ARTIKEL-29-Datenschutzgruppe

1022 /05/DE
WP 110

Stellungnahme 2/2005

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

Angenommen am 23. Juni 2005

Inhaltsverzeichnis

Stellungnahme 2/2005
zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (KOM (2004) 835 endg.)

DIE GRUPPE FÜR DEN SCHUTZ NATÜRLICHER PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1] ,

gestützt auf Artikel 29 sowie Artikel 30 Absatz 1 Buchstabe c und Absatz 3 der Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere Artikel 12 und 14,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Einführung

1.1. Umfang und Auswirkung des Vorhabens

Die geplante Errichtung einer zentralen Datenbank und eines Systems zum Informationsaustausch über Visa für einen kurzfristigen Aufenthalt wirft wichtige Fragen im Zusammenhang mit dem Schutz der Grundrechte und Grundfreiheiten von Personen und insbesondere ihrem Recht auf Privatsphäre auf.

Sie wird dazu führen, dass große Mengen personenbezogener und biometrischer Daten erfasst, verarbeitet und in einer zentralen Datenbank gespeichert und dass umfangreiche Informationen über sehr viele Personen ausgetauscht werden.

Die Datenschutzbehörden sind vor allem über die potenziellen Risiken eines solchen Vorhabens besorgt und weisen nachdrücklich darauf hin, dass die Beachtung der Grundsätze des Datenschutzes sichergestellt sein muss.

Die Frage der Notwendigkeit und der Verhältnismäßigkeit einer so umfangreichen Datenbank wurde bereits wiederholt in der Öffentlichkeit diskutiert, insbesondere im Hinblick auf die Aufnahme biometrischer Daten in das System.

1.2. Hintergrund des Vorschlags

Die Einrichtung des Visa-Informationssystems (VIS) zum Austausch von Visa-Daten zwischen Mitgliedstaaten gehört zu den Schlüsselelementen einer gemeinsamen Visapolitik zur Verwirklichung der Ziele des Artikels 61 EG-Vertrag, nämlich der Gewährleistung des

[1] ABl. L 281 vom 23.11.1995, S. 31, verfügbar unter: http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_de.htm.

freien Personenverkehrs in einem Raum der Freiheit, der Sicherheit und des Rechts. Die Kommission hat sich bei ihrer Tätigkeit an den Leitlinien des Rates Justiz und Inneres vom 19. Februar 2004[2] orientiert. In seinen Schlussfolgerungen hat der Rat die Kommission insbesondere ersucht, bei der Vorbereitung der technischen Implementierung des VIS und des Vorschlags für den Rechtsakt zur Errichtung des VIS den Rechtsvorschriften der Gemeinschaft über den Schutz personenbezogener Daten in vollem Umfang Rechnung zu tragen.

Die Entscheidung 2004/512/EG des Rates vom 8. Juni 2004[3] liefert die Rechtsgrundlage für die Einrichtung des Visa-Informationssystems und die Einplanung der für die technische Entwicklung des Systems erforderlichen Finanzmittel im Gesamthaushalt der Gemeinschaft.

Am 28. Dezember 2004 hat die Kommission den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt vorgelegt.[4]

Mit dieser Verordnung soll die Kommission zur Einrichtung und zum Betrieb des VIS ermächtigt werden, sollen Zweck und Funktionalitäten des VIS sowie die entsprechenden Zuständigkeiten festgelegt und die Verfahren und Bedingungen für den Datenaustausch zwischen Mitgliedstaaten definiert werden.

Wie in der Begründung des Vorschlags ausgeführt, erfordert die Entwicklung und Einrichtung des VIS einen umfassenden rechtlichen Rahmen, darunter insbesondere

- die Änderung der gemeinsamen konsularischen Instruktion (GKI)[5] an die diplomatischen Missionen und die konsularischen Vertretungen der Vertragsparteien der Schengener Übereinkommen,
- die Entwicklung eines Verfahrens für den Datenaustausch mit Irland und dem Vereinigten Königreich (die nicht am Schengen-System teilnehmen), um die Anwendung der Verordnung "Dublin II" zu erleichtern und die Identifizierung illegaler Einwanderer und deren Rückführung zu unterstützen;
- den Datenaustausch über Visa für einen längerfristigen Aufenthalt im Sinne von Artikel 63 EG-Vertrag, der zurzeit nicht Gegenstand der gemeinsamen Visapolitik ist.[6]

Die Verwirklichung des Ziels des freien Personenverkehrs in der gesamten Europäischen Union wird noch weitere Maßnahmen erfordern, darunter die Abschaffung der Kontrollen an den Binnengrenzen und die Verstärkung der Kontrollen an den Außengrenzen. Entsprechende Maßnahmen finden sich in einem Vorschlag für eine Verordnung über den Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen.[7]

---

[2] Ratsdokument 6535/04 VISA 33 COMIX 111

[3] Entscheidung des Rates vom 8. Juni 2004 zur Einrichtung des Visa-Informationssystems (VIS) (2004/512/EG)- ABl. L 213, 15.6.04, S. 5.

[4] Dokument KOM(2004)835-endg., noch nicht im Amtsblatt der Europäischen Union veröffentlicht.

[5] Gemeinsame konsularische Instruktion an die diplomatischen Missionen und die konsularischen Vertretungen, die von Berufskonsularbeamten geleitet werden, ABl C 310, 19.12.03, S.1.

[6] Die gemeinsame Visapolitik der Mitgliedstaaten, die ihre Binnengrenzen zu den beteiligten Ländern abgeschafft und die Freizügigkeit dort verwirklicht haben, richtet sich nach Artikel 62 EG-Vertrag und findet nur Anwendung bei Visa für einen kurzfristigen Aufenthalt (d.h. für höchstens drei Monate); diese Visa werden auf der Grundlage gemeinsamer Regelungen und in einheitlicher Gestaltung (so genannte einheitliche Visa oder Schengen-Visa) ausgestellt.

[7] KOM (2004) 0391 vom 26.05.2004, das die entsprechenden Bestimmungen des Schengener Übereinkommens ersetzen wird. Das Dokument wurde der Arbeitsgruppe nicht zur Stellungnahme vorgelegt.

Es erscheint des Weiteren angebracht, die laufenden Aktivitäten zur Entwicklung des neuen Schengener Informationssystems (SIS II) zu erwähnen. Am 31. Mai hat die Kommission Vorschläge für einen Beschluss und eine Verordnung vorgelegt, die auf Änderungen der Bestimmungen des Schengener Übereinkommens im Hinblick auf das SIS abzielen. Neben der Einführung neuer Funktionen und neuer Datenkategorien sollen auch Anzahl und Kategorien der zugriffsberechtigten Behörden erweitert werden.[8] Zurzeit haben die "Visumbehörden" Zugriff auf das SIS, insbesondere auf die Daten zu Drittstaatsangehörigen, die gemäß Artikel 96 des Übereinkommens zur Einreiseverweigerung ausgeschrieben sind.

Sodann sieht ein Vorschlag der Kommission vom Dezember 2003 für eine – noch nicht vom Rat verabschiedete – Verordnung vor, dass im Rahmen der einheitlichen Gestaltung von Visa (und Aufenthaltstiteln) zwei biometrische Merkmale aufzunehmen sind: ein digitales Lichtbild und digitale Bilder von zwei Fingerabdrücken des Inhabers, beides auf einem Mikrochip gespeichert.[9] Diese Bestimmung scheint die Aufnahme der genannten Daten in das Visa-Informationssystem zu beinhalten und ist insbesondere im Hinblick auf die in Artikel 16 des Vorschlags erwähnte Verwendung der Daten für Grenzkontrollen von Bedeutung.

Das VIS soll aus einer zentralen Struktur und nationalen Schnittstellen bestehen, ergänzt durch die Einrichtung entsprechender Systeme einschließlich fester Computerverbindungen zu Konsulaten und Grenzkontrollpunkten auf nationaler Ebene; es wird neben alphanumerischen Daten zu den Antragstellern auf Erteilung eines (einheitlichen) Visums für einen kurzfristigen Aufenthalt auch biometrische Daten enthalten, insbesondere die bei der Antragstellung abgenommenen Fingerabdrücke der betreffenden Person.

Ursprünglich war die Einrichtung und der Betrieb des VIS in zwei Abschnitten vorgesehen: zunächst sollten die Funktionen für alphanumerische Daten eingerichtet werden, und danach die Funktionen für die Verarbeitung biometrischer Daten.

Laut den Schlussfolgerungen des Rates Justiz und Inneres vom 19. Februar 2004 sollen später - im Einklang mit der Wahl der biometrischen Identifikationsmerkmale im Visabereich und unter Berücksichtigung der Ergebnisse der gegenwärtigen technischen Entwicklungen - biometrische Daten über die Visumantragsteller in das VIS aufgenommen werden.

Unter Berücksichtigung der technischen Probleme bei der Aufnahme biometrischer Daten in die Visa, die zur Verzögerung der Annahme der Verordnung geführt haben, hat der Rat im Februar 2005 die Kommission ersucht, "nach besten Kräften - auch auf der Ebene der Haushaltsplanung - dafür zu sorgen, dass der Einsatz der Biometrie beim Aufbau des zentralen Teils des Visa-Informationssystems (VIS) auf das Jahr 2006 vorgezogen wird."[10] Es ist darauf hinzuweisen, dass dies keinerlei Verpflichtung für die Kommission begründet und somit auch nicht die Notwendigkeit einer Änderung von Artikel 36 Absatz 2 des Vorschlags beinhaltet.
Vor dem Hintergrund des vom Rat verfolgten Ansatzes und auch, um die Konsistenz bei der Einführung biometrischer Daten in das Visa-Informationssystems sicherzustellen, ist eine geeignete Rechtsgrundlage für die Verpflichtung zur Bereitstellung dieser Daten erforderlich.

---

[8] Vorschlag für einen Beschluss des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) [KOM (2005) 230 endg.]; sowie Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) [KOM (2005) 236 endg.].

[9] Entwurf für eine Verordnung des Rates zur Änderung der Verordnungen 1683/95 und 1030/2002 des Rates über eine einheitliche Visagestaltung beziehungsweise die einheitliche Gestaltung des Aufenthaltstitels für Drittstaatenangehörige (KOM (2003) 558 endg., 24.9.2003).

[10] Entwurf der Schlussfolgerungen des Rates gemäß Dokument 6492/05 vom 17. Februar 2005.

Dazu plant die Kommission eine weitere spezifische Maßnahme in Form eines Verordnungsentwurfs zur Anpassung der GKI. Wie in der Begründung dargelegt, wird dieses neue Instrument insbesondere die "Normen und Verfahren zur Erfassung biometrischer Daten einschließlich der Pflicht und der Ausnahmen zur Speicherung biometrischer Merkmale" betreffen.

Die Einführung dieser neuen Pflicht ergänzt die Anforderungen des Verordnungsentwurfs zum VIS; deshalb ist davon auszugehen, dass die Hinweise im vorliegenden Vorschlag auf Aufnahme und Verwendung von biometrischen Daten vom Inkrafttreten und der effektiven Umsetzung der entsprechenden Pflichten der Mitgliedstaaten gemäß Annahme der Verordnung zur Anpassung der GKI abhängig sind.

1.3. Beschreibung des Vorschlags

Das Visa-Informationssystem zielt auf den Austausch von Visa-Daten zwischen den Mitgliedstaaten ab, "die die Kontrollen an ihren Binnengrenzen eingestellt haben" und "an der Regelung der Freizügigkeit ohne Kontrollen an den Binnengrenzen" teilnehmen; die entsprechende Rechtsgrundlage findet sich in Artikel 62 Absatz 2 Buchstabe b Ziffer ii und Artikel 66 EG-Vertrag.

Der Vorschlag ist als Maßnahme zur Förderung der gemeinsamen Visapolitik und somit als Weiterentwicklung des Schengen-Besitzstands spezifiziert.

Der Vorschlag enthält detaillierte Bestimmungen zum System und seinem Betrieb, zu den einzutragenden Datenkategorien, zu den Behörden, die Daten eintragen und auf sie zugreifen können, zu den Speicherfristen, zum Recht der Betroffenen auf Zugang, Aktualisierung und Löschung der Daten, zu den zu ergreifenden Sicherheitsvorkehrungen sowie zur Überwachung auf unionsweiter und nationaler Ebene.

Im Einklang mit der Entscheidung des Rates folgt das VIS strukturell dem Konzept der zentralisierten Systemarchitektur, die aus folgenden Komponenten besteht: einem zentralen Visa-Informationssystem (*Central Visa Information System* CS-VIS), das die in den Artikeln 5 bis 12 des Verordnungsentwurfs festgelegten Informationen enthält, einer nationalen Schnittstelle in jedem Mitgliedstaat (*National Interface* NI-VIS), die die Verbindung zu der betreffenden zentralen nationalen Behörde des jeweiligen Mitgliedstaats herstellt, und der Kommunikationsinfrastruktur zwischen dem CS-VIS und den nationalen Schnittstellen. Die Entwicklung des VIS basiert auf einer gemeinsamen technischen Plattform mit dem Schengener Informationssystem der zweiten Generation ("SIS II").[11]

Auch die Synergieeffekte mit dem Schengener Informationssystem werden in der Entscheidung des Rates betont, derzufolge die Kommission bei der Ausübung der ihr übertragenen Durchführungsbefugnisse von dem gemäß Artikel 5 Absatz 1 der Verordnung (EG) Nr. 2424/2001 des Rates vom 6. Dezember 2001 eingerichteten Ausschuss SIS II unterstützt wird.

Entsprechend dem Finanzierungsplan des Vorschlags ist die Kommission für Einrichtung, Wartung und Betrieb des zentralen Visa-Informationssystems sowie für die Kommunikationsinfrastruktur zwischen dem zentralen System und den nationalen Schnittstellen zuständig. Erfassung und Verarbeitung der Daten im VIS fällt in die

[11] Dieses soll gegenüber dem gegenwärtigen SIS zusätzliche Funktionen und Datenkategorien enthalten und unter Verweis auf den neuen Vorschlag für eine Verordnung zu SIS II auch die nach der Erweiterung hinzugekommenen neuen Mitgliedstaaten einbeziehen. Siehe auch Fußnote Nr. 8.

Zuständigkeit der Mitgliedstaaten. Die Kommission übernimmt die Verantwortung für das "technische" Management des Systems.

Die Systemkapazität soll - insbesondere im Hinblick auf biometrische Daten - so ausgelegt werden, dass das VIS ab 2007 jährlich ca. 20 Millionen Daten zu Visumanträgen enthalten kann. Das hieße, dass während der im Vorschlag genannten fünfjährigen Speicherfrist 70 Millionen Fingerabdrücke im System gespeichert wären – zur Ermittlung dieser Zahl wurden für "Vielreisende" bereits 30 % von der Gesamtsumme abgezogen.

Die Berechnung (und Verteilung) der Kosten für die Gewährleistung des Betriebs erfolgt auf der Grundlage des genannten Finanzplans: Für den Zeitraum 2007-2013 sind 153 Mio. EUR veranschlagt, davon entfallen mehr als 70 % auf die Verarbeitung der biometrischen Daten.

Zu diesen Zahlen müssten noch die Kosten addiert werden, die auf die nationalen Stellen entfallen. Gemäß Artikel 2 Absatz 2 der Entscheidung 2004/512 EG des Rates sind die Mitgliedstaaten für die Anpassung oder Entwicklung der nationalen Infrastruktur hinter den nationalen Schnittstellen zuständig. Sie tragen auch die Kosten für die Entwicklung der Infrastruktur und die Anpassung der bestehenden nationalen Systeme an das VIS, für die weltweiten Verbindungen zu den konsularischen Vertretungen (einschließlich der in Artikel 16 des Vorschlags genannten Grenz- und sonstigen Kontrollstellen) sowie für Ausrüstung, Versand und Schulung.

1.4. Die vorausgehende Stellungnahme der Arbeitsgruppe

In ihrer Stellungnahme zur Aufnahme biometrischer Merkmale in Visa und Aufenthaltstitel unter Berücksichtigung des Aufbaus des Visa-Informationssystems VIS[12] hat die Datenschutzgruppe auf die Grundsätze zum Betrieb einer Datenbank dieser Art verwiesen, um der Kommission und dem Beratenden Ausschuss SIS II im Hinblick auf ihr weiteres Vorgehen hilfreiche Leitlinien an die Hand zu geben.

Die Kommission hat die Datenschutzgruppe formell um eine Stellungnahme zu ihrem Vorschlag für eine Verordnung ersucht.

Der Verordnungsentwurf enthält eine Reihe von Bestimmungen zu den Datenschutzgrundsätzen.

Im Hinblick auf einige grundlegende Aspekte des VIS besteht jedoch noch weiterer Raum für Verbesserungen; zu nennen sind hier die genaue Definition des Zwecks des Systems und der für die Datenverarbeitung verantwortlichen Organe, die Verhältnismäßigkeit der zu erhebenden Daten und die Speicherfristen, die Anwendung des Transparenzgrundsatzes und die genauere Spezifikation der Überwachungs- und Kontrollaufgaben auf zentraler wie auf nationaler Ebene. Hierzu werden in den folgenden Abschnitten gezielte Überlegungen angestellt.

2. Analyse des Vorschlags

Auf der Grundlage der zum Teil bereits angeführten Überlegungen vertritt die Datenschutzgruppe die Auffassung, dass die Bedeutung und besondere Komplexität des Themas eine ausführliche Stellungnahme erfordern, zur weiteren Ergänzung der Überlegungen, die in der bereits erwähnten Stellungnahme Nr. 7/2004 angesprochen wurden.

[12] Stellungnahme Nr. 7/2004 WP96 vom 11.08.2004, verfügbar unter: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp96_en.pdf

2.1. Allgemeine Überlegungen

Diese Initiative wird erhebliche Auswirkungen auf die Grundrechte einer großen und rasch steigenden Zahl von Personen haben, da alle in Artikel 2 aufgelisteten Anträge auf ein Visum für einen kurzfristigen Aufenthalt in Staaten, die am VIS teilnehmen, in diesem System erfasst werden müssen. Zudem sind Verknüpfungen vorgesehen mit den im VIS gespeicherten Visumanträgen, die der Betreffende möglicherweise zu einem früheren Zeitpunkt gestellt hat, sowie mit den Daten der Personen, die mit dem Betreffenden in einer Gruppe reisen, und der Personen, die dem Antragsteller Unterkunft in den EU-Ländern mit Visumpflicht gewähren.

Neben alphanumerischen Daten zu jedem Antrag soll das System eine Vielzahl weiterer Informationen enthalten, insbesondere auch zu den Fotos des Antragstellers und zu seinen Fingerabdrücken.

Mit der Möglichkeit der Speicherung von 70 Millionen personenbezogenen Datensätzen für einen Zeitraum von fünf Jahren ist dieses System im Hinblick auf Umfang und Kapazität derzeit unionsweit konkurrenzlos.

Weit reichende Mechanismen sind auch für den Zugang zum System sowie zum Kreis der zugriffsberechtigten Behörden vorgesehen, auch wenn im Verordnungsentwurf der Versuch unternommen wird, diesen Kreis zu begrenzen.

Ein weiterer Aspekt, der zur Ausweitung der Zugangsmöglichkeiten und damit zur Verwendung des Systems für unterschiedliche Zwecke führen könnte, hängt mit dem Ziel zusammen, die "Interoperabilität der europäischen Datenbanken" zu verstärken und Synergien zwischen SIS II, VIS und Eurodac zu schaffen. Der Verordnungsentwurf enthält keine präzisen Bestimmungen für die Erhebung der im VIS zu erfassenden personenbezogenen Daten. Gemäß Artikel 3 sind die folgenden Datenkategorien zur Speicherung im VIS vorgesehen: alphanumerische Daten über den Antragsteller und über Visa, Fotos, Fingerabdruckdaten und Verknüpfungen zu anderen Anträgen.

Gemäß den in der Richtlinie festgeschriebenen Grundsätzen dürfen Erhebung und Eingabe personenbezogener Daten nur durch die Behörden und nur zu den im Rechtsakt zur Einrichtung des VIS genannten Zwecken erfolgen; der vorliegende Vorschlag sollte hierzu präzise Bestimmungen enthalten, die den Umfang der Einschränkungen der Rechte und Freiheiten des Einzelnen, insbesondere des Rechts auf den Schutz der personenbezogenen Daten festlegen.

a) Das Kriterium der Notwendigkeit

Die Verarbeitung der Daten muss mit den Grundsätzen des Datenschutzes in Einklang stehen, die in Artikel 8 der Charta der Grundrechte der Europäischen Union verankert sind und auf die die Richtlinie 95/46/EG und die einzelstaatlichen Gesetze Bezug nehmen. Die Europäische Menschenrechtskonvention gibt – zum Teil auch im Licht der einschlägigen Gerichtsurteile des Europäischen Gerichtshofes für Menschenrechte – wichtige Leitlinien vor, um die Begrenzung von Eingriffen in die Privatsphäre von Einzelpersonen durch dazu befugte Behörden klarzustellen. Das in Artikel 8 festgeschriebene "Recht auf Achtung des Privat- und Familienlebens" muss gewährleistet sein. Gemäß Artikel 8 Absatz 2 EMRK ist ein Eingriff in die Ausübung dieses Rechts seitens einer öffentlichen Behörde nur statthaft, wenn er gesetzlich vorgesehen und in einer demokratischen Gesellschaft zum Schutz wichtiger öffentlicher Interessen notwendig ist.

Der Europäische Gerichtshof hat klargestellt, dass diese Kriterien zur Beurteilung der Frage heranzuziehen sind, ob die Verarbeitung personenbezogener Daten in Einklang mit dem Gemeinschaftsrecht steht.[13]

Für einen zulässigen Eingriff muss eine geeignete Rechtsgrundlage existieren, die ihrerseits wiederum bestimmten Qualitätsanforderungen genügen muss. Um Willkür auszuschließen, sind die Modalitäten für die Ausübung der den Behörden übertragenen Befugnisse klar zu definieren, und die Regeln müssen leicht zugänglich sein, um dem Einzelnen ein entsprechendes Verhalten zu ermöglichen.

Es muss ein "*zwingendes gesellschaftliches Bedürfnis*" vorliegen; es reicht nicht aus, dass einige Systemfunktionen lediglich "nützlich" sind, sie müssen wirklich notwendig sein – d.h. ohne diese Funktionen können die Zielsetzungen nicht erreicht werden.

Darüber hinaus muss die Maßnahme "in einem angemessenen Verhältnis zu dem verfolgten berechtigten Zweck stehen".

Die Erfüllung dieser Bedingungen ist für den vorliegenden Fall außerordentlich wichtig, deshalb sollte der Vorschlag keine vagen oder sehr weit gefassten Konzepte enthalten.

Aus diesem Grund ist es notwendig, das Ziel des Verordnungsentwurfs zu spezifizieren und die Verhältnismäßigkeit der im System zu erfassenden Daten im Hinblick auf dieses Ziel zu prüfen.

Es muss der gesamte Prozess der Datenverarbeitung berücksichtigt werden; dazu gehören alle geplanten Funktionen der in Rede stehenden Datenbank. Im Einzelnen ist für jede Funktion zu prüfen, ob die Verarbeitungsmechanismen, die Kategorien der zu erhebenden und zu verarbeitenden Daten, die zugangsberechtigten Behörden und die Sicherheitsvorkehrungen vor dem Hintergrund eines "zwingenden gesellschaftlichen Bedürfnisses" tatsächlich notwendig und unerlässlich sind; sodann sind die den Betroffenen zu gewährenden Rechte zu prüfen und es muss sichergestellt werden, dass ein angemessener Mechanismus zur Wahrnehmung dieser Rechte vorhanden ist.

b) Rechtsgrundlage

Es sollte klargestellt werden, ob die Pflicht zur Erteilung dieser Informationen nicht auf einem zusätzlichen spezifischen und detaillierten Rechtsinstrument basieren muss oder ob der Vorschlag selbst als angemessener rechtlicher Rahmen angesehen werden kann. Die Kommission scheint letztere Auffassung zu vertreten, da sie einen Vorschlag zur Änderung der Gemeinsamen Konsularischen Instruktion insbesondere im Hinblick auf bestimmte Standards und Verfahren zur "Erhebung personenbezogener Daten" ankündigt. Die Klarstellung wird zum einen den Prozess der Beschlussfassung zum Vorschlag stärken und

[13] Urteil des Gerichtshofes vom 20. Mai 2003 in den verbundenen Rechtssachen C-465/00, C-138/01 und C-139/01 (Rechnungshof), insbesondere Randnummern 72 und 83:
72 Für die Anwendung der Richtlinie 95/46 und insbesondere der Artikel 6 Absatz 1 Buchstabe c, 7 Buchstaben c und e und 13 ist daher zunächst zu prüfen, ob eine Regelung wie die den Ausgangsverfahren zugrunde liegende einen Eingriff in die Privatsphäre darstellt und gegebenenfalls ob ein solcher Eingriff nach Artikel 8 EMRK gerechtfertigt ist.
83 Nach der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte bedeutet das Eigenschaftswort notwendig in Artikel 8 Absatz 2 EMRK, dass ein zwingendes gesellschaftliches Bedürfnis bestehen und die Maßnahme in einem angemessenen Verhältnis zu dem verfolgten berechtigten Zweck stehen muss (vgl. u. a. EGMR, Urteil Gillow/Vereinigtes Königreich vom 24. November 1986, Série A, Nr. 109, § 55). Die nationalen Behörden verfügen zudem über ein Ermessen, dessen Umfang nicht nur von der Zielsetzung, sondern auch vom Wesen des Eingriffs abhängig ist (vgl. EGMR, Urteil Leander/Schweden vom 26. März 1987, Série A, Nr. 116, § 59).

zum anderen die Prüfung ermöglichen, inwieweit die Grundsätze der Zweckbestimmung und der Verhältnismäßigkeit erfüllt sind.

Auf diese Weise lässt sich deutlich machen, wie der Vorschlag mit den anderen von der Kommission vorgelegten und derzeit im Rat diskutierten Verordnungsentwürfen zusammenhängt und ob er mit diesen kohärent ist.

Vor dem Hintergrund der Entscheidung des Rates, biometrische Daten in das VIS aufzunehmen, sollten auch zum bestehenden Rechtsrahmen im Schengengebiet weitere konkrete Überlegungen zur Erteilung von Visa für einen kurzfristigen Aufenthalt angestellt werden.

Auch der Verweis auf die Gemeinsame Konsularische Instruktion sollte näher geklärt werden, um festzustellen, ob diese als geeignete Rechtsgrundlage für die Erhebung personenbezogener Daten gemäß Artikel 6 der Richtlinie anzusehen ist.

2.2. Verhältnismäßigkeit und Zweckbindung

Der zentrale Aspekt für die Beurteilung der Angemessenheit und der Verhältnismäßigkeit der vorgeschlagenen Maßnahmen, die bei jedem Eingriff in das Grundrecht auf Schutz der Privatsphäre geprüft werden müssen, ist der Zweck bzw. sind die Zwecke der Datenverarbeitung. Dies gilt auch im Hinblick auf die Kriterien der Rechtmäßigkeit gemäß Artikel 6 der auf den Verordnungsentwurf anzuwendenden Richtlinie 95/46/EG. Danach dürfen personenbezogene Daten nur für *festgelegte, eindeutige und rechtmäßige Zwecke* erhoben und nicht in einer *mit diesen Zweckbestimmungen nicht zu vereinbarenden* Weise weiterverarbeitet werden, ferner müssen sie *dem Zweck* entsprechen, für den sie erhoben und/oder verarbeitet werden, und dafür erheblich sein und dürfen nicht darüber hinausgehen.

Die spezifischen Zwecke des VIS müssen klar festgelegt sein, damit geprüft werden kann, ob der Vorschlag dem Grundsatz der Verhältnismäßigkeit entspricht. Dazu müssen in erster Linie die Zwecke der geplanten Datenverarbeitung klar und eng definiert werden.

Laut Artikel 1 Absatz 2 des Vorschlags dient das VIS "zur Verbesserung der Durchführung der gemeinsamen Visapolitik, der konsularischen Zusammenarbeit und der Konsultation zwischen zentralen Konsularbehörden". Der weitere Wortlaut des Textes scheint sich jedoch auf andere Zwecke zu beziehen (siehe die Buchstaben a) bis f) dieses Absatzes). Diese sollten im Hinblick auf die Rechtsgrundlage des Vorschlags eindeutig festgelegt werden.

Möglicherweise ließen sich einige dieser Zwecke auch im Rahmen des Schengener Informationssystems SIS verfolgen; es ist deshalb darauf zu achten, dass keine Überlappungen bzw. Überschneidungen zwischen den beiden Systemen entstehen.[14]

Die Aspekte "*Betrugsbekämpfung*" und Verhinderung der "*Umgehung der Kriterien zur Bestimmung des Mitgliedstaats, der für die Antragsprüfung zuständig ist"* können als weiterer legitimer "Nutzen" betrachtet werden und scheinen mit der von der Kommission gewählten Rechtsgrundlage im Einklang zu stehen.

Die Notwendigkeit einer gesetzlich geregelten legitimen Grundlage gemäß Artikel 8 EMRK beinhaltet, dass die entsprechenden Kriterien öffentlich auf einfache Weise zugänglich sind, sei es durch Einbeziehung in die Verordnung selbst oder durch einen angemessenen Verweis auf die Fundstelle.

[14] Auch das System SIS II wird zurzeit eingerichtet; hier wird auf die von der Gemeinsamen Schengen-Kontrollinstanz in ihrer Stellungnahme vom April 2004 geäußerten Bedenken verwiesen.

Der Verweis auf die "*Bedrohung der inneren Sicherheit*" deutet auf einen umfassenden, sektorübergreifenden Zweck hin, der bereits durch zahlreiche Instrumente der polizeilichen Zusammenarbeit – einschließlich des SIS – verfolgt wird. Er muss hier ausschließlich auf den Hauptzweck des VIS bezogen werden, nämlich die Verbesserung der gemeinsamen Visapolitik, und darf nur insofern zum Einsatz kommen, als er mit der genannten Politik im Einklang steht.

Die Zwecke "*Erleichterung der Kontrollen an den Außengrenzen und im Hoheitsgebiet der Mitgliedstaaten", "Beitrag zur Identifizierung und Rückführung illegaler Einwanderer"* und "*Erleichterung der Anwendung der Verordnung (EG) Nr. 343/2003*" scheinen nicht mit der ersten in Artikel 8 EMRK genannten Forderung im Einklang zu stehen, da sie angesichts der Rechtsgrundlage des Vorschlags nicht zu den Maßnahmen gehören, die angenommen werden können.

Andererseits werden im Verlauf des Vorschlags verschiedene "Zwecke" für bestimmte Verarbeitungsschritte genannt (Artikel 13: " ... zum Zwecke der Prüfung der Anträge", Artikel 14: "Zum Zwecke der Konsultation zwischen Behörden", Artikel 15: ".. zum Zwecke der Erstellung von Berichten und Statistiken", Artikel 16 und 17: "zum Zweck der Identifizierung"). Die Vielzahl dieser "Zwecke" sollte im Hinblick auf die spezifischen Anforderungen erneut überprüft werden, damit der Grundsatz der Begrenzung der Zwecke eingehalten wird.

Vor dem Hintergrund von Artikel 6 der Richtlinie sollten die "Zwecke" der Datenverarbeitungsvorgänge eng definiert und auf die Verbesserung der gemeinsamen Visapolitik begrenzt sein; der Wortlaut des Vorschlags sollte entsprechend abgeändert werden. Der Zweck der Verarbeitungsvorgänge muss mit der von der Kommission verwendeten Rechtsgrundlage für den Vorschlag übereinstimmen, insbesondere mit Artikel 62 Absatz 2 Buchstabe b Ziffer ii und Artikel 66 EG-Vertrag.

2.3. Datenkategorien

Im vorliegenden Vorschlag ist die Aufnahme verschiedener Datenkategorien in das VIS vorgesehen, darunter auch biometrischer Daten.

Laut Artikel 6 der Richtlinie 95/46/EG dürfen personenbezogene Daten nur dann verarbeitet werden, wenn sie den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen.

Die Aufnahme personenbezogener Daten in das System ist auf der Grundlage eines spezifischen Rechtsaktes möglich, demzufolge ein Visum-Antragsteller zur Angabe von Informationen verpflichtet ist, die für das Verfahren zur Visumerteilung und zur Verhinderung von "Visa-Shopping" und Betrug für notwendig erachtet werden.

Selbst unter der Annahme, dass das VIS auf bereits zuvor bestehenden Regelungen gründet – die allerdings nicht durchgängig öffentlich bekannt bzw. eindeutig spezifiziert sind – d.h. unter der Annahme, dass sich das System auf Daten bezieht, die ein Visumantragsteller bereitstellen muss, ist zur Einhaltung der Vorschriften der Richtlinie sorgfältig zu prüfen, ob diese Daten in das System aufgenommen werden müssen.

Je nach Ausgestaltung der Mechanismen für den Zugang zu den Daten, ihrer Übermittlung /Verbreitung und auch der Speicherfrist können einige Daten einen sehr stark in die Privatsphäre eindringenden Charakter haben. Daher ist nach strengen Selektionskriterien vorzugehen, damit nur Daten in das System aufgenommen werden, die für den genannten Zweck, nämlich die Entwicklung einer gemeinsamen Visapolitik, tatsächlich unerlässlich

sind. Alle anderen Daten können, sofern sie notwendig sind, im Wege der Konsultation zwischen den zentralen Behörden ausgetauscht werden, wie es in Artikel 7 des Vorschlags vorgesehen ist.

a) Staatsangehörigkeit zum Zeitpunkt der Geburt

Die Datenschutzgruppe vertritt die Auffassung, dass die in Artikel 6 geforderte Angabe der Staatsangehörigkeit des Antragstellers zum Zeitpunkt der Geburt (neben der derzeitigen Staatsangehörigkeit) für die Durchführung der gemeinsamen Visapolitik nicht von Bedeutung ist und zu einer unrechtmäßigen Diskriminierung zwischen Personen aus ein und demselben Drittland führen kann. Die Datenschutzgruppe ersucht um Streichung dieses Passus aus Artikel 6.

Ob diese Angabe notwendig ist, sollte auf der Grundlage des Einzelfalls geprüft werden; wird die Information als notwendig erachtet, sollte sie in die Akte des Antragstellers eingetragen werden und auf Anfrage gemäß dem in Artikel 7 des Vorschlags beschriebenen Konsultationsverfahren zur Verfügung gestellt werden.

Sollten auch andere Instrumente des Schengen-Besitzstandes die Bereitstellung dieser Information fordern, wäre aus Gründen der Kohärenz eine entsprechende Änderung dieser Instrumente zu erwägen.

b) Gründe für die Ablehnung der Visumerteilung

Die Datenschutzgruppe nimmt Bezug auf die in Artikel 10 Absatz 2 Buchstabe d aufgelisteten Gründe für die Ablehnung der Visumerteilung.

Es muss betont werden, dass die in Buchstabe d genannten Gründe möglicherweise bereits dazu geführt haben, dass ein Antragsteller gemäß Artikel 96 des Schengener Übereinkommens zur Einreiseverweigerung ausgeschrieben wurde (siehe Buchstabe c des Vorschlags) und dass alle Visumbehörden Zugriff auf eine solche Ausschreibung haben; deshalb sollte dieser Sachverhalt unter dem genannten Buchstaben c geregelt werden.

Zum gegenwärtigen Zeitpunkt ist die Aufnahme der Parameters "Gefahr für die öffentliche Gesundheit" in die Standardgründe für die Ablehnung der Visumerteilung eine Neuerung gegenüber dem Schengen-Besitzstand, der Grundlage des Vorschlags. So steht die Anwendung dieser Bestimmung - sofern nicht anders geregelt - im Ermessen des einzelnen Mitgliedstaates. Die Datenschutzgruppe ersucht um Streichung des Buchstaben d beziehungsweise zumindest um eindeutigere und engere Verweise auf die möglichen Gefahren und um zusätzliche präzisere Verweise auf die unionsweit geltenden Definitionen der genannten Konzepte.

Die im Vorschlag vorgesehene Änderung der Gemeinsamen Konsularischen Instruktion im Wege einer weiteren Verordnung des Parlaments und des Rates wäre eine gute Gelegenheit zur Vornahme der erforderlichen Anpassungen und Änderungen.[15]

c) Verknüpfung zu anderen Anträgen

Schließlich macht die Datenschutzgruppe auf Artikel 3 Absatz 1 Buchstabe d "Verknüpfung zu anderen Anträgen" aufmerksam. Dieser Punkt, der sich keineswegs nur auf den technischen Betrieb des Systems bezieht, könnte tatsächlich bestimmte Auswirkungen für die Betreffenden haben. Deshalb müssen der Geltungsbereich dieser Bestimmung und die

[15] Siehe Erwägungsgründe 6 und 8.

entsprechenden Sicherheitsvorkehrungen eindeutig durch Rechtsvorschriften festgelegt werden. Gerade die Möglichkeit der Verknüpfung von Daten kann dazu führen, dass die Informationen von Personen eingesehen werden können, die nicht die entsprechenden Zugriffsrechte besitzen. Es muss gewährleistet sein, dass die geltenden Zugriffsrechte auf die verschiedenen Datenkategorien des VIS nicht durch Verknüpfungsmechanismen ausgehebelt werden können.

2.4. Spezifische Probleme: biometrische Merkmale

Zur Aufnahme biometrischer Daten in das System wird in Erwägungsgrund 9 lediglich auf die Notwendigkeit der "genauen Überprüfung und Identifizierung von Visumantragstellern" verwiesen (die beiden Verfahren werden in Artikel 2 Absatz 10 und 11 definiert). In Artikel 3 werden "Fotos" (Buchstabe b) und "Fingerabdruckdaten" (Buchstabe c) genannt.

Der Vorschlag sollte um angemessene Sicherheitsvorkehrungen zu besonders sensiblen Daten erweitert werden, wie es die Datenschutzgruppe bereits in ihrer Stellungnahme Nr. 7/2004 vom 11.08.2004 gefordert hat. Es wäre wichtig, genau zu wissen, "welche Studien über das Ausmaß und die Gewichtigkeit der drohenden Gefahren belegen, dass dieses Vorgehen zum Schutz der öffentlichen Sicherheit und Ordnung unerlässlich ist, und ob alternative Vorgehensweisen geprüft wurden oder geprüft werden können, die nicht mit derartigen Risiken verbunden sind."

Die Prüfung des Grundsatzes der Verhältnismäßigkeit im Zusammenhang mit der Visa-Erteilung und dem freien Personenverkehr wirft zwangsläufig die Frage nach der grundsätzlichen Legitimität der Erhebung dieser Daten auf; sie beschränkt sich keinesfalls auf die Verarbeitungsprozedur (Zugriffsbedingungen, Speicherzeitraum usw.).

Bei der Entwicklung von Lösungen, die die Aufnahme biometrischer Informationen in die Datenbank beinhalten, ist äußerste Vorsicht angezeigt; außerdem muss die Möglichkeit der Ausdehnung des Zugriffs auf ursprünglich nicht vorgesehene Personenkreise sorgfältig bedacht werden.

Besondere Aufmerksamkeit ist dem Grundsatz der Verhältnismäßigkeit bei einer Lösung zu widmen, die über die rechtliche Prüfung vor Ausstellung der fraglichen Dokumente und über die Aufnahme biometrischer Daten in diese Dokumente hinausgehen und dazu führen würde, dass Biometriedaten aller Ausländer, die ein Visum oder eine Aufenthaltsgenehmigung beantragen, zwecks späterer Kontrolle illegaler Einwanderer (insbesondere Einwanderer ohne Papiere) in Datenbanken gespeichert werden und sich diese Daten auf Spuren beziehen, wie sie jedermann im Alltag hinterlässt.

Die Rechtmäßigkeit der Verarbeitung solcher Daten zum Zwecke der Identifizierung ist vor allem deshalb äußerst sorgfältig zu prüfen, weil für die Betroffenen die Gefahr nachteiliger Auswirkungen besteht, wenn die Daten verloren gehen oder zweckentfremdet werden.

Auch müssen die möglichen Folgen bedacht werden, wenn beim Abnehmen der Fingerabdrücke eine falsche Zuordnung zu den Identifizierungsdaten erfolgt; dies kann auch absichtlich geschehen, wenn z.B. eine Person, deren Fingerabdrücke digital erfasst wurden, nicht ihre tatsächliche Identität preisgibt. In diesem Fällen würde die "gestohlene" Identität auf Dauer mit den betreffenden Fingerabdrücken verknüpft.

Die Umstände, unter denen die Fingerabdrücke abgenommen werden, müssen hundertprozentige Zuverlässigkeit garantieren.

Der Vorschlag sollte um Informationen zur "Erfassungsphase" der Abnahme der Fingerabdrücke und zu den (von den Visumbehörden umzusetzenden) Mechanismen der Erhebung biometrischer Daten ergänzt werden; in diesem Zusammenhang ersucht die Datenschutzgruppe um die Aufnahme spezifischer Bestimmungen in den Vorschlag, die ein hohes Maß an Zuverlässigkeit bei der Erfassung und Verifizierung der biometrischen Daten gerade in dieser Phase sicherstellen und insbesondere die Gefahr des "Identitätsdiebstahls" verhindern.

Es sollten auch Garantien für Personen vorgesehen werden, die ein üblicherweise verwendetes biometrisches Merkmal, beispielsweise Fingerabdrücke, nicht vorweisen können (z. B. wegen Verlust oder Verletzung der Finger) und allein deshalb nicht die Möglichkeit der Beantragung und Erteilung eines Visums erhalten. Besonderer Berücksichtigung bedürfen Kinder und ältere Menschen.

Ferner sollte möglicherweise durch besondere Schutzgarantien klargestellt werden, dass die Daten nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise verwendet werden dürfen.

Besonders streng muss geprüft werden, ob diese Biometriedaten in einer zentralen Datenbank gespeichert werden sollen, weil damit das Risiko erheblich zunimmt, dass die Daten in einer Weise verwendet werden, die unverhältnismäßig oder mit dem ursprünglichen Erhebungszweck unvereinbar ist. [16]

Auch wenn gemäß Artikel 13 der Richtlinie 95/46/EG in bestimmten Fällen Einschränkungen dieser Grundsätze zulässig sind, müssen die Voraussetzungen für solche Einschränkungen und die Einschränkungen selbst auf einer klaren, präzisen Rechtsgrundlage beruhen.

Weitgefasste Zielsetzungen sind nur dann legitim, wenn die oben genannten Grundsätze für jede einzelne Zielsetzung berücksichtigt werden.

Bei der Einrichtung einer derart umfangreichen Datenbank kann es zu Zuverlässigkeitsproblemen im Zusammenhang mit dem Zugang und auch bei falsch-positiven und/oder falsch-negativen Ergebnissen kommen – mit möglichen Nachteilen für die Betroffenen.

Die Verwendung biometrischer Daten zu Identifizierungszwecken sollte selektiv begrenzt sein; die Aufnahme solcher Daten in das CS-VIS ist nur in unbedingt notwendigen Fällen vorzusehen, z.B. bei Verdacht auf Verfahrensmissbrauch oder bei Personen, deren Daten bereits im System gespeichert sind und deren Visumantrag aus schwerwiegenden Gründen abgelehnt wurde.

Die Verfügbarkeit biometrischer Daten im VIS sollte auf spezifische Fälle begrenzt werden, in denen das System bereits Daten zu der betreffenden Person enthält; der Austausch dieser Daten sollte ausschließlich im Rahmen der Kooperation zwischen den zuständigen Behörden erfolgen (ein Bereich, der sinnvollerweise in Artikel 7 und nicht in Artikel 6 zu regeln wäre).

Um die genannten Probleme unter Achtung der Menschenwürde und ohne Beeinträchtigung des Sicherheitsstandards der Visapolitik zu lösen, müssen "Ausweichverfahren" erarbeitet und in den Vorschlag aufgenommen werden.

Angesichts der gravierenden Folgen für die rechtmäßigen Inhaber der Dokumente sollten die verwendeten Technologien auf jeden Fall einen sehr geringen Prozentsatz an unberechtigten Zurückweisungen (Erkennungsfehler) garantieren.

---

[16] Siehe insbesondere das Arbeitspapier über Biometrie vom August 2003 (WP 80) http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf.

Insbesondere für den Fall von Erkennungsfehlern bei Grenzkontrollen sind Garantien dafür festzulegen, dass die betroffenen Personen über die Ursachen der Zurückweisung und über ihre Möglichkeiten unterrichtet werden, ihren Standpunkt darzulegen, bevor eine Entscheidung getroffen wird (Artikel 15 der Richtlinie 95/46/EG über automatisierte Einzelentscheidungen), und dass der Sachverhalt unverzüglich geklärt wird.

Zur Verwendung biometrischer Daten für Verifikationszwecke – diese Frage ist insbesondere im Hinblick auf die Anwendung von Artikel 16 des Vorschlags von Bedeutung - wird auf Punkt 2.6 dieser Stellungnahme verwiesen (Verwendung von Daten für Visakontrollen).

2.5. Die betroffenen Personen

Die Datenschutzgruppe äußert Bedenken in Bezug auf die Bestimmung, derzufolge die Daten mehrerer Personenkategorien ohne vorherigen Nachweis der realen Notwendigkeit ihrer Verarbeitung verfügbar gemacht werden sollen.

a) Daten über Drittstaatsangehörige, die ein Visum beantragen

Die Datenschutzgruppe macht beim Thema der Visa für einen kurzfristigen Aufenthalt auf den Status von Drittstaatsangehörigen aufmerksam, die sich rechtmäßig im Hoheitsgebiet eines Mitgliedstaats aufhalten. Nach Artikel 21 des Schengener Übereinkommens kann sich ein Drittstaatsangehöriger mit einem von einer der Vertragsparteien ausgestellten gültigen Aufenthaltstitel bis zu drei Monaten auch im Hoheitsgebiet der anderen Vertragsstaaten frei bewegen.[17] Dieser Sachverhalt sollte im Wortlaut des Vorschlags klargestellt und die Definition des "Drittstaatsangehörigen" zu den Zwecken der Verordnung um den folgenden Passus erweitert werden: "jede Person, die nicht Unionsbürger ist oder keinen rechtmäßigen Wohnsitz in der Europäischen Union hat…". Bei Beibehaltung der derzeitigen Definition müsste klargestellt werden, dass diese Verordnung nicht für Drittstaatsangehörige gilt, die einen rechtmäßigen Wohnsitz in der Europäischen Union haben. Dementsprechend sind die Daten über Visuminhaber, denen später ein Aufenthaltstitel erteilt wird, unverzüglich zu löschen.

b) Daten über Gruppenmitglieder

Die Definition von "Gruppenmitgliedern" gemäß Artikel 2 des Vorschlags und der Verweis auf "in einer Gruppe reisende Antragsteller" in Artikel 5 Absatz 4 (der die Verknüpfung der Antragsdatensätze vorsieht) sollte näher spezifiziert werden, da sonst auch Personen mit relativ unbedeutender Verbindung zueinander (Kunden, Landsleute, Kollegen usw.) einbezogen werden könnten. Die Definition der "Gruppenmitglieder" und die im Hinblick auf "Gruppenvisa" zu treffende Unterscheidung sollten präzisiert werden und auf eindeutigen und objektiven Kriterien basieren.

---

[17] Artikel 21 des Schengen-Besitzstands, auf den in Artikel 1 Absatz 2 des Beschlusses des Rates 1999/435/EG vom 20. Mai 1999 (*), ABl. L 176 vom 10.7.1999, S. 1 Bezug genommen wird, lautet:
"1) Drittausländer, die Inhaber eines gültigen, von einer der Vertragsparteien ausgestellten Aufenthaltstitels sind, können sich aufgrund dieses Dokuments und eines gültigen Reisedokuments höchstens bis zu drei Monaten frei im Hoheitsgebiet der anderen Vertragsparteien bewegen, soweit sie die in Artikel 5 Absatz 1 Buchstaben a), c) und e) aufgeführten Einreisevoraussetzungen erfüllen und nicht auf der nationalen Ausschreibungsliste der betroffenen Vertragspartei stehen.
(2) Das gleiche gilt für Drittausländer, die Inhaber eines von einer der Vertragsparteien ausgestellten vorläufigen Aufenthaltstitels und eines von dieser Vertragspartei ausgestellten Reisedokuments sind."

c) Daten über Personen, die Einladungen aussprechen

Nach Artikel 6 des Vorschlags soll der Datensatz zum Visumantrag auch "Angaben zur Person, die eine Einladung ausgesprochen hat oder verpflichtet ist, die Lebenshaltungskosten während des Aufenthalts zu tragen" enthalten. Die Datenschutzgruppe stellt fest, dass diese Datenkategorie bei präzisen Anfragen zu Einzelpersonen und bei konkreten Verstößen gegen gesetzliche Bestimmungen relevant und notwendig sein kann. Die Verarbeitung dieser Daten wäre jedoch unverhältnismäßig und ginge über das Ziel der routinemäßigen Umsetzung der Visapolitik hinaus, für die die in Artikel 6 genannten Datensätze ausreichen dürften. Daher ersucht die Datenschutzgruppe um Streichung dieser Datenkategorie bzw. zumindest um ihre Verschiebung von Artikel 6 in Artikel 7 (im Fall einer Konsultation zwischen zentralen Behörden in das VIS einzugebende Datenkategorien), sofern die Notwendigkeit nicht erwiesen ist.

2.6. Zugang zur VIS-Datenbank

Die Datenschutzgruppe geht angesichts der Zusagen der Kommission davon aus, dass sie in Kürze einen ausführlichen und vollständigen Überblick über die verschiedenen Initiativen der Kommission und des Rates im Rahmen von Titel IV des EG-Vertrags erhalten wird, die sich auf die Verarbeitung von personenbezogenen Daten und/oder den Austausch entsprechender Informationen beziehen. In diesem Bereich sind die Grundsätze der Richtlinie 95/46/EG in vollem Umfang anzuwenden, und die Wahrung von Artikel 8 der Europäischen Menschenrechtskonvention ist keine Frage der Selbstbescheinigung.

Wie die Sicherheit erfordert auch das Recht auf den Schutz der Privatsphäre eine bereichsübergreifende Betrachtung. Bei den Überlegungen zum Einsatz eines bestimmten Systems sollte der Schutz der Privatsphäre nicht als Hindernis angesehen werden, sondern als zusätzlicher Nutzen. Wenn der Bereich Sicherheit/Privatsphäre erst nach Festlegung der Spezifikationen und Parameter eines Systems ins Blickfeld kommt, ist die Wahrscheinlichkeit hoch, dass bestimmte Elemente des Systems später noch einmal umgestaltet werden müssen, was zu zusätzlichen Kosten führt.

a) Zentral erfasste Daten und Datenempfänger

Die zugriffsberechtigten Behörden und die Operationen, die diese Behörden durchführen können, sind unter Berücksichtigung der jeweils verfolgten Zwecke im Vorschlag aufgelistet.

Gemäß Artikel 4 ist die Veröffentlichung einer Liste der nationalen Behörden mit Zugang zum VIS vorgesehen. Mit Blick auf etwaige Änderungen empfiehlt die Datenschutzgruppe eine – möglichst regelmäßige – Aktualisierung dieser Liste. Im Vorschlag scheint keine Zugangsmöglichkeit auf unionsweiter Ebene vorgesehen zu sein, doch sollten die Datenschutzbehörden zusätzliche Informationen über die bevollmächtigten Dienststellen/Behörden und die jeweiligen Zugangsebenen erhalten, damit sie ihre Überwachungs- und Kontrollfunktionen besser wahrnehmen können.

b) Verwendung von Daten durch andere, in den Artikeln 16 bis 19 des Vorschlags genannte Behörden

Im Hinblick auf die Bestimmungen, denen zufolge der Zugang zum VIS auch anderen als den für die Erteilung von Visa zuständigen Behörden gewährt werden soll, wird auf die oben angeführten Überlegungen zur Sicherstellung der Zweckbindung gemäß der Rechtsgrundlage des Vorschlags verwiesen.

Aus diesem Grund sollte der Einsatz des Systems, auch vor dem Hintergrund der bereits erwähnten Gefahr von Fehlern und/oder des Zugriffs nicht ermächtigter Personen, auf die wesentliche Zielsetzungen der gemeinsamen Visapolitik beschränkt werden.

Andere Zwecke, die enger mit dem Schutz der öffentlichen Sicherheit verbunden sind, werden durch andere Informationssysteme innerhalb der Europäischen Union verfolgt – hier ist an erster Stelle das Schengen-System zu nennen, das durch das VIS ergänzt werden soll.

c) Verwendung von Daten für Visakontrollen

"Die für Kontrollen an den Außengrenzen und im Hoheitsgebiet der Mitgliedstaaten zuständigen Behörden" haben zum Zweck der "Überprüfung der Identität der Person und/oder der Echtheit des Visums" Zugang zum VIS (Artikel 16 des Vorschlags).

Eine solche Überprüfung bestünde in der Zuordnung der in einem vorgelegten Dokument (Pass und/oder Visum) enthaltenen Daten zu der betreffenden Person, also im "Abgleich von Datensätzen zur Überprüfung einer Identitätsangabe", wie es in der Definition heißt.

Grundsätzlich scheint es für Verifizierungszwecke nicht erforderlich, die Referenzdaten in einer Datenbank zu speichern; eine dezentrale Speicherung der personenbezogenen Daten (z. B. auf einem Mikrochip) reicht aus, wie die Datenschutzgruppe in ihrem Arbeitsdokument über Biometrie vom 1. August 2003 ausgeführt hat.[18]

Außerdem wird auf den Vorschlag für eine Verordnung über eine einheitliche Visagestaltung verwiesen, der ein lokales Speichermedium (Mikrochip) oder ein anderes System zur Überprüfung einer Identitätsangabe vor Ort mit Hilfe eines Instruments vorsieht, das sich unter der Kontrolle der betreffenden Person befindet. Die Datenschutzgruppe ist nach wie vor der Auffassung, dass ein solches System auch deswegen vorzuziehen wäre, weil es nicht so stark in die Privatsphäre eingreift.

Zugang zum CS-VIS sollte nur dann erlaubt sein, wenn die Verifizierung negativ ist, die betroffene Person aber identifiziert werden muss. In diesem Fall sollte die Überprüfung allerdings von entsprechend geschultem Personal durchgeführt werden und auch mehr Zeit in Anspruch nehmen als bei Grenzkontrollen üblicherweise vorgesehen. Nicht alle Bediensteten an den Grenzübergangsstellen sollten Zugang zu dem System erhalten; diesem Personal stehen bereits die SIS-Daten – insbesondere Daten zu Personen, die zur Einreiseverweigerung ausgeschrieben sind – und das jeweilige nationale Informationssystem zur Verfügung.

Der gegenwärtige Wortlaut des Verordnungsvorschlags sollte dahingehend verbessert werden, dass die Verarbeitung personenbezogener Daten ausschließlich auf die genannten Zwecke beschränkt ist; hierzu sollten zum einen die Behörden mit Online-Zugang zur VIS-Datenbank präziser und auch selektiver spezifiziert werden, zum anderen sollten Vorkehrungen zur regelmäßigen Überprüfung der Zugriffe durch ein internes Kontrollsystem getroffen werden.

Zum Verfahren der Identitätsüberprüfung durch die zuständigen Behörden "im Hoheitsgebiet" wird vorgeschlagen, diese Behörden genauer zu spezifizieren. Da die Verwendung von Daten für Visakontrollen im Verordnungsentwurf als zusätzlicher Nutzen zur Verwirklichung des Ziels des VIS, der Verbesserung der gemeinsamen Visapolitik, bezeichnet wird, können mit den zuständigen Behörden nur die in Artikel 2 Absatz 3 genannten Visumbehörden gemeint sein – wobei zu berücksichtigen ist, dass die Identitätsüberprüfung im Hoheitsgebiet eines

[18] Dokument WP80 vom 01.08.2003, verfügbar unter: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf.

Staates auch durch das SIS bzw. andere, für polizeiliche Zwecke eingerichtete Datenbanken erfolgen kann.

d) Zugang zum VIS für andere, im Vorschlag der Kommission nicht genannte Behörden

Die Datenschutzgruppe nimmt die vom Rat am 7. März 2005 angenommenen Schlussfolgerungen zur Kenntnis, denen zufolge "die für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten bei der Ausübung ihrer Befugnisse im Bereich der Prävention von Straftaten sowie ihrer Aufdeckung und Ermittlung, einschließlich im Hinblick auf terroristische Handlungen oder Bedrohungen, Zugang zur Abfrage des VIS haben" sollen.

Dieser Zugang soll auf der Grundlagen eines auf Titel VI EUV gestützten Adhoc-Vorschlags gewährt werden, zu dessen Vorlage die Kommission aufgefordert ist, "damit dieser Rechtsakt in einem ähnlichen Zeitrahmen wie die VIS-Verordnung angenommen werden kann".

Zweck der Datenverarbeitung im Rahmen des VIS soll, wie bereits dargelegt, die Durchführung der Visapolitik sein. Der Zugang zu VIS-Daten sollte daher denjenigen Behörden vorbehalten sein, die mit der Durchführung dieser Politik betraut sind, und die technischen Spezifikationen müssen so ausgestaltet werden, dass dieser Zweck erfüllt und diesen Behörden der Zugang gewährt wird.

Der Zugang zu den VIS-Daten und ihre Verwendung durch die Behörden, die mit der Bekämpfung der genannten Straftaten befasst sind, ist vor dem Hintergrund der Ziele des VIS zu betrachten und nur zu diesem Zweck zu gewähren.

Die beabsichtigte Erweiterung der Zugriffsrechte gegenüber den Bestimmungen des Verordnungsentwurfs muss sorgfältig dahingehend geprüft werden, ob sie im Zusammenhang mit den Zwecken des Systems erforderlich ist.

Der Zugriff durch andere Behörden wäre nur auf einer Adhoc-Basis unter bestimmten Umständen und mit angemessenen Schutzmaßnahmen rechtmäßig. Eine Regelung, die den systematischen oder routinemäßigen Zugriff erlaubt, würde ganz klar über eine "in einer demokratischen Gesellschaft notwendige Maßnahme" hinausgehen und könnte nicht als rechtmäßig gelten.

Deshalb müssen die technischen Spezifikationen für den Zugang zu den VIS-Daten so ausgestaltet sein, dass ein *routinemäßiger* Zugriff durch andere Behörden und für andere Zwecke ausgeschlossen ist.

Auch sollte das System technisch nicht so ausgelegt sein, dass bestimmte Zugriffsmöglichkeiten eingerichtet werden, die ausschließlich anderen Zwecken dienen.

Die Datenschutzbehörden müssen angemessen und zu einem frühen Stadium in die Gespräche über die Ausgestaltung dieser technischen Spezifikationen eingebunden werden.

Das Konzept der "für die innere Sicherheit zuständigen Behörden" sollte präzisiert werden, damit der Verweis auf die Strafverfolgungsbehörden klar ist (Einrichtungen der dritten Säule).

2.7. Interoperabilität von VIS und SIS II

Die Datenschutzgruppe hat bereits ihre Bedenken zum großen Umfang der in Aufbau befindlichen Datenbank und zu der Möglichkeit geäußert, dass ihre Verwendung mit Blick auf die Interoperabilität der europäischen Datenbanken bzw. auf die Synergieeffekte zwischen

den gegenwärtigen und den zukünftigen Informationssystemen (SIS II, EURODAC) ausgeweitet werden könnte.

Im Zusammenhang mit dem Ersuchen des Rates an die Kommission, Vorschläge zur Verbesserung der Interoperabilität der europäischen Datenbanken vorzulegen und zu erkunden, welche Synergieeffekte zwischen den bestehenden und den künftigen Informationssystemen (SIS II, VIS und Eurodac) geschaffen werden können, damit der Zusatznutzen, den diese Systeme in ihrem jeweiligen rechtlichen und technischen Rahmen bieten, der Verhütung und Bekämpfung des Terrorismus zugute kommen kann, bekräftigt die Datenschutzgruppe die Notwendigkeit, dass - unbeschadet der Beurteilung der entsprechenden Rechtsgrundlage - die Einhaltung der Zielsetzungen des VIS gewährleistet sein muss.

Es muss klargestellt sein, dass das grundlegende Konzept einer rechtmäßigen, der Forderung der Verhältnismäßigkeit genügenden Erhebung personenbezogener Daten und ihrer weiteren Verarbeitung für einen präzisen und rechtmäßigen Zweck (d. h. die Erteilung eines Schengen-Visums) keinen Raum lassen darf für das Konzept einer Datenbank, auf die verschiedene Behörden zu unterschiedlichen Zwecken zugreifen können.

Die Interoperabilität darf nicht dazu führen, dass eine Behörde, die keine Berechtigung zum Zugang bzw. zur Verwendung bestimmter Daten hat, diese Daten über ein anderes Informationssystem erhalten kann.

Die Datenschutzgruppe bekräftigt ihre feste Absicht, an der konkreten Ausgestaltung dieser Interoperabilität mitzuwirken.

Besonderes Gewicht muss dabei auf eine angemessene öffentliche Diskussion über die Auswirkungen dieser Initiative auf die Persönlichkeitsrechte gelegt werden, an der nicht nur die Parlamente der Mitgliedstaaten, sondern alle Betroffenen beteiligt sein sollen.

Die Datenschutzgruppe möchte ferner auf die Stellungnahme der Gemeinsamen Schengen-Kontrollinstanz[19] zur Entwicklung des SIS II aufmerksam machen. Die Datenschutzgruppe vertraut darauf, dass die Kommission sie rechtzeitig über ihre Vorschlagsentwürfe in Kenntnis setzt, damit sie - anders, als es bedauerlicherweise beim Vorschlagsentwurf zu SIS II der Fall war - ihren Beitrag zeitnah leisten kann.

2.8. Speicherung der Daten

Die Datenschutzgruppe begrüßt die Bestimmung des Verordnungsentwurfs, die Daten für einen Zeitraum von höchstens fünf Jahren zu speichern. Ebenso wird die Aufnahme einer besonderen Bestimmung in Artikel 22 begrüßt, derzufolge - im Einklang mit dem Grundsatz der Spezifizierung der Zweckbestimmung - die Daten eines Antragstellers gelöscht werden müssen, der die Staatsangehörigkeit eines Mitgliedstaats erlangt, wobei diese Bestimmung auch auf Drittausländer angewendet werden sollte, die rechtmäßig ihren Wohnsitz in einem Mitgliedstaat haben (langfristige Migranten).

Es sollten anspruchsvollere Speicherkriterien festgelegt werden, die nicht nur den verschiedenen in der Praxis auftretenden Umständen Rechnung tragen, sondern auch den unterschiedlichen Arten von Visa, die erteilt werden können.

[19] Stellungnahme zur Entwicklung des SIS II, http://escher.drt.garanteprivacy.it/garante/navig/schengen/home.htm.

Beispielsweise könnten die Daten von Personen, die Visumanträge mehrfach oder in betrügerischer Weise unter falschem Namen gestellt haben, länger aufbewahrt werden als die Daten von Personen, deren Reisedokumente ausgestellt wurden und deren Reise problemlos verlaufen ist. Sodann erscheint es nicht angemessen, Daten über Visa für einen höchstens dreimonatigen Aufenthalt für einen Zeitraum von länger als zwei Jahren zu speichern, insbesondere wenn der kurzfristige Aufenthalt ohne besondere Zwischenfälle verlaufen ist.

Ein besonderes Kriterium könnte auch für Vielreisende angewendet werden, wenn sich das Antragsverfahren dadurch beschleunigen lässt.

Dieser Vielzahl spezifischer Umstände sollte durch die Festlegung differenzierter Speicherfristen im VIS begegnet werden; besonders zu berücksichtigen ist dabei die geplante automatische Verknüpfung der Antragsdaten mit anderen im System gespeicherten Informationen.

Diese ausdifferenzierten Speicherfristen sollten aber in keinem Fall den im Vorschlag vorgesehenen Höchstzeitraum von fünf Jahren überschreiten. Im Einzelnen schlägt die Datenschutzgruppe Folgendes vor:

- Die Daten von Personen, denen die Visumerteilung verweigert wurde, sollten grundsätzlich nur für einen in Wochen oder Monaten festzulegenden Zeitraum gespeichert werden, der zur Verhinderung des so genannten "Visa-Shopping" erforderlich ist. Dies sollte insbesondere für Fälle gelten, in denen die Gründe für die Ablehnung verwaltungstechnischer Natur sind, wie z. B. in Artikel 10 Absatz 2 Buchstabe a bzw. Buchstabe b vorgesehen.
- Die Daten von Personen, denen die Visumerteilung aus Gründen der öffentlichen Gesundheit verweigert wurde, sind nach Wegfall dieser Gründe unverzüglich zu löschen.
- Die Speicherfrist für Daten zu Einreiseverweigerungen aufgrund von Ausschreibungen im SIS sollten an die Höchstdauer der Speicherfrist für SIS-Ausschreibungen angepasst werden, die im SIS selbst vorgesehen ist. Dort werden Daten von Drittausländern, denen die Einreise verweigert wurde, drei Jahre lang gespeichert. Mit einer über diesen Zeitraum hinausgehenden Speicherung der SIS-Daten im VIS würden die Bestimmungen zur erneuten Überprüfung der Daten und Löschung aus dem SIS umgangen. Aus diesem Grund sollten die Daten zur Visumverweigerung aufgrund einer Ausschreibung im SIS spätestens drei Jahre nach der erfolgten Ausschreibung im SIS gelöscht werden.
- Biometrische Daten dürfen nur unter den in Abschnitt 2.4 genannten Bedingungen im VIS gespeichert werden.
- Verknüpfungen zu den Daten anderer Gruppenmitglieder sind grundsätzlich nach Ablauf der Gültigkeit des Visums zu löschen.

2.9. Rechte der Betroffenen

a) Auskunft

Im Hinblick auf das Auskunftsrecht der Betroffenen – nicht nur der Antragsteller, sondern auch der Personen, die eine Einladung ausgesprochen haben (Artikel 6 Absatz 4 Buchstabe f) – erscheint der Vorschlag angemessen.

Mit Bezug auf die Antragsteller sollte allerdings Artikel 30 Absatz 1 um die Auskunftspflicht zu folgenden Aspekten ergänzt werden:

- Speicherzeitraum im VIS;
- Mechanismen zur Wahrnehmung der Auskunfts- und Berichtigungsrechte gegenüber den Verantwortlichen (d.h. gegenüber der in jedem Vertragsstaat für die Eingabe in das VIS zuständigen Behörde);
- Name und Kontaktadresse der nationalen Kontrollstelle, an die sich Antragsteller wenden können, wenn sie mit der Antwort nicht einverstanden sind.

Darüber hinaus sollte in Absatz 2 des genannten Artikels deutlicher herausgestellt werden, dass die für die Verarbeitung Verantwortlichen - durch den/die entsprechend Beauftragten in den Konsulaten und diplomatischen Vertretungen - die in Artikel 30 genannten Auskünfte zum Zeitpunkt der Datenerfassung geben müssen; bei biometrischen Daten sollten weitere Informationen zu den elektronisch gespeicherten Daten gegeben werden, insbesondere zu denjenigen, die nicht direkt vom Dokument abgelesen werden können.

b) Auskunft über die eigenen Daten

Der Wortlaut von Artikel 31 sollte dahingehend präzisiert werden, dass sich die Betroffenen zur Wahrnehmung dieses Rechts direkt an die für die Verarbeitung verantwortlichen Behörden im jeweiligen Mitgliedstaat wenden können.

Zu diesem Zweck ist zu spezifizieren, dass mit den "zuständigen Behörden" die für die Verarbeitung Verantwortlichen gemeint sind.

Die Betroffenen müssen spätestens zum Zeitpunkt der Erfassung der Daten darüber informiert werden, welche Behörde für die Verarbeitung verantwortlich ist und wie das Recht auf Auskunft, Korrektur und Löschung direkt bei dieser Behörde wahrgenommen werden kann.

Ferner sollte im Text klargestellt werden, dass auf das CS-VIS keine Zugriffsmöglichkeit besteht, da dieses System die Daten nur im Namen der einzelnen Mitgliedstaaten verarbeitet; deshalb müssen die Betroffenen ihre Rechte durch einen Antrag bei der für die Eingabe der relevanten Daten in das VIS zuständigen Behörde des Mitgliedstaates geltend machen.

Absatz 6 sollte einen Verweis auf die Möglichkeit enthalten, die nationale Datenschutzbehörde anzurufen, wenn der Visumantrag abgelehnt wurde oder der Betroffene nicht mit der Antwort der zuständigen Behörde einverstanden ist.

Die Artikel 32 und 33 sollten einen Verweis auf die Rolle der nationalen Datenschutzbehörden enthalten. Wenn ein Betroffener seinen Rechtsanspruch auf Auskunft über seine Daten durch einen Adhoc-Antrag an den Verantwortlichen gemäß Artikel 31 wahrnimmt, obliegt der Datenschutzbehörde die Durchführung der entsprechenden in den nationalen Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG beschriebenen Aufgaben; auf diesen Sachverhalt sollte in beiden Artikeln verwiesen werden.

Im Titel und im ersten Absatz von Artikel 32 wird auf die Zusammenarbeit der zuständigen Behörden verwiesen, während die anderen beiden Absätze auf die Datenschutzbehörden als diejenigen Organe abstellen, die für die Überwachung und Überprüfung der Rechtmäßigkeit der Verarbeitung zuständig sind.

c) Korrektur*

* Anm. d. Übs.: Dieser Punkt betrifft nicht die deutsche Fassung.

Das Recht der Betroffenen auf Korrektur unrichtiger Daten ist im Entwurf vorgesehen. Die Datenschutzgruppe schlägt vor, den Wortlaut von Artikel 31 Absatz 2 "data recorded unlawfully *may* be deleted" in "*must* be deleted" abzuändern.

2.10. Sicherheit

Der Verordnungsentwurf enthält genaue Bestimmungen zu den Risiken der Datenverarbeitung und zur Art der zu schützenden Daten. Die Datenschutzgruppe unterstreicht die Bedeutung angemessener Sicherheitsvorkehrungen und empfiehlt insbesondere die folgenden Maßnahmen:

- Einführung von Maßnahmen zur systematischen Überwachung der Wirksamkeit der (vor allem in den Artikeln 25 und 26 genannten) Sicherheitsvorkehrungen und zur entsprechenden Berichterstattung;
- Erweiterung der Überwachungs- und Bewertungsaufgaben der Kommission auch auf alle Aspekte der Rechtmäßigkeit des Verarbeitungsvorgangs;
- Erstellung präziser Nutzerprofile und einer vollständigen Liste der Benutzeridentitäten, die insbesondere den nationalen Datenschutzbehörden zur Verfügung stehen sollte;
- zusätzlich zur Aufzeichnung aller Verarbeitungsvorgänge sollten auch regelmäßige Eigenkontrollen des VIS vorgesehen werden. Die entsprechenden Berichte sollten den Datenschutzbehörden zur Verfügung stehen, damit die Kontrollverfahren durch gezielte Ausrichtung auf die kritischen Aspekte erleichtert werden;
- Verschlüsselung der Daten vor einer Übertragung im VIS-System, damit unbefugte Dritte nicht darauf zugreifen können;
- Hinzufügung von Funktionen zur sofortigen Wiederherstellung der Daten bei Systemabstürzen und Einrichtung von Sicherheitsmaßnahmen, damit bereits gespeicherte Daten nicht infolge eines Systemfehlers korrumpiert werden können.

Darüber hinaus wünscht die Datenschutzgruppe präzise Informationen darüber, welche Maßnahmen die Visumbehörden ergreifen, um die eindeutige Identifizierung von Personen sicherzustellen, deren biometrische Daten erfasst und dann mit Zensusdaten verknüpft werden, sowie weitere Angaben zur Informationspflicht der genannten Behörden gegenüber den Betroffenen. Im Einzelnen ist zu gewährleisten:

- dass die Daten nur von der Behörde geändert werden können, die für die Ausstellung des Dokuments zuständig ist, und zwar gemäß den Empfehlungen des in Erwägungsgrund 2 aufgeführten Dokuments Nr. 9303 der ICAO (von der ICAO zertifizierte elektronische Signatur); und
- dass auf die im Mikrochip des ausgestellten Dokuments gespeicherten Daten nicht ohne Wissen der betroffenen Person zugegriffen werden kann. Nicht befugte öffentliche oder private Stellen dürfen keinen Zugang zu diesen Daten haben.

In diesem Zusammenhang hat die Datenschutzgruppe in ihrer Stellungnahme Nr. 7/2004 darauf hingewiesen, dass eine Verschlüsselung der Daten zwecks Gewährleistung der Vertraulichkeit angebracht wäre und dass der Lesezugriff auf den Speicherinhalt darüber hinaus mit einem persönlichen Code geschützt werden könnte, der nur dem Inhaber bekannt ist.

2.11. Zuständigkeit für das System und unabhängige Kontrolle

a) Zuständigkeit für das System (Mitgliedstaaten/Kommission)

Laut Artikel 23 Absatz 2 des Verordnungsentwurfs werden die Daten "im VIS im Namen der Mitgliedstaaten verarbeitet". Laut Artikel 23 Absatz 3 "benennt jeder Mitgliedstaat die Behörde, die als für die Verarbeitung Verantwortlicher gemäß Artikel 2 Buchstabe d der Richtlinie 95/46/EG tätig ist".

Die Kommission ist für den zentralen Teil (CS-VIS) und für die nationalen Schnittstellen zuständig, die Mitgliedstaaten übernehmen die Zuständigkeit für die nationalen Systeme. Die Dateneingabe erfolgt durch die zuständigen Behörden der Mitgliedstaaten, und gemäß Artikel 21 des Vorschlags haben nur diese Behörden das Recht, die Daten zu ändern.

Im Sinne der Richtlinie ist somit jeder Mitgliedstaat als Verantwortlicher zu betrachten.

Die Zuständigkeiten der Kommission hingegen sind nicht so klar präzisiert. Deshalb verdient die Rolle der Kommission als verantwortliche und/oder als Daten verarbeitende Instanz noch weitere Aufmerksamkeit.

Die Datenschutzgruppe betont daher, dass die Verantwortung der Mitgliedstaaten für das Funktionieren des Systems nicht ausschließt, dass auch die Kommission Mitverantwortung für bestimmte Aspekte übernimmt.

Die Datenschutzgruppe würde eine genauere Beschreibung der Rolle der Kommission beim VIS begrüßen, damit klar wird, bei wem die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung im VIS liegt, und damit die nationalen Datenschutzbehörden und der Europäische Datenschutzbeauftragte (EDPS) ihre Aufgaben wahrnehmen und ihre Aktivitäten besser koordinieren können, so dass bei der Überwachung des Systembetriebs keine Lücken entstehen können.

b) Kontrolle

Die Kontrollaufgaben verteilen sich auf die nationalen Kontrollstellen (für das mit der nationalen Schnittstelle verknüpfte nationale System) und den EDPS (für die Aufgaben, die unter die Zuständigkeit der Kommission fallen).

Eine präzisere Aussage zur Koordinierung von nationalen Datenschutzbehörden und EDPS ist erst möglich, wenn die angeforderte Klarstellung der Rolle der Kommission vorliegt.

c) Durchführung

Nach Auffassung der Datenschutzgruppe liegen nicht genügend Informationen über die verschiedenen laufenden Initiativen, Studien und Aktivitäten vor.

Wegen der erheblichen Auswirkungen auf bestimmte Grundrechte wie den Schutz personenbezogener Daten und wegen der noch ausstehenden Klarstellungen verbleibt eine Reihe sensibler Fragen, die nicht ausschließlich im Wege des Ausschussverfahrens entschieden werden sollten.

Daher sollte die letzte Entscheidung in allen Fragen mit möglichen Auswirkungen auf die Grundrechte und den Schutz personenbezogener Daten einem Instrument des Primärrechts vorbehalten bleiben, mit dem die sorgfältige Beurteilung der Verhältnismäßigkeit der in Rede stehenden Maßnahmen besser gewährleistet wäre.

Das Ausschussverfahren könnte hilfreich dabei sein, die technischen Schritte zur Umsetzung des in der oben genannten Weise festgelegten rechtlichen Vorgehens näher zu spezifizieren.

3. Schlussfolgerungen

Die Verordnung zum VIS ist als wichtiges Element des Raums der Freiheit, der Sicherheit und des Rechts gedacht.

Der Vorschlag der Kommission enthält recht komplexe Überlegungen und erfordert eine detaillierte und gründliche Analyse, die die Datenschutzgruppe in den vorausgehenden Abschnitten skizziert hat.

Die Datenschutzgruppe erinnert mit Genugtuung daran, dass der Vizepräsident der Kommission in seinen Reden vor den Datenschutzbehörden vom 21. Dezember 2004 und vom 18. Januar 2005 eine verstärkte Kooperation mit ihnen bei der Einrichtung eines neuen Datenschutzsystems mit neuen Datenbanken, neuen Wegen des Informationsaustauschs und neuen Formen der polizeilichen und justiziellen Zusammenarbeit zugesagt hat.

Bei dieser Gelegenheit hat die Kommission auch die Notwendigkeit eines kohärenten Aktionsplans betont und auf den Grundsatz der Verhältnismäßigkeit und die Auswirkungen der neuen Gesetzgebungsinitiativen auf die Grundrechte hingewiesen; die Einbindung der Datenschutzbehörden stelle dabei einen Mehrwert dar, den es zu nutzen gelte.

Dies vorausgeschickt bedankt sich die Datenschutzgruppe für die Aufmerksamkeit, die sie erhalten hat, und stellt fest, dass im Verordnungsentwurf konkrete Verbesserungen nötig sind. So muss zum einen ein systematischerer Überblick über alle laufenden Rechtsetzungstätigkeiten im Rahmen ähnlicher Initiativen und die damit zusammenhängenden Maßnahmen gegeben werden, und zum anderen muss erklärt werden, wie sich die Architektur eines komplexen Informationssystems auswirkt, das Daten über mehrere Millionen von Menschen enthalten wird.

Die Datenschutzgruppe bekräftigt ihre Bereitschaft, einen Beitrag zur zügigen Verabschiedung von Rechtsvorschriften zu leisten, in denen die Grundrechte der Personen, deren Daten erfasst werden, und das öffentliche Interesse in ausgewogener Weise miteinander in Einklang gebracht werden; dies wäre mittels weiterer Stellungnahmen möglich, die die Kommission hoffentlich anfordern wird, aber auch über andere geeignete Mechanismen der Kooperation.

In diesem Rahmen empfiehlt die Datenschutzgruppe die Abänderung des Verordnungsvorschlags auf der Grundlage der folgenden Anmerkungen:

1. Die Datenschutzgruppe betont, dass die im Vorschlag anvisierte Struktur des VIS zur Erfassung und Verarbeitung einer riesigen Menge personenbezogener Daten führen wird, was weit reichenden Konsequenzen für die Grundrechte der Betroffenen, insbesondere das Recht auf den Schutz der Privatsphäre haben wird. Es ist von größter Bedeutung, dass die Verarbeitung dieser Daten mit den Grundsätzen der Europäischen Menschenrechtskonvention, der Europäischen Charta der Grundrechte, der Konvention des Europarates Nr. 108 und insbesondere der Richtlinie 95/46/EG im Einklang steht.
2. Die strikte Einhaltung der Grundsätze der Notwendigkeit und der Verhältnismäßigkeit muss gewährleistet sein.

3. Der Zweck der Erfassung und Verarbeitung personenbezogener Daten im VIS muss im Einklang mit der Rechtsgrundlage des Vorschlags klar definiert und auf die Verbesserung der gemeinsamen Visapolitik begrenzt sein.

4. Es sollten nur die Kategorien von Daten verarbeitet werden, die für diesen Zweck unbedingt erforderlich sind; Datenkategorien, die zu diskriminierenden Auswirkungen führen können, wie z.B. die Staatsangehörigkeit des Antragstellers bei Geburt, sind auszuschließen.

5. Die Standardisierung der "Gründe für die Ablehnung der Visumerteilung" oder die Verwendung von "Verknüpfungen zu anderen Anträgen" sollten nur unter der Bedingung einer präzisen Definition der Datenkategorien erfolgen, damit der Ermessensspielraum bei der Ausübung hoheitlicher Befugnisse begrenzt wird.

6. Was die Kategorien von Betroffenen angeht, werden folgende Änderungen vorgeschlagen: Im VIS sollten keine Daten von Drittstaatsangehörigen gespeichert werden, die einen gültigen Aufenthaltstitel besitzen bzw. denen zu einem späteren Zeitpunkt ein solcher Aufenthaltstitel erteilt wird; der Parameter "andere Gruppenmitglieder" sollte nur auf der Grundlage einer präzisen und eindeutigen Definition dieses Begriffs aufgenommen werden; die Daten zu den "Personen, die die Einladung ausgesprochen haben", sollten nicht für die routinemäßige Durchführung der Visapolitik zur Verfügung stehen, sondern nur bei präzisen Anfragen im Zusammenhang mit Verstößen gegen die gesetzlichen Bestimmungen.

7. Die Datenschutzgruppe begrüßt, dass der Verordnungsentwurf eine Speicherung der Daten für eine Dauer von höchstens fünf Jahren vorsieht. In den Entwurf sollten jedoch noch weitere Selektivitätskriterien zur Datenspeicherung aufgenommen werden, die den verschiedenen in der Praxis auftretenden Situationen, den unterschiedlichen Arten von Visa und den verschiedenen Gründen für die Ablehnung der Visumerteilung Rechnung tragen.

8. Im Hinblick auf die Verarbeitung biometrischer Daten sind noch weitere Sicherheitsvorkehrungen zu treffen, insbesondere:

    a. Bei der Erhebung biometrischer Daten muss ein hoher Zuverlässigkeitsgrad gewährleistet sein, um insbesondere die Möglichkeit des "Identitätsdiebstahls" zu verhindern.

    b. Die Speicherung in einer zentralen Datenbank muss stark eingegrenzt und in jedem Fall streng überprüft werden.

    c. Die Verwendung für Identifizierungszwecke ist auf zwingend notwendige Fälle zu begrenzen, d.h. auf Fälle missbräuchlicher Nutzung des Verfahrens nach vorheriger Ablehnung der Visumerteilung. Dabei muss eine äußerst geringe Rate von Falschzurückweisungen gewährleistet sein, und für den Fall einer Zurückweisung sind angemessene Sicherheitsvorkehrungen zu treffen (Information über die Gründe und Instrumente zur nicht automatisierten Überprüfung der automatischen Zurückweisung).

9. Der Zugang zu den Daten ist auf die angegebenen Behörden zu begrenzen und muss im Einklang mit der Zielsetzung des Systems stehen. Der routinemäßige Zugriff auf die VIS-Daten muss den für die Durchführung der Visapolitik zuständigen Behörden vorbehalten bleiben. Anderen Behörden, insbesondere Organen der Strafverfolgung, sollte der Zugang nur auf Einzelfallbasis bei spezifischen Anfragen und mit den entsprechenden Sicherheitsvorkehrungen gewährt werden. Die technische

Ausgestaltung des Systems einschließlich der Interoperabilität muss so erfolgen, dass diese Einschränkungen nicht unterlaufen werden, insbesondere im Hinblick auf die geplanten Verknüpfungen mit dem SIS.

10. Die Rolle der Kommission im Zusammenhang mit dem VIS ist näher zu spezifizieren, damit insbesondere die nationalen Datenschutzbehörden und der Europäische Datenschutzbeauftragte ihre Aufsichtsfunktionen wahrnehmen und ihre jeweiligen Aktivitäten besser koordinieren können.

11. Die Bestimmungen zur Rolle der Kommission im Rahmen der Durchführung gemäß dem Ausschussverfahren (Artikel 39) sollten dahingehend präzisiert werden, dass sie nur bei Fragestellungen Anwendung finden, die keine Auswirkungen auf die Grundfreiheiten und den Schutz personenbezogener Daten haben.

Brüssel, 23. Juni 2005

Für die Datenschutzgruppe
Der Vorsitzende
Peter Schaar