht de facto in die Kategorie von Reisenden eingeordnet werden, die ein größeres Risiko bedeuten.

- Grundlage des Überprüfungsprozesses vor der Registrierung sollte ein selektiver Zugang zu genau festgelegten Datenbanken sein.

106. Im Zusammenhang mit Sicherheitsaspekten vertritt der EDSB die Ansicht, dass für EES und RTP ein Notfallplan sowie Maßnahmen des Informationssicherheitsrisikomanagements zwecks Bewertung und Einordnung der Risiken in eine Rangfolge ausgearbeitet werden sollten. Außerdem sollte eine enge Zusammenarbeit zwischen der Agentur und den Mitgliedstaaten vorgesehen werden.

Brüssel, den 18. Juli 2013

(unterzeichnet)

Peter HUSTINX
Europäischer Datenschutzbeauftragter