11224/04/DE
WP 96

Stellungnahme Nr. 7/2004 zur Aufnahme biometrischer Merkmale in Visa und Aufenthaltstitel unter Berücksichtigung des Aufbaus des Visa-Informationssystems VIS

Angenommen am 11. August 2004

Stellungnahme Nr. 7/2004 zur Aufnahme biometrischer Merkmale in Visa und Aufenthaltstitel unter Berücksichtigung des Aufbaus des Visa-Informationssystems VIS

DIE GRUPPE FÜR DEN SCHUTZ VON 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 und auf Artikel 30 Absatz 1 Buchstabe c und Absatz 3 der Richtlinie,

gestützt auf seine Geschäftsordnung, insbesondere auf Artikel 12 und 14,

HAT FOLGENDE STELLUNGNAHME ABGEGEBEN:

EINFÜHRUNG

Der Europäische Rat bekräftigte auf seiner Tagung in Thessaloniki am 19. und 20. Juni 2003, es müsse „in der EU ein kohärenter Ansatz in Bezug auf biometrische Identifikatoren oder biometrische Daten verfolgt werden, der in harmonisierte Lösungen für Dokumente für Staatsangehörige von Drittländern, Pässe für EU-Bürger und Informationssysteme (VIS und SIS II) mündet". Er forderte die Kommission ferner auf, „entsprechende Vorschläge auszuarbeiten und mit dem Bereich Visa zu beginnen".

Ende September 2003 unterbreitete die Europäische Kommission Entwürfe für Verordnungen 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.). Am 18. Februar 2004 legte sie darüber hinaus einen Entwurf für eine Verordnung über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger vor.

Die vorgeschlagene Änderung bei der einheitlichen Gestaltung von Visa und Aufenthaltstiteln soll die Mitgliedstaaten hauptsächlich veranlassen, zum einen den Schlusstermin für die Umsetzung der Bestimmungen über die obligatorische Aufnahme des Lichtbilds in die Visummarke und die Aufenthaltstitel auf 2005 vorzuziehen (in den 2002 verabschiedeten Verordnungen war ursprünglich 2007 vorgesehen) und zum anderen künftig die Speicherung zweier biometrischer Merkmale auf einem hoch sicheren Datenträger (kontaktloser Chip) zwingend vorzuschreiben, und zwar ein digitales Gesichtsbild als wichtigstes biometrisches Identifikationsmerkmal sowie zwei digitale Fingerabdruckbilder vom flachen Finger. Der Begründung zufolge kann die Zahl der Fingerabdruckbilder gemäß den gesammelten Erfahrungen und der Qualität der Ergebnisse erhöht werden.

[1] ABl. L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/internal_market/privacy/law_de.htm

Die Interoperabilität der biometrischen Daten in Visa und Aufenthaltstiteln ist sicherzustellen, ferner sollten diese Daten in das Visa-Informationssystem VIS aufgenommen werden. Entsprechend sollten die digitalen Fingerabdrücke der im Schengener Abkommen genannten Personen in das Schengener Informationssystem der zweiten Generation SIS II überführt werden.

SIS II und VIS werden derzeit aufgebaut[2]. Im Zuge der Vorbereitungen für das europäische Visa-Informationssystem VIS verabschiedete der Rat am 19. Februar 2004 Schlussfolgerungen mit allgemeinen Leitlinien, die die Kommission bei der Gestaltung des Rechtsrahmens für den Aufbau und den Betrieb dieses Systems zu berücksichtigen hat. Laut diesen Schlussfolgerungen sollen später - im Einklang mit der Wahl der biometrischen Identifikationsmerkmale im Visabereich und unter Berücksichtigung des Ergebnisses der gegenwärtigen technischen Entwicklungen - biometrische Daten über die Visumantragsteller in das VIS aufgenommen werden.

Kurz danach ebnete der Europäische Rat in seiner Erklärung zum Kampf gegen den Terrorismus vom 25. März 2004 den Weg für die Optimierung der Informationssysteme als Teil der Bemühungen zur Verstärkung der Zusammenarbeit zwischen den Mitgliedstaaten. In der Erklärung wird die Notwendigkeit für rasches Handeln besonders hervorgehoben: „Die Kommission und der Rat werden dringend aufgefordert, die Beratungen über das Visa-Informationssystem (VIS) im Einklang mit den im Februar 2004 angenommenen Schlussfolgerungen voranzutreiben“.

Angesichts der Dringlichkeit verabschiedete der Rat am 8. Juni 2004 eine Entscheidung zur Einrichtung des Visa-Informationssystems (VIS)[3], die die Rechtsgrundlage für die Bereitstellung der entsprechenden Finanzmittel bildet.

In der Erklärung vom 25. März 2004 forderte der Europäische Rat die Kommission außerdem auf, Vorschläge zur Verbesserung der Interoperabilität europäischer Datenbanken vorzulegen und außerdem zu erkunden, welche Synergieeffekte zwischen bestehenden und künftigen Informationssystemen (SIS II, VIS und EURODAC) erzielt 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.

Alle Maßnahmen in diesem Bereich dürften sich erheblich auf die Grundrechte der betroffenen Personen auswirken, d. h. auf die Grundrechte aller Ausländer, die ein Visum beantragen, und das sind Zigmillionen Menschen. Bei künftigen Entscheidungen über die Einrichtung und Anwendung dieser neuen europäischen Informationssysteme sind die Datenschutzgrundsätze gebührend zu beachten, 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.

Vor diesem Hintergrund sollte die vorliegende Stellungnahme lediglich als vorläufig aufgefasst werden. Sie bezieht sich vornehmlich auf die Vorschläge für Verordnungen zur einheitlichen Gestaltung von Visa und Aufenthaltstiteln, mit deren Prüfung die

---

[2] Siehe Vorschlag der Kommission vom 11. Dezember 2003 für eine Verordnung des Rates über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger (KOM(2004) 116 endg.); darin geht es um die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II) und mögliche Synergien mit einem künftigen Visa-Informationssystem (VIS).

[3] Entscheidung des Rates vom 8. Juni 2004 zur Einrichtung des Visa-Informationssystems (VIS) (2004/512/EG).

Arbeitsgruppe formell von der Europäischen Kommission beauftragt wurde. Die Arbeitsgruppe äußert sich ferner zu den grundsätzlichen Aspekten, die der Rat in seinen Schlussfolgerungen vom 20. Februar 2004 über die Einrichtung eines Visa-Informationssystems (VIS) angesprochen hat, wohl wissend, dass die Ausschreibungen für das System bereits laufen. Diese Vorgehensweise entspricht dem Wunsch der Kommission und steht außerdem im Einklang mit Artikel 30 der Richtlinie 95/46/EG, wonach die Datenschutzgruppe ganz allgemein die Aufgabe hat, die Kommission bei allen Entwürfen von Gemeinschaftsmaßnahmen zu beraten, die sich auf die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten auswirken.

Die Arbeitsgruppe weist in diesem Zusammenhang ausdrücklich darauf hin, dass sie konsultiert werden muss, bevor Vorschläge in diesem Bereich erarbeitet werden, da sie ihre richtliniengemäßen Aufgaben nur dann erfüllen kann, wenn die laufenden Verfahren wirklich transparent sind.

Schließlich sei noch angemerkt, dass die Fragen hinsichtlich des eventuellen Aufbaus einer zentralen Datenbank mit biometrischen Daten von Passinhabern nicht Gegenstand dieser Stellungnahme ist und gesondert behandelt werden. Die Arbeitsgruppe wird sich in Kürze damit befassen.

1. ALLGEMEINE ERWÄGUNGEN ZUR AUFNAHME BIOMETRISCHER DATEN IN AUFENTHALTSTITEL UND VISA SOWIE ZUM VISA-INFORMATIONSSYSTEM VIS

Die Datenschutzgruppe hat Verständnis für das Bestreben, „Visa-Shopping“ (Mehrfachanträge bei mehreren Mitgliedstaaten) und „Identitätsdiebstahl“ zu bekämpfen, die höchst unangenehme Folgen für die Opfer haben.

Gleichwohl sind gemäß der Argumentation der Arbeitsgruppe in ihrem Arbeitspapier über Biometrie[4], das am 1. August 2003 angenommen wurde, bei der Aufnahme biometrischer Informationen in Visa und Aufenthaltstitel sowie bei der Verarbeitung der entsprechenden personenbezogenen Daten eine Reihe von Grundsätzen zu beachten, die sich auf den Schutz der Grundrechte und Grundfreiheiten von Personen beziehen, insbesondere was den Schutz ihrer Rechte bei der Verarbeitung ihrer personenbezogenen Daten anbelangt. Die Beachtung dieser Grundsätze ist außerordentlich wichtig bei der Verarbeitung biometrischer Daten, die zwangsläufig Informationen über konkrete Einzelpersonen liefern, zumal unter Umständen im Alltagsleben Spuren hinterlassen werden, ohne dass den Betroffenen klar ist, dass diese als Daten gesammelt werden können (digitale Fingerabdrücke sind ein anschauliches Beispiel).

Gemäß Artikel 6 der Richtlinie 95/46/EG dürfen personenbezogene Daten daher nur „für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden“. Darüber hinaus müssen sie dem Zweck angepasst sein, für den sie erhoben und weiterverarbeitet werden, sie müssen dafür erheblich sein und dürfen nicht darüber hinausgehen (Grundsatz der Zweckbindung).

Die Beachtung dieses Grundsatzes erfordert zunächst die eindeutige Bestimmung des Zwecks, für den die biometrischen Daten erhoben und verarbeitet werden. Aufgrund der

[4] MARKT/10595/03/DE – - WP 80, siehe http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp80_de.pdf.

Bestimmung dieses klaren und eindeutigen Zwecks kann dann beurteilt werden, ob die Aufnahme biometrischer Daten in Visa und Aufenthaltstitel gerechtfertigt ist, denn damit lässt sich prüfen, ob die Erhebung und Verarbeitung dieser Daten in einem angemessenen Verhältnis zur ursprünglichen Zweckbestimmung steht.

In dieser Frage verweist die Datenschutzgruppe auf den Zweckbindungsgrundsatz und betont, dass das zunehmende Interesse am Einsatz biometrischer Identifikationstechniken nach einer extrem sorgfältigen Prüfung der Rechtsmäßigkeit der Datenverarbeitung zum Zwecke der Identifikation verlangt, da biometrische Daten reale Risiken für die Betroffenen bergen, sollten sie verloren gehen oder zweckentfremdet werden. Insbesondere besteht die nicht unerhebliche Gefahr, dass eine Person, deren Fingerabdrücke digital erfasst wurden, ihre tatsächliche Identität sonst nicht preisgibt, vor allem wenn die Umstände, unter denen die Fingerabdrücke genommen wurden, keine hundertprozentige Zuverlässigkeit garantieren; die gestohlene Identität würde dann immer mit den betreffenden digitalen Fingerabdrücken in Verbindung gebracht werden. Angesichts solcher Risiken müssen diese Systeme unbedingt auf mögliche Schwachstellen bei der korrekten Identifizierung von Personen untersucht werden, bevor eine diesbezügliche Verarbeitung erfolgt (einige der dazu unterbreiteten Vorschläge sahen diese Möglichkeit nicht vor).

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.).

In dieser Hinsicht meldet die Datenschutzgruppe vor allem im Hinblick auf den Grundsatz der Verhältnismäßigkeit größte Vorbehalte gegen eine Lösung an, die über die rechtliche Prüfung vor Ausstellung der fraglichen Dokumente und über die Aufnahme biometrischer Daten in diese Dokumente hinausgeht. Die Vorbehalte richten sich gegen eine Lösung, die 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 Datenschutzgruppe weist ferner auf das mögliche Zuverlässigkeitsproblem im Zusammenhang mit dem Aufbau und der Abfrage einer derart umfangreichen Datenbank und auf den möglichen Schaden für die Betroffenen[5] hin.

Die Datenschutzgruppe möchte daher auch in Kenntnis gesetzt 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; außerdem möchte sie wissen, ob alternative Vorgehensweisen geprüft wurden oder geprüft werden können, die nicht mit derartigen Risiken verbunden sind.

---

[5] Die Möglichkeit, die Daten zu einer bestimmten Person in einer Biometriedatenbank aufzufinden, steht im umgekehrten Verhältnis zum gespeicherten Datenvolumen, selbst wenn die Suche automatisch erfolgt. In diesem Zusammenhang sei daran erinnert, dass über einen Zeitraum von fünf Jahren etwa 100 Millionen Visa-Anträge in VIS zu speichern wären.

Im Übrigen sind alle geeigneten Maßnahmen zur Ausschließung einer Zweckentfremdung der Daten zu ergreifen. Wie die Datenschutzgruppe bereits in der vorausgehenden Arbeitsunterlage ausgeführt hat, muss besonders streng geprüft werden, ob diese Biometriedatenbank 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.

Schließlich sei daran erinnert, dass die Voraussetzungen für derartige Einschränkungen und die Einschränkungen selbst auf einer klaren, präzisen Rechtsgrundlage beruhen müssen, wenn auch gemäß Artikel 13 der Richtlinie 95/46/EG in bestimmten Fällen Einschränkungen zulässig sind. Die Datenschutzgruppe vertritt die Auffassung, dass diese Erfordernisse nicht durch zu weit gefasste, unscharf formulierte Zielsetzungen umgangen werden dürfen. Mit anderen Worten: derartige Zielsetzungen sind nur dann legitim, wenn die oben genannten Grundsätze für jede einzelne Zielsetzung berücksichtigt werden.

2. SCHWIERIGKEITEN BEI DER UMSETZUNG EUROPÄISCHER VORHABEN ZUR AUFNAHME BIOMETRISCHER DATEN IN AUFENTHALTSTITEL UND VISA UND MIT DEM VISA-INFORMATIONSSYSTEM VIS

2.1 PROBLEME HINSICHTLICH DER VERORDNUNGSVORSCHLÄGE ZUR EINHEITLICHEN GESTALTUNG VON VISA UND AUFENTHALTSTITELN

2.1.1 MIT DER AUFNAHME BIOMETRISCHER MERKMALE IN VISA UND AUFENTHALTSTITEL VERFOLGTE ZIELE

- Die Aufnahme dieser Merkmale zielt darauf ab, „eine verlässlichere Verbindung zwischen dem Inhaber und dem Visum bzw. dem Aufenthaltstitel“ herzustellen[6], damit es möglich wird, die im Dokument enthaltenen Daten mit denen des Inhabers zu vergleichen, ohne auf eine Datenbank zuzugreifen.
- Längerfristig, d. h. wenn die entsprechende Infrastruktur beschlossen und aufgebaut ist, sollen „Nachforschungen in Datenbanken“[7] möglich werden.

Die Datenschutzgruppe hält die erste Zielsetzung für gerechtfertigt, vertritt aber die Auffassung, dass sie im Text der beiden Verordnungen verankert werden sollte, denn nur so kann die Liste der Personen erstellt werden, die auf die gespeicherten Daten zugreifen dürfen, und erst dann kann der Ausschuss nach Artikel 6 Absatz 2 der Verordnung 1683/95 die technischen Spezifikationen für die Aufnahme der betreffenden Daten in das Speichermedium und den Zugriff darauf festlegen.

Da die zweite Zielsetzung nicht näher umrissen ist, befürchtet die Datenschutzgruppe gravierende Kollisionen mit dem Verhältnismäßigkeitsgrundsatz, die mit den

---

6 Siehe Ziffer 3 Absatz 1 Ende der Begründungen zu den Vorschlägen für Verordnungen des Rates zur Änderung der Verordnungen 1683/95 und 1030/2002 des Rates über eine einheitliche Visagestaltung beziehungsweise die einheitliche Gestaltung des Aufenthaltstitels (KOM/2003/558 endg.). Siehe außerdem die Erwägungen 2 bzw. 3 der Verordnungsvorschläge.

7 a.a.O., Begründungen, Ziffer 3, Absatz 6, am Ende.

Schwierigkeiten zusammenhängen, die sich allein schon aus dem Aufbau des VIS (siehe unten) ergeben.

2.1.2 ALLGEMEINE MERKMALE DER ZWECKS EINHEITLICHER GESTALTUNG VON VISA UND AUFENTHALTSTITELN VERWENDETEN BIOMETRISCHEN VERFAHREN UND DIE FOLGEN UNBERECHTIGTER ZURÜCKWEISUNGEN

Die Datenschutzgruppe unterstreicht die Notwendigkeit eines hohen Zuverlässigkeitsgrads bei der Erhebung und Überprüfung biometrischer Daten. Unabhängig davon, wie konsequent das System optimiert wurde, sollten die verwendeten Technologien auf jeden Fall einen sehr geringen Prozentsatz an unberechtigten Zurückweisungen (Erkennungsfehler) garantieren, weil derartige Fehler gravierenden Folgen für die rechtmäßigen Inhaber der Dokumente haben.

Ferner hält die Datenschutzgruppe folgende Vorkehrungen für erforderlich:

- Maßnahmen, die den betroffenen Personen den Zugriff auf die Chipdaten ermöglichen, und sei es nur, damit sie den Inhalt insbesondere hinsichtlich ihrer eigenen biometrischen Merkmale überprüfen können (Artikel 12 der Richtlinie 95/46/EG);
- Garantien für Personen, die ein üblicherweise verwendetes biometrisches Merkmal, beispielsweise Fingerabdrücke, nicht aufweisen können (z. B. wegen Verlust oder Verletzung der Finger);
- Garantien, insbesondere für den Fall von Erkennungsfehlern bei Grenzkontrollen, 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); ferner Garantien, dass der Sachverhalt unverzüglich geklärt wird.

2.1.3 INTEROPERABILITÄT UND SICHERHEIT DES SPEICHERMEDIUMS FÜR VISA UND AUFENTHALTSTITEL

Aufgrund der nach Artikel 4a der beiden Verordnungsvorschläge vorgesehenen Interoperabilität erhalten neben den Behörden, die die Daten eingegeben haben, auch andere Behörden die Möglichkeit, auf die im Chip gespeicherten Bilddaten zuzugreifen. Da es sich bei dem Speichermedium um einen kontaktlosen Chip handelt, wünscht die Datenschutzgruppe, dass ihr rechtzeitig vor Verabschiedung der Vorschläge ein Papier vorgelegt wird, aus dem hervorgeht, dass die geplanten Spezifikationen für die Speicherung der Daten im Chip und für den Zugriff darauf Folgendes gewährleisten:

- dass die im Chip gespeicherten Daten nur von der Behörde geändert werden können, die für die Ausstellung des Dokuments zuständig ist, und zwar gemäß den Empfehlungen des jeweils in Erwägungsgrund 3 aufgeführten Dokuments Nr. 9303 der ICAO (von der ICAO zertifizierte elektronische Signatur);

- dass rechtlich nicht dazu befugte öffentliche Stellen oder private Stellen nicht ohne Wissen der betroffenen Person auf die Daten zugreifen dürfen; dabei wäre eine Verschlüsselung der Daten zwecks Gewährleistung der Vertraulichkeit

angebracht; der Lesezugriff auf den Speicherinhalt könnte darüber hinaus mit einem persönlichen Code geschützt werden, der nur dem Inhaber bekannt ist;

- dass jede zugriffsberechtigte Behörde nur Zugang zu den Informationen erhält, die zur Erfüllung ihres konkreten Auftrags nötig sind.

2.1.4 BESTIMMUNGEN ÜBER MASCHINENLESBARE INFORMATIONEN IN VISA UND AUFENTHALTSTITELN

Die Datenschutzgruppe ist der Auffassung, dass es Artikel 4 Unterabsatz 2 der Vorschläge zur Änderung der beiden Verordnungen, der die maschinenlesbaren Informationen begrenzt, an Klarheit mangelt:

> „[Die einheitliche Visummarke bzw. der Aufenthaltstitel] enthält keine maschinenlesbaren Informationen, außer wenn dies in der Verordnung oder im Anhang vorgesehen oder dem betreffenden Reisedokument zu entnehmen ist."

Deshalb wünscht die Datenschutzgruppe, dass diese Bestimmung:

- die personenbezogenen Informationen, die in maschinenlesbarer Form enthalten sein dürfen, ausdrücklich benennt;
- vorschreibt, dass die betroffenen Personen in Kenntnis gesetzt werden, welche Informationen ggf. nicht unmittelbar vom Dokument abgelesen werden können, womit die elektronisch gespeicherten Informationen gemeint sind;
- Maßnahmen vorschreibt, die es den betroffenen Personen ermöglichen, die Informationen bei Ausstellung des Dokuments und danach zu überprüfen, vor allem im Hinblick auf ihr Auskunfts- und Berichtigungsrecht.

2.2 SCHWIERIGKEITEN MIT DEM INFORMATIONSSYSTEM VIS

Die Datenschutzgruppe hat bereits in Ziffer 1 Vorbehalte angemeldet gegen den Aufbau einer zentralen Datenbank mit Biometriedaten aller Ausländer, die ein Visum oder eine Aufenthaltsgenehmigung beantragen, zwecks späterer Kontrolle illegaler Einwanderer, sofern sich diese Daten auf Spuren beziehen, wie sie jedermann im Alltag hinterlässt.

Ungeachtet dieser Vorbehalte und der noch ausstehenden Arbeiten der Kommission und des Ausschusses nach Artikel 5 Absatz 1 der Verordnung (EG) Nr. 2424/2001 des Rates vom 6. Dezember 2001 bezüglich der Regeln für den Betrieb von VIS möchte sich die Datenschutzgruppe wie folgt zu den Grundsätzen äußern, nach denen eine Datenbank dieser Art betrieben werden sollte.

2.2.1 ALLGEMEINE MERKMALE DES INFORMATIONSSYSTEMS VIS

- **Zielsetzung**

Die vom Rat verfolgten Ziele sind sehr weit gefasst; danach soll das System durch Informationsaustausch zwischen den Mitgliedstaaten nicht nur Visa-Shopping und

Identitätsbetrug verhindern, sondern auch der Identifizierung illegaler Einwanderer ohne Papiere dienen und zur inneren Sicherheit und zur Bekämpfung des Terrorismus beitragen. Manche dieser Zielsetzungen überschneiden sich mit denen des Schengener Informationssystems der zweiten Generation (SIS II), das sich ebenfalls im Aufbau befindet.

Aus diesem Grund ersucht die Datenschutzgruppe die Kommission, eine Bewertung dieser Zielsetzungen im Lichte von Ziffer 1 dieser Stellungnahme vorzunehmen, v. a., was die Verhältnismäßigkeit der geplanten Maßnahmen betrifft.

- **Zentral erfasste Daten und Zugriffsberechtigte**

Bisher wurde noch keine Liste der einzelstaatlichen Behörden erstellt, die auf die Daten in der zentralen Datenbank zugreifen dürfen.
Erst wenn die Verwendungszwecke des Systems definiert sind, kann die Art der Daten bestimmt werden, die auf europäischer Ebene gespeichert werden dürfen; dasselbe gilt für die Liste der zugriffsberechtigten Behörden und die Zugriffsbedingungen.

Die Datenschutzgruppe möchte schon jetzt auf zwei Datenarten aufmerksam machen, deren Vereinbarkeit mit dem Verhältnismäßigkeitsgrundsatz einer besonderen Prüfung bedürfen: die Standardbegründungen für eine Zurückweisung, die noch nicht europaweit zusammengestellt worden sind; ferner zwecks Aufdeckung illegaler Einwanderungsstrukturen die Informationen über Personen, die Einladungen aussprechen oder für die Unterkunfts- und Verpflegungskosten von Ausländern aufkommen.

- **Datenzugriff durch Drittländer**

Die Datenschutzgruppe hat den Eindruck gewonnen, dass einige Mitgliedstaaten der Auffassung sind, dass den Behörden in Drittländern der Zugriff auf Informationen der Datenbank VIS ermöglicht werden sollte.

Nach Ansicht der Datenschutzgruppe würde dies zu einer schwerwiegenden Kollision mit den Bestimmungen der Richtlinie 95/46/EG führen, insbesondere im Hinblick auf den Zweckbindungsgrundsatz und die Erfordernisse von Artikel 25 Absatz 1 hinsichtlich der Angemessenheit des Datenschutzesniveaus in den Ländern, in denen die Datenempfänger niedergelassen sind.

- **Speicherfrist für die Daten in der VIS-Datenbank**

Die Datenschutzgruppe ist der Meinung, dass aus Gründen der Verhältnismäßigkeit eine Aufbewahrungsdauer von fünf Jahren für Daten nicht die Mindest-, sondern die Höchstdauer darstellen sollte.

Die Datenschutzgruppe schlägt außerdem vor, anspruchsvollere Speicherkriterien festzulegen, die den jeweiligen, in der Praxis auftretenden Situationen Rechnung tragen. Beispielsweise könnten die Daten von Personen, die Anträge mehrfach oder in betrügerischer Weise unter falschen Namen gestellt haben, länger aufbewahrt werden als die Daten von Personen, denen Reisedokumente ausgestellt wurden und deren Reise problemlos verlaufen ist. Ein besonderes Kriterium könnte auch für Vielreisende

aufgestellt werden, wenn das Antragsverfahren dadurch beschleunigt werden kann. Solch vielfältigen Situationen sollte Rechnung getragen werden, wenn die einzelnen Speicherfristen für das VIS festgelegt werden.

Schließlich verweist die Datenschutzgruppe darauf, dass nach dem Grundsatz der Zweckbindung Daten von Personen gelöscht werden müssen, die die Staatsangehörigkeit eines Mitgliedstaats erworben haben oder über einen von einem Mitgliedstaat erteilten gültigen Aufenthaltstitel verfügen[8].

- **Benachrichtigung der Ausländer zum Zeitpunkt der Datenerhebung**

Die Datenschutzgruppe hat die Aufgabe, zur einheitlichen Anwendung der Richtlinie 95/46 beizutragen; deshalb wird sie im Lichte der VIS-relevanten Merkmale und unter Beachtung des in Artikel 10 und 11 der Richtlinie 95/46/EG verankerten Grundsatzes der Verarbeitung „nach Treu und Glauben" vorschlagen, welche Informationen die betroffenen Ausländer erhalten sollten.

- **Sicherheit des Systems**

Die Datenschutzgruppe misst dem Sicherheitsniveau, das bei der Entwicklung der VIS-Struktur erreicht werden muss, besondere Bedeutung bei. In Einklang mit Artikel 17 der Richtlinie 95/46/EG ist daher zu fordern, dass „die geeigneten technischen und organisatorischen Maßnahmen" ergriffen werden, „die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang - insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden - und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind".

Es ist unabdingbar, dass das im VIS zu erreichende Sicherheitsniveau unter Beachtung der Verarbeitungsrisiken und der Art der zu schützenden Daten festgelegt wird. Beispielsweise ist zu fordern, dass die Daten vor einer Übertragung im VIS-System verschlüsselt werden, damit unbefugte Dritte nicht darauf zugreifen können. Ferner müssen Zugriffsprotokolle geführt werden, insbesondere bei der Verarbeitung vertraulicher und/oder sensibler Daten, damit die zuständigen Behörden die Verarbeitung überwachen können; dieser Protokolle sind eine angemessene Zeit aufzubewahren und anschließend zu zerstören.

- **Interoperabilität von VIS und SIS II**

In der Erklärung vom 25. März 2004 zum Kampf gegen den Terrorismus forderte der Europäische Rat die Kommission auf, Vorschläge zur Verbesserung der Interoperabilität europäischer Datenbanken vorzulegen und außerdem zu erkunden, welche Synergieeffekte zwischen bestehenden und künftigen Informationssystemen (SIS II, VIS und EURODAC) erzielt 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.

[8] Siehe Artikel 25 des Schengener Durchführungsübereinkommens.

Die Datenschutzgruppe würde es begrüßen, wenn sie rechtzeitig zur genauen Ausgestaltung dieser Interoperabilität Stellung nehmen könnte, damit sie die möglichen Auswirkungen auf die Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten angemessen einschätzen kann. Sie bittet die Kommission daher um Benachrichtigung über ihre Vorschläge, damit sie diese Aspekte prüfen kann.

2.2.2 AUFGABE DER DATENSCHUTZKONTROLLSTELLEN

Die europäische Datenbank VIS sollte der Kontrolle des Europäischen Datenschutzbeauftragten unterstellt werden. Die Verarbeitungsoperationen in den einzelnen Staaten werden der Aufsicht der nationalen Datenschutzbehörden unterliegen.

Bei der Veranschlagung der Kosten für die Entwicklung dieser Systeme auf europäischer und einzelstaatlicher Ebene gilt es, die neuen Aufgaben zu berücksichtigen, mit denen die Kontrollstellen befasst werden, außerdem ist der Notwendigkeit einer Aufstockung ihrer Ressourcen Rechnung zu tragen, damit sie ihren gesetzlichen Auftrag effizient erfüllen können.

Es steht auch außer Frage, dass eine Koordinierung und Kooperation zwischen diesen Stellen nötig sein wird (bei Beschwerden, zwecks koordinierter Kontrollen vor Ort usw.). Für eine solche Zusammenarbeit sind ebenfalls angemessene Haushaltsmittel erforderlich.

Die Datenschutzgruppe ersucht die zuständigen Haushaltsbehörden, die nötigen Maßnahmen zu treffen, um die Ressourcen der Datenschutzbehörden entsprechend aufzustocken.

Da dem Europäischen Datenschutzbeauftragten die Zuständigkeit für die Überwachung der zentralen Komponente des Visa-Informationssystems VIS übertragen werden sollte, wäre die Zusammenarbeit zwischen ihm und den nationalen Kontrollstellen in allen Einzelheiten zu regeln, damit die einheitliche Anwendung der Datenschutzbestimmungen gewährleistet ist.

Die Datenschutzgruppe ersucht die Kommission, diese Frage zu prüfen und ihr die diesbezüglichen Schlussfolgerungen schnellstmöglich mitzuteilen.

Gemäß Artikel 46 der Verordnung (EG) Nr. 45/2001 arbeitet der Europäische Datenschutzbeauftragte mit den in Artikel 28 der Richtlinie 95/46/EG genannten einzelstaatlichen Kontrollstellen zusammen, ferner mit den im Rahmen von Titel VI („dritte Säule“) des Vertrags über die Europäische Union eingerichteten Datenschutzgremien. Er beteiligt sich außerdem an den Arbeiten der Datenschutzgruppe[9].

[9] Artikel 28 Absatz 6 der Richtlinie 95/46/EG erwähnt zwar den Datenschutzbeauftragten nicht, dies ist aber lediglich darauf zurückzuführen, dass die Institution des Datenschutzbeauftragten zum Zeitpunkt der Verabschiedung der Richtlinie noch nicht geschaffen war.

2.3 SCHLUSSFOLGERUNGEN – ROLLE DER ARTIKEL-29-DATENSCHUTZGRUPPE BEI DER SCHAFFUNG DER RECHTSGRUNDLAGE FÜR DIE VERARBEITUNG DER BETREFFENDEN PERSONENBEZOGENEN DATEN

Die Datenschutzgruppe kann nicht genug betonen, wie wichtig es ihr ist, bereits in der Vorbereitungsphase an der Entscheidungsfindung in besonderes schwierigen und sensiblen Fragen beteiligt zu werden. Wird sie von den geplanten Entscheidungen nicht oder zu spät informiert, kann sie die Kommission nicht zufrieden stellend beraten, was nach Artikel 30 der Richtlinie 95/46/EG ihre Aufgabe ist und womit sichergestellt werden soll, dass bei der betreffenden Datenverarbeitung ein ausgewogenes Verhältnis zwischen den Erfordernissen der öffentlichen Sicherheit und dem Schutz der nach Gemeinschafts- und nationalem Recht verliehenen persönlichen Freiheitsrechte erzielt wird.

Die Datenschutzgruppe betont, dass die Ausgewogenheit zwischen diesen unterschiedlichen Erfordernissen nur erreicht werden kann, wenn die Grundprinzipien des Datenschutzes beachtet werden; dies gilt besonders für die in Kapitel 1 genannten Grundsätze der Zweckbindung und der Verhältnismäßigkeit.

Darüber hinaus stellt die Datenschutzgruppe fest, dass sich die verschiedenen Arten der Verarbeitung im Rahmen der Initiativen zu grenzüberschreitenden Personenbewegungen[10], die eine Vernetzung mit sich bringen dürfte, hinsichtlich der Zweckbestimmung, der Art und der Merkmale voneinander unterscheiden und daher je nach ihrer Zuordnung zur ersten oder zur dritten Säule in unterschiedliche Zuständigkeitsbereiche fallen.

Aus diesem Grund äußerte die Datenschutzgruppe auf ihrer Sitzung am 23. und 24. November 2003 den Wunsch zur Einrichtung einer Unterarbeitsgruppe oder Taskforce, die die Gesamtentwicklung bei der Verarbeitung personenbezogener Daten in diesem Bereich untersuchen soll.

Da die Kommission nicht klar geäußert hatte, ob sie sich an der Einrichtung dieses Gremiums beteiligen würde, entschlossen sich die Mitglieder der Artikel-29-Datenschutzgruppe zusammen mit dem Europäischen Datenschutzbeauftragten und den Vertretern der Datenschutzkontrollstellen der dritten Säule, dieses Gremiums auf der Frühjahrskonferenz der europäischen Datenschutzbeauftragten in Rotterdam im April 2004 einzuberufen.

Das Gremium trat im Juni 2004 erstmalig in Brüssel zusammen und wird in regelmäßigen Abständen tagen. Es soll dafür Sorge tragen, dass die Mitglieder unmittelbar und umfassend über alle betreffenden Vorschläge und Initiativen informiert werden und sie entsprechend prüfen können.

Die Datenschutzgruppe verleiht ihrem Wunsch Ausdruck, dass besonders die Kommission und der Rat zielführend mit diesem Gremium zusammenarbeiten werden.

---

[10] Beispielsweise die Vorschläge für Verordnungen des Rates zur Änderung der Verordnungen über eine einheitliche Visagestaltung beziehungsweise die einheitliche Gestaltung des Aufenthaltstitels, die laufenden Arbeiten am Visa-Informationssystem VIS und seine Ausrichtung mit SIS II (Schengen II) und der mittlerweile (am 18. Februar 2004) von der Kommission angenommene Vorschlag für eine Verordnung des Rates über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger.

Brüssel, 11. August 2004

Für die Datenschutzgruppe

Der Vorsitzende

Peter SCHAAR