DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für den kurzfristigen Aufenthalt (KOM(2004) 835 endg.)

(2005/C 181/06)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 286,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 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,

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, insbesondere auf Artikel 41,

gestützt auf das am 25. Januar 2005 eingegangene Ersuchen der Kommission um Stellungnahme nach Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. **EINLEITUNG**

1.1. **Vorbemerkungen**

Der Aufbau des Visa-Informationssystems (VIS) ist ein wichtiger Bestandteil der gemeinsamen Visumpolitik der EU und Gegenstand verschiedener ineinander greifender Rechtsakte.

— Im April 2003 wurde eine von der Kommission in Auftrag gegebene Durchführbarkeitsstudie ([1]) zum VIS vorgelegt.

— Im September 2003 schlug die Kommission die Änderung ([2]) einer früheren Verordnung vor, mit der ein einheitliches Visumformat festgeschrieben worden war. Hauptziel der Änderung war es, biometrische Daten (Gesichtsbild und zwei Fingerabdrücke) in das neue Visumformat aufzunehmen. Die biometrischen Daten sollen auf einem Mikrochip gespeichert werden.

([1]) Von der EG in Auftrag gegebener und unter der Leitung von Trasys erstellter Abschlussbericht zum Visa-Informationssystem, April 2003.
([2]) KOM(2003) 558 endg. sowie 2003/0217 (CNS) und 2003/0218 (CNS).

— Im Juni 2004 wurde durch einen Beschluss des Rates ([1]) der Prozess für den Aufbau des Visa-Informationssystems in die Wege geleitet und die Rechtsgrundlage für dessen Einbeziehung in den EU-Haushaltsplan geschaffen. Der Beschluss sieht eine zentrale Datenbank mit Informationen über Visumanträge und ein Ausschussverfahren im Hinblick auf die technische Entwicklung des VIS vor.

Im Dezember 2004 hat die Kommission einen Vorschlag für eine Verordnung über das VIS und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt ([2]) (im Folgenden „der Vorschlag") angenommen, der Gegenstand dieser Stellungnahme ist. Eine Studie zur ausführlichen Folgenabschätzung des Visa-Informationssystems ([3]) (im Folgenden „ausführliche Folgenabschätzung") ist dem Vorschlag beigefügt.

Wie aus der Begründung des Vorschlags hervorgeht, werden noch weitere Rechtsakte benötigt, um die Verordnung zu ergänzen, insbesondere

— zur Änderung der Gemeinsamen Konsularischen Instruktion an die diplomatischen Missionen und konsularischen Vertretungen der Vertragsparteien des Schengener Übereinkommens (im Folgenden „Gemeinsame Konsularische Instruktion") in Verbindung mit der Einführung von biometrischen Daten in die Verfahren;

— zur Entwicklung eines neuen Mechanismus für den Datenaustausch mit Irland und dem Vereinigten Königreich;

— für den Datenaustausch über Visa für einen langfristigen Aufenthalt.

Wie vom Rat (Justiz und Inneres) auf seiner Tagung vom 5./6. Juni 2003 beschlossen und in Artikel 1 Absatz 2 des oben genannten Beschlusses des Rates vom Juni 2004 beschrieben, wird das VIS über eine zentralisierte Architektur mit einer Datenbank, in der Datensätze über Visumanträge gespeichert werden — das zentrale Visa-Informationssystem (CS-VIS) –, sowie über eine nationale Schnittstelle (NI-VIS) in jedem Mitgliedstaat verfügen. Die Mitgliedstaaten benennen ([4]) eine zentrale nationale Behörde, die mit der nationalen Schnittstelle verbunden ist und über die die jeweils zuständigen Behörden Zugang zum CS-VIS haben.

1.2. **Hauptelemente des Vorschlags aus Sicht des Datenschutzes**

Der Vorschlag zielt darauf ab, die Verwaltung der gemeinsamen Visumpolitik dadurch zu verbessern, dass der Datenaustausch zwischen Mitgliedstaaten durch Aufbau einer zentralen Datenbank erleichtert wird. Die Verordnung sieht die Einführung biometrischer Daten (Foto und Fingerabdruck) in das Visaantrags-Verfahren und deren Speicherung in der zentralen Datenbank vor.

Biometrische Daten könnten auch in der Visummarke verwendet werden, wie in einer von der Kommission vorgeschlagenen Verordnung vorgesehen ist, die auf eine Änderung der Vorschriften über die einheitliche Visumgestaltung — nämlich Einführung von Foto und Fingerabdruck, die in einem Mikrochip gespeichert werden — abstellt (ein Beschluss des Rates hierzu steht noch aus, da er von Analyseergebnissen abhängt, die noch ausstehen).

In dem Vorschlag werden die verschiedenen Datentransaktionen (Eingabe, Änderung, Löschung und Abfrage) sowie die verschiedenen, in das VIS je nach Entwicklung des Antrags (Gewährung, Ablehnung, usw. …) einzugebenden Daten eingehend beschrieben.

Der Vorschlag sieht für die Speicherung der Antragsdatensätze jeweils eine Frist von fünf Jahren vor.

In dem Vorschlag sind die zuständigen Behörden, die nicht Visum-Behörden sind, aber Zugang zum VIS haben werden, erschöpfend aufgeführt; ferner werden die Zugangsrechte definiert, die ihnen gewährt werden sollen. Es handelt sich dabei um

— die für Visakontrollen an den Außengrenzen sowie im Hoheitsgebiet des Mitgliedstaats zuständigen Behörden,

— die zuständigen Einwanderungsbehörden,

([1]) 2004/512/EG, ABl. L 213 vom 15.6.2004, S. 5
([2]) KOM(2004) 835 endg. sowie 2004/0287 (COD).
([3]) Studie zur ausführlichen Folgenabschätzung des Visa-Informationssystems, EPEC-Abschlussbericht, Dezember 2004.
([4]) Artikel 24 Absatz 2 des Vorschlags.

— die zuständigen Asylbehörden.

In dem Vorschlag wird im Rahmen der Beschreibung des VIS-Betriebs und der damit zusammenhängenden Verantwortlichkeiten betont, dass die Kommission die VIS-Daten im Namen der Mitgliedstaaten verarbeitet. Es wird auf die Notwendigkeit hingewiesen, zur Gewährleistung der Datensicherheit die Aufzeichnungen über die Datenverarbeitungsvorgänge zu verwenden; ferner werden detaillierte Angaben betreffend die jeweiligen Verantwortlichkeiten zur Sicherstellung dieses Sicherheitsniveaus gemacht.

Der Vorschlag enthält ein Kapitel über den Datenschutz, in dem die Aufgaben der nationalen Behörden sowie des Europäischen Datenschutzbeauftragten (im Folgenden „EDPS“) im Einzelnen aufgeführt sind.

Gemäß dem Vorschlag werden die technische Implementierung des VIS und die Wahl der erforderlichen Technologien einem Ausschuss nach Artikel 5 Absatz 1 der Verordnung (EG) Nr. 2424/2001 über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II) übertragen.

Eine von der Kommission in Auftrag gegebene und unter Leitung des EPEC durchgeführte ausführliche Folgenabschätzung des VIS ist dem Vorschlag beigefügt. Fazit dieser Folgenabschätzung ist, dass die Option eines VIS, das durch die Verwendung von biometrischen Daten unterstützt wird, die bestmögliche Lösung für eine Verbesserung der gemeinsamen Visumpolitik darstellt.

2. **RELEVANTER RAHMEN**

Der Vorschlag wird erhebliche Auswirkungen auf die Privatsphäre und andere persönliche Grundrechte haben; daher ist er Gegenstand einer datenschutzrechtlichen Kontrolle. Bei unserer Prüfung sind wir in erster Linie von folgenden Bezugspunkten ausgegangen:

— Die Wahrung der Privatsphäre ist in Europa seit dem Erlass der Konvention zum Schutz der Menschenrechte und Grundfreiheiten (im Folgenden „EMRK“) durch den Europarat im Jahre 1950 sichergestellt. In Artikel 8 EMRK ist „das Recht auf Achtung des Privat- und Familienlebens“ festgeschrieben.

  Nach Artikel 8 Absatz 2 ist der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts nur statthaft, insoweit er „gesetzlich vorgesehen“ und „in einer demokratischen Gesellschaft“ zum Schutz wichtiger Interessen „notwendig“ ist. Der Europäische Gerichtshof für Menschenrechte hat aufgrund dieser Bedingungen in seiner Rechtsprechung zusätzliche Anforderungen vorgesehen, die die Art der Rechtsgrundlage für einen solchen Eingriff, dessen Verhältnismäßigkeit sowie die Notwendigkeit angemessener Maßnahmen zum Schutz vor Missbrauch betreffen.

  Elementare Grundsätze für den Personenschutz im Zusammenhang mit der Verarbeitung personenbezogener Daten wurden im Rahmen des vom Europarat erstellten und 1981 verabschiedeten Datenschutz-Übereinkommens ausgearbeitet.

— In jüngerer Zeit wurden das Recht auf Achtung des Privatlebens und der Schutz personenbezogener Daten in Artikel 7 bzw. 8 der Charta der Grundrechte der Europäischen Union festgeschrieben, die in Teil II der neuen EU-Verfassung aufgenommen wurde.

  Nach Artikel 52 der Charta können diese Rechte Einschränkungen unterliegen, vorausgesetzt dass ähnliche Bedingungen erfüllt sind wie unter Artikel 8 EMRK. Diese Bedingungen sind bei Entscheidungen über einen vorgeschlagenen Eingriff stets zu berücksichtigen.

Die Grundregeln für den Datenschutz sind im EU-Recht derzeit in folgenden Rechtsakten niedergelegt:

— 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 (ABl. L 281, S. 31) (im Folgenden „Richtlinie 95/46/EG“). Diese Richtlinie enthält detaillierte Grundsätze, an denen der Vorschlag insoweit zu messen sein wird, als er auf die Mitgliedstaaten Anwendung finden soll. Dies gilt umso mehr, als der Vorschlag zusammen mit den nationalen Rechtsvorschriften, die der Richtlinie Rechtswirksamkeit verleihen, angewendet werden wird. Die Effizienz der vorgeschlagenen Bestimmungen und Schutzmaßnahmen wird somit in jedem einzelnen Fall von der Effizienz dieser Kombination abhängen.

— 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 (ABl. L 8, S. 1) (im Folgenden „Verordnung 45/2001"). Diese Verordnung enthält ähnliche Grundsätze wie die Richtlinie 95/46/EG und ist hier insoweit relevant, als der Vorschlag zusammen mit den Bestimmungen der Verordnung auf die Tätigkeit der Kommission Anwendung finden soll. Diese Kombination ist daher ebenfalls zu prüfen.

Die Richtlinie 95/46/EG und die Verordnung 45/2001 sind in Verbindung mit anderen Rechtsakten zu sehen, d.h. dass die Richtlinie und die Verordnung, insoweit sie die Verarbeitung personenbezogener Daten betreffen, die die Grundfreiheiten und insbesondere das Recht auf Privatsphäre verletzen könnten, unter Berücksichtigung der Grundrechte auszulegen sind. Dies ergibt sich auch aus der Rechtsprechung des Europäischen Gerichtshofs ([1]).

— Schließlich wird der EDPS in seine Analyse auch die von der Datenschutzgruppe „Artikel 29" ([2]) ausgearbeitete Stellungnahme Nr. 7/2004 vom 1. August 2004 „zur Aufnahme biometrischer Merkmale in Visa und Aufenthaltstitel unter Berücksichtigung des Aufbaus des Visa-Informationssystems VIS" einbeziehen. In dieser Stellungnahme äußerte die Gruppe Bedenken in Bezug auf mehrere Elemente des Vorschlags. Der EDPS wird prüfen, ob und wie der Vorschlag diesen Bedenken Rechnung trägt.

3. ANALYSE DES VORSCHLAGS

3.1. Allgemeines

Der EDPS erkennt an, dass für die weitere Entwicklung einer gemeinsamen Visumpolitik ein effizienter Austausch relevanter Daten erforderlich ist. Einer der Mechanismen, der einen reibungslosen Informationsfluss gewährleisten kann, ist das VIS. Allerdings sollte ein derartiges neues Instrument beschränkt werden auf die Erhebung und den Austausch von Daten, soweit sie für die Entwicklung einer gemeinsamen Visumpolitik erforderlich sind und in einem adäquaten Verhältnis zu diesem Ziel stehen.

Der Aufbau des VIS kann positive Auswirkungen auf andere berechtigte öffentliche Interessen haben, was am Zweck des VIS jedoch nichts ändert. Der begrenzte Zweck des Systems spielt eine erhebliche Rolle im Hinblick auf die Bestimmung des rechtmäßigen Inhalts und der rechtmäßigen Verwendung des Systems und somit auch auf die Gewährung eines Rechts auf Zugang zum VIS (oder zu Teilen der VIS-Daten) für Behörden der Mitgliedstaaten im Interesse berechtigter öffentlicher Interessen.

Darüber hinaus sieht der Vorschlag die Einführung biometrischer Daten in das VIS vor. Der EDPS erkennt die Vorteile der Nutzung biometrischer Daten an, macht aber darauf aufmerksam, dass die Verwendung solcher Daten erhebliche Folgen hat, und schlägt die Einbeziehung strikter Schutzmaßnahmen für die Verwendung biometrischer Daten vor.

Diese Stellungnahme versteht sich unter Berücksichtigung dieser grundsätzlichen Erwägungen und sollte in der Präambel der Verordnung vor den Erwägungsgründen erwähnt werden („gestützt auf die Stellungnahme ...").

([1]) In diesem Zusammenhang sei auf das Urteil des Gerichtshofs in der Rechtssache Österreichischer Rundfunk und andere (Verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, Urteil vom 20. Mai 2003, Plenum, Slg. 2003, I-4989) hingewiesen. Der Gerichtshof hatte über ein österreichisches Gesetz zu entscheiden, das die Weitergabe von Daten betreffend die Bezüge von öffentlichen Bediensteten an den österreichischen Rechnungshof und deren anschließende Veröffentlichung vorsah. In seinem Urteil legt der Gerichtshof anhand von Artikel 8 der Europäischen Konvention für Menschenrechte eine Reihe von Kriterien fest, die bei der Anwendung der Richtlinie 95/46/EG gelten sollen, insoweit diese Richtlinie gewisse Einschränkungen des Rechts auf Privatsphäre gestattet.

([2]) Es handelt sich um ein unabhängiges Beratungsgremium aus Vertretern der Datenschutzbehörden der Mitgliedstaaten, des EDPS und der Kommission, die mit der Richtlinie 95/46/EG eingesetzt wurde.

3.2. **Zweck**

Der Zweck des VIS ist von größter Bedeutung sowohl im Lichte des Artikels 8 EMRK als auch des allgemeinen Rahmens des Datenschutzes. Nach Artikel 6 der Richtlinie 95/46/EG müssen personenbezogene Daten „für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden". Nur eine klare Definition der Zweckbestimmungen wird eine korrekte Bewertung der Verhältnismäßigkeit und der Zweckdienlichkeit der Verarbeitung personenbezogener Daten ermöglichen, die in Anbetracht der Art der Daten (einschließlich der biometrischen Daten) und des Umfangs des in Betracht gezogenen Verarbeitungsvorgangs heikel ist.

Der Zweck des VIS ist in Artikel 1 Absatz 2 des Vorschlags klar umrissen:

> „Das VIS dient zur Verbesserung der Durchführung der gemeinsamen Visapolitik, der konsularischen Zusammenarbeit und der Konsultation zwischen zentralen Konsularbehörden durch die Erleichterung des Datenaustausches zwischen Mitgliedstaaten über Visumanträge und die diesbezüglichen Entscheidungen".

Infolgedessen müssen alle Elemente des VIS notwendige und angemessene Instrumente zur Erreichung dieses politischen Ziels im Interesse der gemeinsamen Visumpolitik sein.

In Artikel 1 Absatz 2 des Vorschlags sind ferner zusätzliche Vorteile einer Verbesserung der Visumpolitik aufgeführt, bei denen es z.B. darum geht,

a) einer Bedrohung der inneren Sicherheit eines Mitgliedstaats vorzubeugen;

b) die Betrugsbekämpfung zu erleichtern;

c) Kontrollen an den Außengrenzen zu erleichtern.

Der EDPS betrachtet diese Elemente zwar als Beispiele für positive Auswirkungen des Aufbaus des VIS und der Verbesserung der gemeinsamen Visumpolitik, aber nicht an sich als autonome Zweckbestimmungen.

Dies hat zum gegenwärtigen Zeitpunkt zweierlei Hauptfolgen:

— Der EDPS ist sich bewusst, dass die Strafverfolgungsbehörden an einem VIS-Zugang interessiert sind; der Rat hat am 7. März 2005 Schlussfolgerungen in diesem Sinne angenommen. Da der Zweck des VIS die Verbesserung der gemeinsamen Visumpolitik ist, sei festgestellt, dass ein Routinezugang der Strafverfolgungsbehörden nicht im Einklang mit dieser Zweckbestimmung steht. Gemäß Artikel 13 der Richtlinie 95/46/EG könnte ein solcher Zugang zwar unter bestimmten Umständen und vorbehaltlich angemessener Schutzmaßnahmen auf Ad-hoc-Basis gewährt werden; ein systematischer Zugang kann aber nicht gestattet werden.

  Generell ist eine Bewertung der Verhältnismäßigkeit und der Notwendigkeit entscheidend im Hinblick auf künftige Beschlüsse darüber, ob bestimmten anderen Behörden ein Zugang zum VIS gewährt werden soll. Die Aufgaben, für die ein solcher Zugang gewährt wird, müssen mit den Zweckbestimmungen des VIS vereinbar sein.

— Der ausdrückliche Hinweis auf die „Vorbeugung einer Bedrohung der inneren Sicherheit eines Mitgliedstaats" unter Buchstabe a ist ungeschickt. Hauptvorteil des VIS ist die Vorbeugung des Betrugs und des Visum-Shopping (die Betrugsbekämpfung ist auch der Hauptgrund für die Einbeziehung der biometrischen Daten in das System) ([1]). Die Vorbeugung einer Bedrohung der Sicherheit sollte daher als „sekundär" angesehen werden, auch wenn sie einen sehr willkommenen Vorteil darstellt.

  Der EDPS empfiehlt, dass diese Unterscheidung zwischen „Zweck" und „Vorteilen" im Wortlaut des Artikels 1 Absatz 2 expliziter zum Ausdruck kommt, beispielsweise durch folgende Formulierung:

  „Zweck des VIS ist es, die Durchführung der gemeinsamen Visumpolitik, der konsularischen Zusammenarbeit und der Konsultation zwischen zentralen Konsularbehörden durch die Erleichterung des Datenaustauschs zwischen Mitgliedstaaten über Visumanträge und die diesbezüglichen Entscheidungen zu verbessern. Damit trägt es auch dazu bei, …".

([1]) In der ausführlichen Folgenabschätzung kommt dies sehr deutlich zum Ausdruck (S. 6 Nr. 2.7). Darin heißt es, dass die mangelnde Effizienz bei der Bekämpfung des Visa-Shopping und des Betrugs sowie bei den Kontrollen auch eine mangelnde Effizienz in Bezug auf die innere Sicherheit der Mitgliedstaaten zur Folge hat. Dies bedeutet, dass Bedrohungen für die Sicherheit zum Teil einer ineffizienten Visumpolitik zuzuschreiben sind. Hier gilt es als Erstes, die Visumpolitik zu verbessern, insbesondere durch Betrugsbekämpfung und bessere Kontrollen. Eine Verbesserung der Sicherheit wird sich dann aus der Verbesserung der Visumpolitik ergeben.

In diesem Zusammenhang sei ferner darauf hingewiesen, dass in den vom JI-Rat am 13. Juni 2002 angenommenen „Leitlinien für die Einführung eines gemeinsamen Systems für den Austausch von Visa-Daten" ([1]) die Vorbeugung einer Bedrohung der inneren Sicherheit am Ende der Liste steht. Dies wäre auch hier möglich und stünde im Übrigen mit dem Zweck des VIS stärker in Einklang.

3.3. **Datenqualität**

Nach Artikel 6 der Richtlinie 95/46/EG ist ferner vorzusehen, dass personenbezogene Daten „den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen". Damit wird Bezug genommen auf die Verhältnismäßigkeit des VIS selbst, aber auch auf die Daten, die erhoben und im VIS gespeichert werden sollen, auf ihre weitere Verwendung sowie auf die zusätzlichen Schutzmaßnahmen, die in diesem Zusammenhang angewendet werden. Diese Elemente sind gleichermaßen wichtig für die Bewertung des Vorschlags im Lichte des Artikels 8 EMRK.

Der Aufbau des VIS stellt ohne jeden Zweifel schon allein wegen des Umfangs des Systems und der Kategorie der verarbeiteten personenbezogenen Daten einen erheblichen Eingriff in die Ausübung des Rechts auf Privatsphäre dar. Daher ersucht die Gruppe „Artikel 29" in ihrer Stellungnahme Nr. 7/2004 auch darum, in Kenntnis gesetzt zu werden, „welche Studien über das Ausmaß und die Gewichtigkeit der drohenden Gefahren belegen, dass dieses Vorgehen zum Schutz der öffentlichen Sicherheit und Ordnung unerlässlich ist".

Der EDPS hat den in der ausführlichen Folgenabschätzung enthaltenen Nachweis mit Sorgfalt zur Kenntnis genommen. Auch wenn dieser nicht gänzlich schlüssig ist, so dürften doch ausreichende Gründe vorliegen, die den Aufbau des VIS zum Zwecke der Verbesserung der gemeinsamen Visumpolitik rechtfertigen.

Infolgedessen dürfte es im Ermessensbereich des Gesetzgebers liegen, über den Aufbau des VIS als einem Instrument zur Verbesserung der Bedingungen für die Visumerteilung durch die Mitgliedstaaten zu entscheiden. Ein solches System könnte sich gut in den Raum der Freiheit, der Sicherheit und des Rechts, wie im EG-Vertrag vorgesehen, einfügen und dessen schrittweise Einführung stützen.

Allerdings dürften der Aufbau und die Verwendung des VIS keinesfalls zur Folge haben, dass ein hohes Schutzniveau für personenbezogene Daten in diesem Bereich nicht mehr gewährleistet wird. Zur beratenden Funktion des EDPS gehört es zu prüfen, inwieweit das VIS das bestehende Datenschutzniveau für die von den Daten betroffenen Personen beeinträchtigt.

Vor diesem Hintergrund wird sich der EDPS in dieser Stellungnahme auf die folgenden Punkte konzentrieren:

— Verhältnismäßigkeit und Angemessenheit der Daten und ihrer Verwendung (z.B. Datenkategorien, Datenzugang der einzelnen betroffenen Behörden und Speicherungszeitraum);

— Betrieb des Systems (z.B. Verantwortlichkeiten und Sicherheit);

— Rechte der von den Daten betroffenen Personen (z.B. Unterrichtung, Möglichkeit der Korrektur oder Löschung ungenauer oder irrelevanter Daten);

— Überwachung und Aufsicht des Systems.

Von den folgenden Abschnitten abgesehen gibt der Vorschlag keinen Anlass zu umfangreichen Kommentaren hinsichtlich der für eine Aufnahme in das VIS vorgesehenen Datenkategorien und ihrer Verwendung. Die einschlägigen Bestimmungen wurden mit der gebührenden Sorgfalt abgefasst und scheinen insgesamt kohärent und angemessen.

([1]) *Rahmenbeschluss des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung* (2002/475/JI), ABl. L 164 vom 22. Juni 2002, S. 3.

3.4. **Biometrische Daten**

3.4.1. *Auswirkungen der Verwendung von biometrischen Daten*

Die Verwendung von biometrischen Daten in Informationssystemen ist keineswegs eine unbedeutende Entscheidung, besonders dann nicht, wenn das betreffende System eine solch hohe Zahl von Personen betrifft. Biometrische Daten stellen nicht einfach nur eine andere Informationstechnologie dar. Vielmehr ändern sie unwiderruflich die Beziehung zwischen Körper und Identität, insofern sie die Merkmale des menschlichen Körpers „maschinenlesbar" machen und damit ihre weitere Verwendung ermöglichen. Auch wenn die biometrischen Daten nicht vom menschlichen Auge gelesen werden können, so können sie doch mit entsprechenden Hilfsmitteln gelesen und verwendet werden, und das für unbegrenzte Zeit, wo immer die betreffende Person sich auch aufhält.

So nützlich biometrische Daten für bestimmte Zwecke auch sein mögen, ihre weit verbreitete Verwendung wird weit reichende Auswirkungen auf die Gesellschaft haben und sollte offen und umfassend erörtert werden. Der EDPS muss darauf hinweisen, dass eine solche Erörterung vor der Ausarbeitung des Vorschlags nicht wirklich stattgefunden hat. Dies unterstreicht umso mehr die Notwendigkeit strikter Schutzmaßnahmen für die Verwendung biometrischer Daten und einer sorgfältigen Reflexion und Erörterung im Laufe des Gesetzgebungsprozesses.

3.4.2. *Besondere Natur der biometrischen Daten*

Wie bereits in verschiedenen Stellungnahmen der Gruppe „Artikel 29" betont ([1]), müssen für die Einführung und die Verarbeitung von biometrischen Daten für Identitätsdokumente besonders konsequente und strenge Schutzmaßnahmen vorgesehen werden. Aufgrund einiger spezifischer Merkmale handelt es sich bei biometrischen Daten nämlich um höchst sensible Daten.

So ist der Verlust biometrischer Daten kaum möglich, im Gegensatz zum Verlust eines Passworts oder eines Schlüssels. Die biometrischen Daten weisen eine *nahezu absolute Einmaligkeit* auf, d.h. jede Person besitzt einzigartige biometrische Daten. Sie ändern sich im Laufe des Lebens fast nie, so dass diese Merkmale *konstanter Natur* sind. Jeder verfügt über dieselben physischen „Faktoren", was den biometrischen Daten *Universalität* verleiht.

Allerdings ist die Annullierung biometrischer Daten nahezu unmöglich: ein Finger oder ein Gesicht ist schwer zu verändern. Dieses an sich positive Element birgt in vielerlei Hinsicht eine negative Komponente im Falle des *Identitätsdiebstahls*: die Speicherung von Fingerabdrücken und eines Fotos in einer Datenbank in Verbindung mit einer gestohlenen Identität könnte größere und dauerhafte Probleme für den tatsächlichen Eigentümer dieser Identität zur Folge haben. Darüber hinaus sind biometrische Daten naturgemäß *nicht geheim*; sie können sogar *Spuren hinterlassen* (Finger-abdrücke, DNA), die die Erhebung dieser Daten ermöglichen, *ohne dass ihr Eigentümer es bemerkt*.

Aufgrund dieser Risiken, die sich aus der Natur der biometrischen Daten ergeben, ist die Einführung umfangreicher Schutzmaßnahmen unerlässlich (insbesondere im Hinblick auf die Wahrung des Grundsatzes der Zweckbindung, auf die Zugangsbeschränkung und auf die Sicherheitsmaßnahmen).

3.4.3. *Technische Mängel bei Fingerabdrücken*

Die wichtigsten, oben beschriebenen Vorteile von biometrischen Daten (Universalität, Einmaligkeit, Konstanz, Benutzbarkeit, usw.) sind niemals absolut. Dies hat direkte Auswirkungen auf die Effizienz der in der Verordnung vorgesehenen biometrischen Erfassimgs- und Überprüfungsverfahren.

Schätzungen zufolge ([2]) können bis zu 5 % der Menschen nicht erfasst werden (weil ihre Fingerabdrücke nicht lesbar oder gar inexistent sind). Nach der dem Vorschlag beigefügten ausführlichen Folgenabschätzung werden für 2007 rund 20 MillionenVisum-Antragsteller erwartet, was bedeutet, dass bis zu 1 Million Menschen sich nicht für das „normale" Erfassungsverfahren eignen werden, mit offensichtlichen Folgen für Visumantrag und Grenzkontrollen.

([1]) Stellungnahme 7/2004 zur Aufnahme biometrischer Merkmale in Visa und Aufenthaltstitel unter Berücksichtigung des Aufbaus des Visa-Informationssystems VIS (Markt/11487/04/EN - WP 96) sowie Arbeitsunterlage über biometrische Daten (MARKT/10595/03/EN - WP 80).

([2]) A. Sasse, *Cybertrust and Crime Prevention: Usability and Trust in Information Systems, in*„Foresight cybertrust and crime prevention project", 04/1151, 10. Juni 2004, S. 7, und „Using Biometrics for Border Security", United States General Accounting Office, GAO-03-174, November 2002.

Die biometrische Identifizierung ist außerdem definitionsgemäß ein statistischer Prozess. Eine Fehlerrate von 0,5 bis 1 % ist normal ([1]), d.h. dass das Kontrollsystem an den Außengrenzen eine Falschrückweisungsrate (FRR) zwischen 0,5 und 1 % aufweisen wird. Der genaue Wert dieser Rate hängt von einer der Risikopolitik der zuständigen Behörden entsprechenden Marge ab (und entspricht der Bilanz aus der Zahl der fälschlicherweise zurückgewiesenen Personen und der fälschlicherweise akzeptierten Personen). Daher ist wohl kaum davon auszugehen, dass diese Technologien eine „genaue Identifizierung" der jeweiligen Person gestatten, wie es im Erwägungsgrund 9 der vorgeschlagenen Verordnung heißt.

Gemäß einer vom LIBE-Ausschuss des Europäischen Parlaments in Auftrag gegebenen und unlängst durchgeführten Prospektivstudie ([2]) sollten Ausweichverfahren (*fallback procedures*) als wesentliche Schutzmaßnahmen für die Einführung biometrischer Daten zur Verfügung stehen, da letztere weder für alle zugänglich noch absolut genau sind. Solche Verfahren sollten eingeführt und in Anspruch genommen werden, um die Würde der Personen, die den Erfassungs-Prozess nicht erfolgreich absolvieren konnten, zu wahren und zu vermeiden, dass sie unter den Mängeln des Systems zu leiden haben ([3]).

Der EDPS empfiehlt daher, dass Ausweichverfahren entwickelt und in den Vorschlag einbezogen werden. Diese Verfahren sollten weder eine Senkung des Sicherheitsniveaus im Bereich der Visumpolitik zur Folge haben noch einzelne Personen mit „unlesbaren" Fingerabdrücken stigmatisieren.

3.5. **Besondere Datenkategorien**

Abgesehen von den biometrischen Daten erfordern auch einige andere Datenkategorien besondere Beachtung: die Daten betreffend die Gründe für die Ablehnung der Visumerteilung (3.5.1.) und die Daten betreffend andere Mitglieder einer Gruppe (3.5.2.).

3.5.1. *Gründe für die Ablehnung der Visumerteilung*

Artikel 10 Absatz 2 des Vorschlags regelt die Verarbeitung der Daten betreffend die Ablehnungsgründe, d.h. in den Fällen, in denen eine Entscheidung ergangen ist, mit der die Visumerteilung abgelehnt wird. Diese Ablehnungsgründe sind gänzlich standardisiert.

— Die ersten beiden Gründe unter den Buchstaben a und b sind vor allem administrativer Natur: keine Vorlage eines gültigen Reisedokuments bzw. keine Vorlage von Unterlagen zum Nachweis des Zwecks und der Bedingungen des geplanten Aufenthalts.

— Buchstabe c lautet „der Antragsteller ist zur Einreiseverweigerung ausgeschrieben"; dazu ist eine Konsultation der SIS-Datenbank erforderlich.

— Schließlich wird unter Buchstabe d als Grund für die Ablehnung der Visumerteilung Folgendes angegeben: „der Antragsteller stellt eine Gefahr für die öffentliche Ordnung, die innere Sicherheit, die öffentliche Gesundheit oder die internationalen Beziehungen eines Mitgliedstaats dar".

([1])

Biometrische Daten	Gesicht	Finger	Iris
FTE % Nutzerausfallrate	entfällt	4	7
FNMR % Rückweisungsrate	4	2,5	6
FMR1 % Erkennungsfehler-Rate bei Überprüfung	10	< 0,01	< 0,001
FMR2 % Erkennungsfehler-Rate bei Identifizierung dB Größe > 1 m	40	0,1	entfällt
FMR3 % Erkennungsfehler-Rate beim Screening dB Größen = 500	12	< 1	entfällt

A.K. Jain u.a., *Biometrics: A grand Challenge*, Berichte der Internationalen Konferenz für Mustererkennung, Cambridge, UK, August 2004.

([2]) *Biometrics at the frontiers: assessing the impact on Society*, Februar 2005, Institut für Technologische Zukunftsforschung, GD Gemeinsame Forschungsstelle, EG.

([3]) *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (Fortschrittsbericht über die Anwendung der Grundsätze des Übereinkommens 108 auf die Erfassung und Verarbeitung biometrischer Daten)*, Europarat, 2005, S. 11.

Alle Ablehnungsgründe müssen in Anbetracht ihrer Folgen für die betroffene Person mit großer Sorgfalt angewendet werden. Einige dieser Gründe — nämlich die unter den Buchstaben c und d — werden die Verarbeitung „sensibler Daten" im Sinne des Artikels 8 der Richtlinie 95/46/EG nach sich ziehen.

Der EDPS möchte insbesondere auf das Kriterium der öffentlichen Gesundheit hinweisen, das vage erscheint und die Verarbeitung sehr sensibler Daten zur Folge hat. Gemäß dem Kommentar zu den Artikeln, der dem Vorschlag beigefügt ist, geht die Bezugnahme auf die Gefahr für die öffentliche Gesundheit zurück auf den „Vorschlag für eine Verordnung des Rates über den Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen" (KOM(2004) 391 endg.).

Der EDPS ist sich bewusst, dass ein Kriterium der „öffentlichen Gesundheit" in den Gemeinschaftsvorschriften über die Freizügigkeit vielfach herangezogen und sehr strikt angewendet wird; ein Beispiel dafür ist die Richtlinie 2004/38/EG des Europäischen Parlaments und des Rates vom 29. April 2004 über das Recht der Unionsbürger und ihrer Familienangehörigen, sich im Hoheitsgebiet der Mitgliedstaaten frei zu bewegen und aufzuhalten. Artikel 29 dieser Richtlinie legt die Bedingungen für eine Anwendung des Kriteriums der Gefahr für die öffentliche Gesundheit fest: „Als Krankheiten, die eine die Freizügigkeit beschränkende Maßnahme rechtfertigen, gelten ausschließlich die Krankheiten mit epidemischem Potenzial im Sinne der einschlägigen Rechtsinstrumente der Weltgesundheitsorganisation und sonstige übertragbare, durch Infektionserreger oder Parasiten verursachte Krankheiten, sofern gegen diese Krankheiten Maßnahmen zum Schutz der Staatsangehörigen des Aufnahmemitgliedstaats getroffen werden."

— Dennoch sei darauf hingewiesen, dass der oben genannte Vorschlag bislang nur ein Vorschlag ist und dass die Einbeziehung der Bedingung, dass keine Gefahr für die öffentliche Gesundheit vorliegen darf, in die VIS-Verordnung von der Annahme Vorschlags über den Gemeinschaftskodex abhängt.

— Darüber hinaus ist dieser Grund für eine Ablehnung der Einreise, sollte dieser Vorschlag angenommen werden, restriktiv auszulegen. Der Vorschlag für einen Gemeinschaftskodex stützt sich nämlich seinerseits auf die vorstehend erwähnte Richtlinie 2004/38/EG.

Der EDPS empfiehlt daher, dass eine Bezugnahme auf Artikel 29 der Richtlinie 2004/38/EG in den Vorschlagstext aufgenommen wird, um sicherzustellen, dass eine „Gefahr für die öffentliche Gesundheit" unter Berücksichtigung der dort genannten Bestimmung ausgelegt wird. In jedem Fall sollten die betreffenden Daten in Anbetracht ihrer Sensibilität nur verarbeitet werden, wenn die Gefahr für die öffentliche Gesundheit tatsächlich, gegenwärtig und erheblich ist.

3.5.2. *Daten über andere Mitglieder einer Gruppe*

In Artikel 2 Absatz 7 wird der Begriff „Gruppenmitglieder" wie folgt definiert: „andere Antragsteller, mit denen der Antragsteller gemeinsam reist, einschließlich des Ehegatten und der Kinder, die den Antragsteller begleiten". In dem Kommentar zu den Artikeln wird darauf hingewiesen, dass sich die Begriffsbestimmungen in Artikel 2 des Vorschlags auf den Vertrag bzw. den Schengen-Besitzstand im Bereich der Visumpolitik beziehen, mit Ausnahme einiger Begriffe — zu denen auch der Begriff „Gruppenmitglieder" gehört – , die speziell für die Zwecke dieser Verordnung definiert werden. Daher kann davon ausgegangen werden, dass sich diese Begriffsbestimmung nicht auf die Definition des Begriffs „Gruppenvisum" in Artikel 2.1.4 der Gemeinsamen Konsularischen Instruktion bezieht. In dem Kommentar zu den Artikeln heißt es „Antragsteller, die in einer Gruppe mit anderen Antragstellern reisen, z.B. im Rahmen eines ADS-Abkommens, oder zusammen mit Familienmitgliedern".

Der EDPS betont, dass die Verordnung eine genaue und umfassende Definition des Begriffs „Gruppenmitglieder" enthalten sollte. Im derzeitigen Vorschlag fehlt eine genaue Bezugnahme auf den Vertrag bzw. den Schengen-Besitzstand, so dass der EDPS feststellen muss, dass die Definition zu vage ist. Dem derzeitigen Wortlaut zufolge könnte der Begriff auch Kollegen, andere Kunden desselben Reisebüros, die an einer organisierten Reise teilnehmen, usw. umfassen. Die Folgen sind in der Tat gravierend:

nach Artikel 5 des Verordnungsentwurfs wird der Antragsdatensatz eines Antragstellers nämlich mit denen der anderen Gruppenmitglieder verknüpft.

3.6. **Speicherung der Daten**

Nach Artikel 20 des Verordnungsentwurfs werden alle Antragsdatensätze für eine Frist von fünf Jahren gespeichert. Die Festsetzung einer angemessenen Frist ist eine politische Entscheidung des Gemeinschaftsgesetzgebers.

Es ist nicht nachzuweisen — insbesondere nicht im Lichte der in dem Kommentar zu den Artikeln genannten Gründe -, dass die politische Entscheidung, die für diesen Vorschlag getroffen wurde, unangemessen ist oder inakzeptable Folgen hätte, sofern alle adäquaten Korrekturmechanismen in Kraft treten. Das bedeutet, dass eine Korrektur oder eine Löschung von Daten gewährleistet sein muss, wenn die Daten nicht mehr exakt sind, insbesondere dann, wenn eine Person die Staatsangehörigkeit eines Mitgliedstaats oder einen Status erhalten hat, der ihre Erfassung im System nicht erfordert.

Darüber hinaus dürfen die Daten, solange sie sich noch im System befinden, keinesfalls eine neue Entscheidung präjudizieren. Einige Ablehnungsgründe (der Antragsteller ist zur Einreiseverweigerung ausgeschrieben, insbesondere Gefahr für die öffentliche Gesundheit) haben nur eine zeitlich begrenzte Gültigkeit. Die Tatsache, dass sie zu einem bestimmten Zeitpunkt triftige Gründe für eine Einreiseverweigerung waren, darf eine neue Entscheidung nicht beeinflussen. Die Situation muss für jeden neuen Visumantrag völlig neu bewertet werden und dies sollte aus der Verordnung an den entsprechenden Stellen explizit hervorgehen.

3.7. **Datenzugang und -verwendung**

3.7.1. *Vorbemerkungen*

Vorab räumt der EDPS ein, dass die Regelungen für den Zugang zu den VIS-Daten und ihre Verwendung offensichtlich mit großer Sorgfalt ausgearbeitet wurden. Jede Behörde hat Zugang zu verschiedenen Daten und zu verschiedenen Zwecken. Dies ist ein adäquater Ansatz, zu dem der EDPS nur ermutigen kann. Die nachfolgenden Bemerkungen stellen darauf ab, diesen Ansatz auch voll und ganz in die Praxis umzusetzen.

3.7.2. *Visakontrollen an den Außengrenzstellen und im Hoheitsgebiet der Mitgliedstaaten*

In Bezug auf die Visakontrollen an den Außengrenzen werden in Artikel 16 des Vorschlags eindeutig die beiden genauen Zweckbestimmungen genannt:

— „Überprüfung der Identität der Person", d.h. ein Eins-zu-Eins-Vergleich gemäß der bestehenden Definition;

— „Überprüfung der Echtheit des Visums". Entsprechend der ICAO-Normen könnte im Mikrochip des Visums ein PKI-System (*public/private key infrastructure)* zur Verwaltung dieses Authentisierungsprozesses verwendet werden.

Diesen beiden Zweckbestimmungen lässt sich durch den ausschließlichen Zugang der zuständigen Behörden zu dem geschützten Mikrochip zum Zwecke der Durchführung der Visakontrollen ordnungsgemäß Rechnung tragen. Ein Zugang zu der zentralen VIS-Datenbank wäre in diesem konkreten Fall hingegen unangemessen. Eine solche Option würde eine größere Zahl von mit dem VIS verbundenen Behörden bedeuten, was die Gefahr des Missbrauchs erhöhen würde. Sie dürfte auch kostspieliger sein, da die Zahl der gesicherten und überwachten VIS-Zugänge und damit verbunden der Bedarf an spezifischer Ausbildung ebenfalls zunehmen würde.

Im Übrigen bestehen Bedenken in Bezug auf die Angemessenheit des Datenzugangs, wie er in Artikel 16 Absatz 2 vorgesehen ist. So kann die zuständige Behörde nach Absatz 2 Buchstabe a in Fällen, in denen eine erste Suche ergibt, dass Daten über den Antragsteller im VIS gespeichert sind (was grundsätzlich der Fall sein sollte), ebenfalls zum Zwecke der Überprüfung der Identität der Person andere Daten abfragen. Diese Daten betreffen alle Informationen über den Antrag, Fotos, Fingerabdrücke sowie etwaige früher erteilte, für nichtig erklärte, widerrufene, zurückgenommene oder verlängerte Visa.

Verläuft eine Überprüfung erfolgreich, so ist keineswegs klar, aus welchen Gründen die restlichen Daten noch gebraucht werden. Sie sollten nämlich nur — unter restriktiven Bedingungen — zugänglich gemacht werden, wenn die Überprüfungsverfahren fehlgeschlagen sind. In diesem Fall wäre es angemessen, die in Artikel 16 Absatz 2 genannten Daten für ein Ausweichverfahren zu verwenden, das dazu beiträgt, die Identität der Person festzustellen. Die Daten sollten dann nicht dem gesamten Personal an den Grenzübergangsstellen zugänglich sein, sondern ausschließlich den mit schwierigen Aufgaben betrauten Beamten.

Schließlich sollten die Behörden, denen Zugang gewährt wird, genauer definiert werden. Insbesondere ist nicht klar, welches die „für Kontrollen an den Außengrenzen und im Hoheitsgebiet der Mitgliedstaaten zuständigen Behörden" sind. Der EDPS vermutet, dass es sich dabei um die für *Visa*kontrollen zuständigen Behörden handelt; Artikel 16 sollte daher in diesem Sinne geändert werden.

3.7.3. *Verwendung von Daten zur Identifizierung und Rückführung illegaler Einwanderer sowie für Asylverfahren*

In den Fällen, die in den Artikeln 17, 18 und 19 (Rückführung illegaler Einwanderer und Asylverfahren) beschrieben werden, wird das VIS zum Zwecke der Identifizierung in Anspruch genommen. Zu den Daten, die zum Zwecke der Identifizierung verwendet werden können, gehören Fotos. Nach dem derzeitigen Stand der Technologie der automatischen Gesichtserkennung für IT-Systeme derart großen Maßstabs können Fotos nicht zur Identifizierung verwendet werden („*one-to-many*"-Beziehung), da das Ergebnis nicht verlässlich ist. Sie sind daher als für die Zwecke der Identifizierung nicht adäquat zu betrachten.

Der EDPS schlägt infolgedessen nachdrücklich vor, dass die „Fotos" aus dem ersten Teil der genannten Artikel gestrichen und nur im zweiten Teil beibehalten werden (Fotos können durchaus als ein Instrument zur Überprüfung der Identität einer Person verwendet werden, nicht aber zur Identifizierung in einer Großdatenbank).

Eine andere Option würde darin bestehen, Artikel 36 dahin gehend zu ändern, dass die Funktionen für die Verarbeitung von Fotos zu Identifizierungszwecken nur greifen, wenn die betreffende Technologie als verlässlich betrachtet wird (möglicherweise nach Konsultation des technischen Ausschusses).

3.7.4. *Veröffentlichung der Listen der Behörden, die Zugang zum VIS haben*

Nach Artikel 4 des Vorschlags werden die Listen der in den einzelnen Mitgliedstaaten für den Zugang zum VIS benannten zuständigen Behörden im Amtsblatt der Europäischen Union veröffentlicht. Diese Veröffentlichung sollte regelmäßig (jährlich) erfolgen, um über Änderungen auf nationaler Ebene zu informieren. Der EDPS unterstreicht die Bedeutung dieser Veröffentlichung als ein unerlässliches Kontrollinstrument sowohl auf europäischer als auch auf nationaler bzw. lokaler Ebene.

3.8. **Verantwortlichkeiten**

An dieser Stelle sei daran erinnert, dass das VIS über eine zentralisierte Architektur mit einer zentralen Datenbank, in der alle Visa-Daten gespeichert werden, sowie über nationale Schnittstellen in den Mitgliedstaaten verfügen wird, die deren zuständigen Behörden den Zugang zum zentralen System ermöglichen. Gemäß den Erwägungsgründen 14 und 15 des Vorschlags findet die Richtlinie 95/46/EG Anwendung auf die gemäß der Verordnung erfolgende Verarbeitung personenbezogener Daten durch die Mitgliedstaaten und die Verordnung 45/2001 auf die Tätigkeiten der Kommission im Bereich des Schutzes personenbezogener Daten. Wie in diesem Zusammenhang in den genannten Erwägungsgründen erwähnt, zielt der Vorschlag darauf ab, bestimmte Punkte, u.a. im Hinblick auf die Verantwortung für die Verwendung der Daten und die Kontrolle des Datenschutzes, klarzustellen.

In der Tat dürften diese Punkte einige äußerst wichtige Details betreffen, ohne die das System von Schutzmaßnahmen gemäß der Richtlinie 95/46/EG und der Verordnung 45/2001 nicht greifen bzw. nicht voll im Einklang mit dem Vorschlag stehen würde. Die Anwendbarkeit nationaler Rechtsvorschriften gemäß der Richtlinie setzt normalerweise einen in dem betreffenden Mitgliedstaat niedergelassenen Verantwortlichen voraus (Artikel 4), während die Anwendbarkeit der Verordnung für die Verarbeitung personenbezogener Daten durch ein Organ oder eine Einrichtung der Gemeinschaft bei der Ausübung von Tätigkeiten greift, die ganz oder teilweise unter das Gemeinschaftsrecht fallen (Artikel 3).

Nach Artikel 23 Absatz 2 des Vorschlags werden die Daten „im VIS im Namen der Mitgliedstaaten verarbeitet". Nach Artikel 23 Absatz 3 benennen die Mitgliedstaaten die Behörde, die als Verantwortlicher gemäß Artikel 2 Buchstabe d der Richtlinie 95/46/EG betrachtet wird. Dies scheint darauf hinzudeuten, dass nach dem System der Richtlinie die Kommission als Auftragsverarbeiter betrachtet werden soll. Der Kommentar zu den Artikeln ([1]) bestätigt diese These.

Mit diesen Bezeichnungen wird die sehr umfangreiche und wirklich entscheidende Rolle, die der Kommission sowohl in der Entwicklungsphase als auch während des Normalbetriebs des Systems zukommt, unterbewertet. Es ist schwer, die Rolle der Kommission exakt dem Konzept des Verantwortlichen oder dem des Auftragsverarbeiters zuzuordnen; die Kommission ist entweder ein Auftragsverarbeiter mit außergewöhnlichen Befugnissen (u.a. bei der Entwicklung des Systems) oder ein eingeschränkt Verantwortlicher (da die Daten von den Mitgliedstaaten eingegeben und verwendet werden). Die Kommission nimmt im VIS in der Tat eine *sui generis*-Funktion ein ([2]).

Diese bedeutende Rolle sollte durch eine umfassende Beschreibung der Aufgaben der Kommission anerkannt werden, statt durch einen Wortlaut, der den Realitäten nicht ganz gerecht wird, weil er zu restriktiv ist, am VIS-Betrieb nichts ändert und nur Verwirrung stiftet. Dies ist auch wichtig im Hinblick auf eine konsequente und effiziente Kontrolle des VIS (siehe auch Nummer 3.11.). Der EDPS empfiehlt infolgedessen die Streichung des Artikels 23 Absatz 2.

Der EDPS betont, dass eine vollständige Beschreibung der Aufgaben der Kommission in Bezug auf das VIS umso wichtiger ist, als die Kommission erwägt, eine andere Stelle mit den Managementaufgaben zu betrauen. In dem „Finanzbogen", der dem Vorschlag beigefügt ist, wird die Möglichkeit erwähnt, diese Aufgaben der Grenzschutzagentur zu übertragen. Im Hinblick darauf ist es äußerst wichtig, dass die Kommission den Umfang ihrer Zuständigkeiten unmissverständlich festlegt, damit ihr Nachfolger weiß, innerhalb welcher Grenzen er tätig werden kann.

3.9. **Sicherheit**

Management und Wahrung eines optimalen VIS-Sicherheitsniveaus sind eine Voraussetzung dafür, den erforderlichen Schutz von in der VIS-Datenbank gespeicherten personenbezogenen Daten sicherzustellen. Um ein angemessenes Schutzniveau zu erreichen, müssen spezielle Schutzmaßnahmen für den Umgang mit den potenziellen Risiken vorgesehen werden, die mit der Infrastruktur des Systems und den beteiligten Personen verbunden sind. Dieses Problem wird in verschiedenen Teilen des Vorschlags erörtert; hier wären einige Verbesserungen angebracht.

In Artikel 25 und 26 des Vorschlags sind verschiedene Maßnahmen für die Datensicherheit vorgesehen; ferner sind die Arten des Missbrauchs aufgeführt, denen es vorzubeugen gilt. Diese Bestimmungen könnten jedoch sinnvoll durch Maßnahmen ergänzt werden, mit denen die Effizienz der bereits erwähnten Sicherheitsmaßnahmen überwacht und entsprechend Bericht erstattet wird. Konkret empfiehlt der EDPS, dass diesen Artikeln Bestimmungen über die (Eigen-)Kontrolle von Sicherheitsmaßnahmen hinzugefügt werden.

Hier besteht eine Verbindung zu Artikel 40 des Vorschlags, in dem die Überwachung und Bewertung vorgesehen sind. Dies sollte nicht nur die Ergebnisse, die Kostenwirksamkeit und die Qualität der Dienste betreffen, sondern auch die Einhaltung der rechtlichen Erfordernisse, insbesondere im Bereich des Datenschutzes. Der EDPS empfiehlt daher, dass der Anwendungsbereich von Artikel 40 auf die Überwachung der Rechtmäßigkeit der Verarbeitung und die entsprechende Berichterstattung ausgedehnt wird.

Darüber hinaus sei in Ergänzung zu Artikel 24 Absatz 4 Buchstabe c bzw. Artikel 26 Absatz 2 Buchstabe e betreffend die zum Zugang zu den Daten ermächtigten Bediensteten hinzugefügt, dass die Mitgliedstaaten sicherstellen sollten, dass genaue Nutzerprofile vorliegen (die den nationalen Kontrollstellen für Überprüfungen zur Verfügung stehen sollten). Zusätzlich zu diesen Nutzerprofilen müssen die Mitgliedstaaten eine vollständige Liste der Nutzeridentitäten erstellen und auf dem neuesten Stand halten. Dasselbe gilt für die Kommission: Artikel 25 Absatz 2 Buchstabe b sollte daher in diesem Sinne ergänzt werden.

([1]) siehe S. 40 des Vorschlags

([2]) obgleich die Definition des Verantwortlichen in der Richtlinie 95/46/EG und in der Verordnung 45/2001 auch die Möglichkeit mehrerer Verantwortlicher mit unterschiedlichen Verantwortlichkeiten vorsieht.

Diese Sicherheitsmaßnahmen werden durch Überwachungs- und organisatorische Schutzmaßnahmen vervollständigt. Artikel 28 des Vorschlags legt fest, unter welchen Bedingungen und zu welchen Zwecken Aufzeichnungen über alle Datenverarbeitungsvorgänge geführt werden müssen. Diese Aufzeichnungen werden nicht nur zur Überwachung des Datenschutzes und zur Gewährleistung der Datensicherheit gespeichert, sondern auch zur Durchführung regelmäßiger Eigenkontrollen des VIS. Die Berichte über die Eigenkontrollen werden zur effizienten Erledigung der Aufgaben der Kontrollstellen beitragen, die imstande sein werden, die Schwachstellen zu identifizieren und im Rahmen ihres eigenen Kontrollverfahrens konkret auf sie einzugehen.

3.10. **Rechte der von den Daten betroffenen Personen**

3.10.1. *Unterrichtung der betroffenen Personen*

Die Unterrichtung der von den Daten betroffenen Personen zur Sicherstellung einer Verarbeitung nach Treu und Glauben ist von größter Bedeutung. Sie stellt einen unerlässlichen Schutz der Rechte des Einzelnen dar. Artikel 30 des Vorschlags lehnt sich zu diesem Zweck im Wesentlichen an Artikel 10 der Richtlinie 95/46/EG an.

Dieser Bestimmung kämen allerdings einige Änderungen zugute, die es ermöglichen würden, sie besser an den Rahmen des VIS anzupassen. So sieht die Richtlinie in der Tat vor, dass bestimmte Informationen mitgeteilt werden; sie gestattet aber auch, dass ggf. mehr Informationen mitgeteilt werden ([1]). Infolgedessen sollte Artikel 30 zur Einbeziehung folgender Punkte geändert werden:

— Die betroffenen Personen sollten auch über die für ihre Daten geltende Speicherungsfrist unterrichtet werden.

— Artikel 30 Absatz 1 Buchstabe e betrifft „das Bestehen von Auskunfts- und Berichtigungsrechten" bezüglich der Daten. Exakter wäre die Formulierung „das Recht auf Zugang zu den Daten und das Recht auf *Beantragung einer* Berichtigung *oder einer Löschung* der Daten". Dabei sollten die betroffenen Personen über die Möglichkeit informiert werden, bei den zuständigen Kontrollstellen um Beratung oder Unterstützung nachzusuchen.

— Schließlich sieht Artikel 30 Absatz 1 Buchstabe a Informationen über die Identität des für die Verarbeitung Verantwortlichen und ggf. seines Vertreters vor. Da der Verantwortliche stets im Gebiet der Europäischen Union niedergelassen ist, besteht kein Bedarf für diese Bestimmung.

3.10.2. *Recht auf Zugang, Korrektur und Löschung*

In Artikel 31 Absatz 1 letzter Satz heißt es: „Diese Datenauskunft wird nur von einem Mitgliedstaat erteilt.". Dies bedeutet wohl, dass der Zugang zu den Daten (oder deren Übermittlung) nicht durch die Zentraleinheit gewährt werden kann, sondern nur durch einen Mitgliedstaat. Der EDPS empfiehlt, dass explizit zum Ausdruck gebracht wird, dass eine Übermittlung von Daten in jedem Mitgliedstaat beantragt werden kann.

Darüber hinaus beinhaltet der Wortlaut dieser Bestimmung offenbar auch, dass der Zugang nicht verweigert werden kann und dass er ohne die Genehmigung des verantwortlichen Mitgliedstaats gewährt wird. Dies würde erklären, warum die nationalen Behörden zusammenarbeiten müssen, um die Rechte nach Artikel 31 Absätze 2, 3 und 4 durchzusetzen, nicht aber die in Artikel 31 Absatz 1 ([2]).

3.10.3. *Unterstützung durch die Kontrollstellen*

Nach Artikel 33 Absatz 2 bestehen die Pflichten der nationalen Kontrollstellen zur Unterstützung und Beratung der betroffenen Person während des gesamten Verfahrens (vor einem Gericht). Die Bedeutung dieses Absatzes ist nicht klar. Die nationalen Kontrollstellen haben unterschiedliche Standpunkte in Bezug auf ihre Rolle im Rahmen von Gerichtsverfahren. Die Bestimmung könnte dahin gehend ausgelegt werden, dass die Kontrollstellen vor Gericht als Anwalt des Klägers aufzutreten haben, was jedoch in vielen Ländern nicht möglich ist.

([1]) In Artikel 10 heißt es: *„weitere Informationen (…), sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten*".

([2]) Infolgedessen könnte Artikel 31 Absatz 3 betreffend die Zusammenarbeit zwischen den nationalen Behörden bei der Ausübung des Rechts auf Korrektur bzw. Löschung im Interesse der Klarheit in diesem Sinne geändert werden: „Wird der Antrag *nach Artikel 31 Absatz 2* (…)". Die Anträge nach Artikel 31 Absatz 1 (Zugang) erfordern keine Zusammenarbeit zwischen den Behörden.

3.11. **Kontrolle**

Gemäß dem Vorschlag verteilen sich die Kontrollaufgaben auf die nationalen Kontrollstellen und den EDPS. Dies steht im Einklang mit dem Konzept, das in dem Vorschlag in Bezug auf das anwendbare Recht und die Verantwortlichkeiten für Betrieb und Verwendung des VIS verfolgt wird, sowie mit dem Erfordernis einer effizienten Kontrolle. Der EDPS begrüßt infolgedessen dieses Konzept in den Artikeln 34 und 35.

Die nationalen Kontrollstellen überwachen die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten, *einschließlich ihrer Übermittlung an das und von dem VIS*. Der EDPS überwacht die Tätigkeiten der Kommission, um sicherzustellen, *(...) dass die personenbezogenen Daten rechtmäßig zwischen den nationalen Schnittstellen und dem zentralen Visa-Informationssystem übermittelt werden*. Dies könnte zu Doppelarbeit führen, da die nationale Kontrollstelle und der EDPS zugleich verantwortlich sind für die Überwachung der Rechtmäßigkeit der Datenübermittlung zwischen den nationalen Schnittstellen und dem zentralen Visa-Informationssystem.

Infolgedessen schlägt der EDPS eine Änderung des Artikels 34 vor, um klarzustellen, dass die nationalen Kontrollstellen die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch den betreffenden Mitgliedstaat einschließlich der Übermittlung der Daten an das und von dem VIS überwachen.

Was die Kontrolle des VIS anbelangt, so sei ferner betont, dass die Kontrolltätigkeiten der nationalen Kontrollstellen und des EDPS bis zu einem gewissen Grad koordiniert werden sollten, damit ein ausreichendes Maß an Kohärenz und globaler Effizienz sichergestellt wird. In der Tat sind eine Harmonisierung in Bezug auf die Durchführung der Verordnung sowie die Ausarbeitung eines gemeinsamen Konzepts zur Lösung gemeinsamer Probleme unerlässlich. Zur Sicherheit sei im Übrigen angemerkt, wird das Sicherheitsniveau des VIS letzten Endes von dem Sicherheitsniveau seines schwächsten Glieds abhängen wird. Auch in dieser Hinsicht muss die Zusammenarbeit zwischen dem EDPS und den nationalen Behörden strukturiert und verbessert werden. Artikel 35 sollte daher eine entsprechende Bestimmung enthalten, wonach der EDPS mindestens einmal jährlich eine Sitzung mit allen nationalen Kontrollstellen einberuft.

3.12. **Durchführung**

Artikel 36 Absatz 2 des Vorschlags sieht Folgendes vor: „*Die erforderlichen Maßnahmen zur technischen Umsetzung der Funktionen nach Absatz 1 werden gemäß dem Verfahren nach Artikel 39 Absatz 2 angenommen.*". Artikel 39 betrifft einen Ausschuss zur Unterstützung der Kommission, der im Dezember 2001 eingesetzt ([1]) und bereits für verschiedene Rechtsakte herangezogen wurde.

Die technische Umsetzung der VIS-Funktionen (Interaktion zwischen den zuständigen Behörden sowie einheitliche Visagestaltung) hat in mehreren Punkten potenziell bedenkliche Auswirkungen auf den Datenschutz. So wirkt sich beispielsweise die Entscheidung für oder gegen die Einbeziehung eines Mikrochips in Visa auf die Art und Weise aus, wie die zentrale Datenbank genutzt wird; auch das für den Austausch biometrischer Daten verwendete Standardformat wird die betreffende Datenschutzpolitik beeinflussen bzw. für deren Gestaltung ausschlaggebend sein ([2]).

Diese Wahl der Technologien wird entscheidende Auswirkungen auf die eigentliche Umsetzung der Grundsätze der Zweckbindung und der Verhältnismäßigkeit haben und sollte daher überwacht werden. Aus diesem Grund sollten technologische Entscheidungen, die wesentliche Auswirkungen auf den Datenschutz haben, vorzugsweise im Wege einer Verordnung nach dem Mitentscheidungsverfahren getroffen werden. Nur dann kann die erforderliche politische Kontrolle gewährleistet werden. In allen anderen Fällen, bei denen mit Auswirkungen auf den Datenschutz zu rechnen ist, sollte der EDPS die Möglichkeit erhalten, den genannten Ausschuss bei seinen Entscheidungen zu beraten.

3.13. **Interoperabilität**

Die Interoperabilität ist eine wichtige und entscheidende Voraussetzung für die Effizienz von IT-Großsystemen wie dem VIS. Sie ermöglicht es, die Gesamtkosten konsequent zu senken und eine etwaige naturgemäße Redundanz heterogener Elemente aufzufangen. Die Interoperabilität kann ferner dem Ziel einer gemeinsamen Visumpolitik dienen, indem für alle Bestandteile dieser Politik dieselben Verfahrensstandards vorgesehen werden. Allerdings ist es äußerst wichtig, zwischen zwei verschiedenen Interoperabilitätsgraden zu unterscheiden:

— Die Interoperabilität zwischen den EU-Mitgliedstaaten ist in hohem Maße wünschenswert; so müssen die von den Behörden eines Mitgliedstaats übermittelten Visumanträge interoperabel mit denen sein, die von den Behörden eines anderen Mitgliedstaats übermittelt werden.

([1]) Verordnung (EG) Nr. 2424/2001 des Rates vom 6. Dezember 2001 über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II)

([2]) Der Vorschlag für eine Verordnung des Rates zur Änderung der Verordnung (EG) Nr. 1683/95 des Rates über eine einheitliche Visagestaltung vom September 2003 enthielt einen ähnlichen Artikel.

— Die Interoperabilität zwischen für unterschiedliche Zwecke konzipierten Systemen oder mit Drittstaatssystemen ist weitaus fragwürdiger.

Unter den Schutzmaßnahmen, die zur Zweckbindung des Systems und zur Vorbeugung eines „*function creep*“ (schleichende Ausweitung der Anwendung des Systems) zur Verfügung stehen, kann die Verwendung unterschiedlicher technologischer Standards einen Beitrag zu dieser Zweckbegrenzung leisten. Darüber hinaus sollte jede Form der Interaktion zwischen zwei verschiedenen Systemen eingehend dokumentiert werden. Die Interoperabilität darf keinesfalls dazu führen, dass eine Behörde, die nicht berechtigt ist, Zugang zu bestimmten Daten zu haben oder letztere zu verwenden, einen solchen Zugang über ein anderes Informationssystem erhalten kann.

In diesem Zusammenhang weist der EDPS auf die Erklärung des Rates vom 25. März 2004 zum Kampf gegen den Terrorismus hin, in der die Kommission ersucht wird, Vorschläge vorzulegen, um die Interoperabilität und die Synergieeffekte zwischen den Informationssystemen (SIS, VIS und Eurodac) zu verbessern.

Er weist ferner auf die laufende Debatte über die Frage hin, welche Stelle in Zukunft mit dem Management der verschiedenen Großsysteme betraut werden könnte (siehe auch Abschnitt 3.8.).

Der EDPS unterstreicht erneut, dass die Interoperabilität der Systeme nicht unter Verletzung des Grundsatzes der Zweckbindung umgesetzt werden darf und dass ihm alle einschlägigen Vorschläge unterbreitet werden sollten.

4. **FAZIT**

4.1. **Allgemeines**

1. Der EDPS erkennt an, dass die weitere Entwicklung einer gemeinsamen Visumpolitik einen effizienten Austausch relevanter Daten erfordert. Einer der Mechanismen, die einen reibungslosen Informationsfluss gewährleisten können, ist das VIS. Der EDPS hat den in der ausführlichen Folgenabschätzung enthaltenen Nachweis mit Sorgfalt zur Kenntnis genommen. Obgleich dieser nicht ganz schlüssig ist, dürften doch ausreichende Gründe vorliegen, die den Aufbau des VIS zum Zwecke der Verbesserung der gemeinsamen Visumpolitik rechtfertigen.

   Allerdings sollte dieses neue Instrument auf die Erhebung und den Austausch von Daten begrenzt werden, soweit diese für die Entwicklung einer gemeinsamen Visumpolitik erforderlich sind und in einem angemessenen Verhältnis zu dem genannten Ziel stehen.

2. Der Aufbau des VIS kann positive Auswirkungen auf andere berechtigte öffentliche Interessen haben; dies ändert jedoch nichts am Zweck des VIS. Alle Elemente des VIS müssen daher notwendige und angemessene Instrumente zur Erreichung des oben genannten politischen Ziels sein. Im Übrigen

   — stünde ein Routinezugang der Strafverfolgungsbehörden nicht im Einklang mit diesem Zweck;

   — empfiehlt der EDPS, dass diese Unterscheidung zwischen „Zweck“ und „Vorteilen“ im Wortlaut des Artikels 1 Absatz 2 expliziter zum Ausdruck kommt;

   — darf die Interoperabilität mit anderen Systemen nicht unter Verletzung des Grundsatzes der Zweckbindung umgesetzt werden.

3. Der EDPS erkennt die Vorteile einer Nutzung biometrischer Daten an, betont jedoch die umfangreichen Auswirkungen, die eine Verwendung solcher Daten nach sich zieht, und schlägt die Aufnahme strikter Schutzmaßnahmen für die Verwendung biometrischer Daten vor. Außerdem ist es aufgrund der technischen Mängel bei Fingerabdrücken notwendig, Ausweichverfahren zu entwickeln und in den Vorschlag einzubeziehen.

4. Auf diese Stellungnahme sollte in der Präambel der Verordnung vor den Erwägungsgründen Bezug genommen werden („gestützt auf die Stellungnahme ...“).

4.2. **Sonstiges**

5. Gründe für eine Ablehnung der Visumerteilung: In den Text des Vorschlags sollte eine Bezugnahme auf Artikel 29 der Richtlinie 2004/58/EG aufgenommen werden, um sicherzustellen, dass das Kriterium der „Gefahr für die öffentliche Gesundheit" im Lichte dieser Bestimmung ausgelegt wird.

6. Daten über Gruppenmitglieder haben in dem Vorschlag eine besondere Bedeutung: daher ist eine präzise und umfassende Definition des Begriffs „Gruppenmitglieder" erforderlich.

7. Es ist nicht nachzuweisen, dass die in diesem Vorschlag getroffene politische Entscheidung über die Frist für die Datenspeicherung unangemessen ist oder inakzeptable Folgen hätte, sofern alle adäquaten Korrekturmechanismen vorgesehen werden.

   Darüber hinaus sollte aus dem Vorschlag explizit hervorgehen, dass personenbezogene Daten bei jedem neuen Visumantrag völlig neu bewertet werden müssen.

8. Visakontrollen an den Außengrenzen: Artikel 16 des Vorschlags sollte geändert werden, da ein Zugang zu der zentralen VIS-Datenbank hier unangemessen wäre. Ein ausschließlicher Zugang der zuständigen Behörden zu dem geschützten Mikrochip zum Zwecke der Durchführung der Visakontrollen reicht aus.

   Im Übrigen ist für den Fall, dass eine Identitätsüberprüfung erfolgreich verläuft, nicht klar, aus welchen Gründen die restlichen Daten noch gebraucht werden.

9. Verwendung von Daten für die Identifizierung und Rückführung illegaler Einwanderer sowie für Asylverfahren: „Fotos" sollten aus dem ersten Teil der Artikel 17, 18 und 19 gestrichen und im zweiten Teil beibehalten werden.

10. Verantwortlichkeiten der Kommission und der Mitgliedstaaten: Artikel 23 Absatz 2 sollte gestrichen werden.

11. Bestimmungen über die systematische (Eigen-)Kontrolle von Sicherheitsmaßnahmen sollten in den Vorschlag aufgenommen werden. Der Anwendungsbereich des Artikels 40 muss auf die Überwachung der Rechtmäßigkeit der Verarbeitung und die entsprechende Berichterstattung ausgeweitet werden. Im Übrigen

   — sollten die Mitgliedstaaten eine vollständige Liste der Nutzeridentitäten erstellen und auf dem neuesten Stand halten. Dasselbe gilt für die Kommission: Artikel 25 Absatz 2 Buchstabe b sollte in diesem Sinne ergänzt werden;

   — legt Artikel 28 des Vorschlags fest, unter welchen Bedingungen und zu welchen Zwecken Aufzeichnungen über alle Datenverarbeitungsvorgänge geführt werden müssen. Diese Aufzeichnungen werden nicht nur zur Überwachung des Datenschutzes und zur Gewährleistung der Datensicherheit gespeichert, sondern auch zur Durchführung regelmäßiger Eigenkontrollen des VIS.

12. Rechte der von den Daten betroffenen Personen:

   — Artikel 30 sollte geändert werden, um sicherzustellen, dass die betroffenen Personen auch über die für ihre Daten geltende Speicherungsfrist unterrichtet werden.

   — In Artikel 30 Absatz 1 Buchstabe e sollte auf „das Recht auf Zugang zu den Daten und das Recht auf Beantragung einer Berichtigung oder einer Löschung der Daten" Bezug genommen werden.

   — In Artikel 31 Absatz 1 muss explizit zum Ausdruck gebracht werden, dass die Übermittlung bestimmter Daten in jedem Mitgliedstaat beantragt werden kann.

13. Kontrolle:

— Artikel 34 sollte geändert werden, um klarzustellen, dass die nationalen Kontrollstellen die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch den betreffenden Mitgliedstaat einschließlich der Übermittlung der Daten an die nationale Schnittstelle des VIS und von dieser überwachen.

— Artikel 35 sollte daher eine Bestimmung enthalten, wonach der EDPS mindestens einmal jährlich eine Sitzung mit allen nationalen Kontrollstellen einberuft.

14. Durchführung:

— Technologische Entscheidungen, die wesentliche Auswirkungen auf den Datenschutz haben, sollten vorzugsweise im Wege einer Verordnung nach dem Mitentscheidungsverfahren getroffen werden.

— In anderen Fällen sollte der EDPS die Möglichkeit erhalten, den in dem Vorschlag vorgesehenen Ausschuss bei seinen Entscheidungen zu beraten.

Geschehen zu Brüssel am 23. März 2005

Peter HUSTINX

Der Europäische Datenschutzbeauftragte