



WP134

Stellungnahme Nr. 3/2007 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Gemeinsamen Konsularischen Instruktion an die diplomatischen Missionen und die konsularischen Vertretungen, die von Berufskonsularbeamten geleitet werden, zur Aufnahme biometrischer Identifikatoren einschließlich Bestimmungen über die Organisation der Entgegennahme und Bearbeitung von Visumanträgen (KOM(2006)269 endg.)

Angenommen am 1. März 2007

Diese Arbeitsgruppe wurde durch Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist ein unabhängiges EU-Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG und in Artikel 14 der Richtlinie 97/66/EG aufgeführt.

Die Sekretariatsgeschäfte werden wahrgenommen von: Europäische Kommission, GD Justiz, Freiheit und Sicherheit, Direktion C (Ziviljustiz, Grundrechte und Unionsbürgerschaft), B-1049 Brüssel, Belgien, Büro LX-46 01/43.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

INHALTSVERZEICHNIS

1. HINTERGRUND	3
2. EINFÜHRUNG	4
3. EINLEITENDE BEURTEILUNG UND ALLGEMEINE VORAUSSETZUNG	5
4. VERARBEITUNG BIOMETRISCHER DATEN	6
A) WAHL DES RECHTSINSTRUMENTS	6
B) PFLICHT ZUR ABNAHME VON FINGERABDRÜCKEN: ERFASSUNGSPHASE	7
C) BEFREIUNG VON DER PFLICHT ZUR ABGABE VON FINGERABDRÜCKEN	8
<i>c1) Alter der Visumantragsteller</i>	8
<i>c2) Fälle, in denen keine Erfassung möglich ist</i>	9
5. SONSTIGE BESONDERE GARANTIEN	9
A) ZUSAMMENARBEIT MIT EXTERNEN DIENSTLEISTERN	10
B) GEMEINSAME VISUMSANTRAGSTELLEN	11
6. SCHLUSSFOLGERUNGEN	12

Stellungnahme Nr. 3/2007 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Gemeinsamen Konsularischen Instruktion an die diplomatischen Missionen und die konsularischen Vertretungen, die von Berufskonsularbeamten geleitet werden, zur Aufnahme biometrischer Identifikatoren einschließlich Bestimmungen über die Organisation der Entgegennahme und Bearbeitung von Visumanträgen (KOM(2006)269 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 1995¹,

gestützt auf Artikel 29 sowie Artikel 30 Absatz 1 Buchstabe c und Absatz 3 der Richtlinie, gestützt auf ihre Geschäftsordnung, insbesondere auf die Artikel 12 und 14,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Hintergrund

Vor dem Hintergrund der gemeinsamen Visumpolitik und einer verstärkten Integration der Auslandsvertretungen der Mitgliedstaaten soll mit dem aktuellen Vorschlag zur Änderung der Gemeinsamen Konsularischen Instruktion die Rechtsgrundlage für die obligatorische Erfassung biometrischer Identifikatoren von Personen, die ein Visum beantragen, geschaffen und die Organisation der Auslandsvertretungen geregelt werden.

Die Annahme einer Verordnung zur Änderung der Gemeinsamen Konsularischen Instruktion zur Aufnahme biometrischer Identifikatoren ist eine „Voraussetzung“ für die Anwendung des Visa-Informationssystems (VIS)², da diese Verordnung „den Rechtsrahmen für die Erfassung der erforderlichen biometrischen Identifikatoren vorgibt“.

Das Visa-Informationssystem wird eingerichtet, wenn die Verordnung des Europäischen Parlaments und des Rates über das VIS und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt, die die entsprechenden Regelungen für dieses System enthält, über die aber derzeit noch beraten wird, in Kraft getreten ist.

Der Aufbau einer zentralen Datenbank mit Daten zu Visumantragstellern, einschließlich Fingerabdrücken und digitalisierten Gesichtsbildern, sowie Daten zu Gruppenreisenden und zu Personen, die in den Zielländern der Antragsteller als Gastgeber fungieren, soll zu den grundlegenden Voraussetzungen für die Umsetzung einer gemeinsamen Visumpolitik und die Verwirklichung der Ziele gemäß Artikel 61 des Vertrags zur Gründung der Europäischen

¹ ABl. L 281 vom 23.11.1995, S. 31; siehe:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

² 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.), von der Kommission am 28. Dezember 2004 vorgelegt.

Gemeinschaft (EGV), insbesondere des freien Personenverkehrs in einem Raum der Freiheit, der Sicherheit und des Rechts, gehören.

Die Datenschutzgruppe hat 2004 und 2005 bereits zwei Stellungnahmen³ abgegeben, in denen sie ihre Bedenken zum Ausdruck brachte und eine Reihe von Vorschlägen unterbreitete, die bei der folgenden Analyse berücksichtigt wurden.

Der Europäische Datenschutzbeauftragte hat ebenfalls eine Stellungnahme zu dem Verordnungsentwurf abgegeben.⁴

Im Einklang mit Erwägungsgrund 9 wurde die Datenschutzgruppe um ihre Stellungnahme zu dem aktuellen Verordnungsentwurf ersucht.

2. Einführung

Mit der Gemeinsamen Konsularischen Instruktion (GKI) werden Mindestgepflogenheiten festgelegt, an die sich die konsularischen Vertretungen der Mitgliedstaaten bei der Ausstellung einheitlicher Visa halten müssen. Die GKI bildet das grundlegende Instrument zur Regelung der Verfahren und Bedingungen für die Erteilung von Visa für einen kurzfristigen Aufenthalt, von Durchreisevisa und von Visa für den Flughafentransit.

Die GKI wurde im Zuge der zwischenstaatlichen Schengen-Zusammenarbeit ausgearbeitet.

Die Schengen-Bestimmungen zur Visumpolitik haben eine Rechtsgrundlage erhalten und sind somit fester Bestandteil der Gemeinschaftsvorschriften. Mit dem Beschluss 1999/436/EG des Rates wird Artikel 62 Nummer 2 Buchstabe b EG-Vertrag als Rechtsgrundlage für die wichtigsten Bestimmungen der GKI festgelegt. Allerdings sah dieser Beschluss weder vor, dass die GKI in den EG-Vertrag einbezogen wird, noch enthielt er eine Rechtsgrundlage für die gesamte GKI.

Der derzeitige Wortlaut der GKI wird momentan neu gefasst, wobei die Bestimmungen des aktuellen Vorschlags zusammen mit den überarbeiteten Visavorschriften in die neue Fassung aufgenommen werden. Mit dem neuen Vorschlag, der ebenfalls in Form einer Verordnung vorgelegt werden wird, sollen eine Reihe von Bestimmungen, die während eines längeren Zeitraums entwickelt worden sind und größtenteils Handlungsanweisungen für Auslandsvertretungen enthalten, präzisiert und transparent gemacht werden.

In der neuen Fassung soll klarer zwischen Rechtsgrundsätzen und Verwaltungsvorschriften unterschieden werden, damit ein echter Visakodex der Gemeinschaft nach dem Muster des kürzlich angenommenen Schengener Grenzkodex entsteht. Das übergeordnete Ziel besteht darin, die Bestimmungen des Schengener Übereinkommens betreffend die Schaffung eines Raums ohne Grenzen an den Rechtsrahmen der Gemeinschaft anzupassen.

Nach dem Vorhaben der Kommission sollen im Zuge dieser Neufassung auch die bei der Beantragung von Visa auszufüllenden Vordrucke neu gestaltet werden; sie sollen vereinfacht und die bei der Antragstellung anzugebenden Kategorien und Daten verringert werden.

³ Dok. WP 96 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp96_de.pdf
Dok. WP 110 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp110_de.pdf
Schreiben vom 27. Juli 2006 an den Vorsitzenden des Strategischen Ausschusses für Einwanderungs-, Grenz- und Asylfragen. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2006_24_07_vis_en.pdf

⁴ Stellungnahme vom 27. Oktober 2006.
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2006/06-10-27_CCI_DE.pdf

3. Einleitende Beurteilung und allgemeine Voraussetzung

Der rechtliche Bezugsrahmen für die Einrichtung des VIS ist noch nicht vollständig festgelegt worden.

Somit hat die Datenschutzgruppe Gelegenheit, erneut ihre Auffassung darzulegen und ihre Erfahrung im Bereich des Schutzes der grundlegenden Menschenrechte (insbesondere des in Artikel 8 der EU-Grundrechtecharta verankerten Rechts auf Schutz personenbezogener Daten) in den Rechtsetzungsprozess einzubringen, der derzeit unter Beteiligung der zuständigen Gemeinschaftsorgane stattfindet.

Die gemeinsame Visumpolitik fällt vollständig in den Anwendungsbereich des Gemeinschaftsrechts. Den einheitlichen Bezugsrahmen für Aspekte, die die Menschenrechte und den Schutz personenbezogener Daten betreffen, bildet daher die Richtlinie 95/46/EG, welche die Grundsätze enthält, die im Hinblick auf eine rechtmäßige Verarbeitung von Daten zu beachten sind.

Die Datenschutzgruppe erinnert daran, dass in Artikel 6 der Richtlinie 95/46/EG der Grundsatz festgelegt ist, wonach personenbezogene Daten nur dann rechtmäßig verarbeitet werden können, wenn sie den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen.

In früheren Stellungnahmen zum VIS⁵ hatte die Datenschutzgruppe die Frage der Notwendigkeit und der Verhältnismäßigkeit einer so umfangreichen EU-Datenbank aufgeworfen und vor den damit verbundenen Risiken gewarnt, insbesondere den Risiken bezüglich der Erhebung von Millionen biometrischer Daten und deren Eingabe in das System.

Bei der Prüfung des Grundsatzes der Verhältnismäßigkeit im Zusammenhang mit der Visumerteilung und dem freien Personenverkehr stellt sich daher zwangsläufig die Frage nach der grundsätzlichen Legitimität der Erhebung biometrischer Identifikatoren, wobei sich dies nicht auf die Verarbeitungsverfahren und die technischen Aspekte der Erhebung dieser Daten beschränkt.

Bei der Eingabe und der Speicherung der Daten in der zentralen VIS-Datenbank ergeben sich sowohl hinsichtlich des Datenzugriffs als auch hinsichtlich falscher positiver Ergebnisse und/oder falscher negativer Ergebnisse ethische Probleme und Zuverlässigkeitsprobleme.

Die Datenschutzgruppe ist der Auffassung, dass sorgfältig abgewogen werden muss, welche Kategorien von Daten in das zentrale Datenbanksystem (C-VIS) eingegeben werden, und dass ferner zu prüfen ist, ob in die VIS-Verordnung ein Passus aufgenommen werden kann, der die erforderliche Flexibilität gewährleistet.

Ungeachtet des nach der Visumbeantragung erstellten Datensatzes sollte außerdem berücksichtigt werden, inwieweit sich die Aufnahme biometrischer Daten und die mögliche Verwendung von Fingerabdrücken auf die Menschenwürde und die Grundrechte auswirken, wenn Suchvorgänge im gesamten System durchgeführt werden. Solche biometrischen Daten könnten künftig durchaus als Suchschlüssel für das SIS und für Eurodac verwendet werden, wie im Zusammenhang mit der Systeminteroperabilität vorgeschlagen wurde.

Ferner sollten die Auswirkungen der verschiedenen Vorschläge, die derzeit erörtert und/oder ausgearbeitet werden, berücksichtigt werden. Diese Vorschläge sollen den für die nationale Sicherheit zuständigen Behörden neben dem Eurodac-Zugang auch den Zugang zum VIS

⁵ WP 110 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp110_de.pdf

ermöglichen. Damit dürfte sich das Risiko eines Missbrauchs erhöhen, und es dürfte leichter werden, das C-VIS für andere Zwecke zu nutzen als für die, für die die Daten erhoben und in das System eingegeben wurden.⁶

Daher sollten alle Entscheidungen über die auf den Standardvordrucken für Visumanträge zu erfassenden Kategorien von Daten zusammen mit den Entscheidungen über die in das C-VIS einzugebenden Daten getroffen werden. Um einen Missbrauch des Systems zu verhindern, sollte auch den Grundsätzen der Verhältnismäßigkeit und der Datensparsamkeit Rechnung getragen werden.

Der Rahmen für den diesbezüglichen Entscheidungsprozess, der beträchtliche Auswirkungen auf die Rechte des Einzelnen hat, sollte nicht zu eng gefasst sein. Es muss für eine demokratische Kontrolle der entsprechenden Verfahren gesorgt werden, und den Datenschutzbehörden muss ermöglicht werden, die ihnen in diesem Bereich anvertrauten Aufgaben wirksam zu erfüllen.

4. Verarbeitung biometrischer Daten

Der aktuelle Vorschlag sieht Folgendes vor: „Die Mitgliedstaaten erfassen ... biometrische Identifikatoren des Antragstellers, nämlich das Gesichtsbild und zehn Fingerabdrücke.“ Den Ausführungen der Kommission zufolge wird damit die Rechtsgrundlage geschaffen, die erforderlich ist, damit die Mitgliedstaaten die obligatorisch zu erfassenden biometrischen Identifikatoren der Visumantragsteller verarbeiten können.

Angesichts der möglicherweise negativen Folgen für die Betroffenen sollte die Verwendung biometrischer Daten zum Zwecke der Identifizierung beschränkt werden und diese Daten sollten entsprechend den Zielen des VIS nur in dieses System eingegeben werden, wenn es unbedingt erforderlich ist und die einschlägigen Grundsätze und Garantien eingehalten werden. Dies ist umso wichtiger im Falle von besonders schutzbedürftigen Gruppen wie Kindern und älteren Menschen.

a) Wahl des Rechtsinstruments

Im Interesse der Klarheit und Transparenz sollten die allgemeinen Grundsätze und Bedingungen, die für die Pflicht zur Erfassung von Fingerabdruckdaten gelten, in der VIS-Verordnung festgelegt werden, während der Verordnungsentwurf, der Gegenstand dieser Stellungnahme ist, schwerpunktmäßig Vorschriften zur Anwendung dieser Grundsätze enthalten und die praktischen Aspekte der Verarbeitung biometrischer Daten regeln sollte.

Wie bereits erwähnt, enthält der Verordnungsentwurf eine Reihe von Vorschlägen zur Änderung der konsolidierten Fassung der GKI, die das Verfahren zur Abnahme biometrischer Daten (Fingerabdrücke und Gesichtsbild) der Antragsteller legitimieren sollen. Dieses Verfahren ist in den diplomatischen Missionen und den konsularischen Vertretungen außerhalb der an dem System teilnehmenden Länder durchzuführen. Nach seiner Annahme wird der Entwurf vor dem Hintergrund der in Bezug auf die GKI bereits erlassenen Bestimmungen zu sehen sein, die sich hauptsächlich an „Praktiker“ richten und als Handlungsrichtschnur für die zu treffenden Maßnahmen gelten.

⁶ Die Datenschutzgruppe erinnert an ihre diesbezüglichen Bemerkungen und Bedenken, die sie in früheren Stellungnahmen von 2004 und 2005 dargelegt hat:
WP 110 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp110_de.pdf
Schreiben vom 27. Juli 2006 an den Vorsitzenden des Strategischen Ausschusses für Einwanderungs-, Grenz- und Asylfragen. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2006_24_07_vis_en.pdf

Als Rechtsinstrument kommt – wie im Falle des VIS – nur eine Verordnung in Frage, die im Mitentscheidungsverfahren unter Beteiligung des Europäischen Parlaments verabschiedet wird. Allerdings hat die Datenschutzgruppe Bedenken, dass die Verordnung als Katalog rein verwaltungstechnischer Anweisungen angesehen werden könnte.

In Anbetracht der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu Artikel 8 der Konvention vertritt die Datenschutzgruppe im Interesse der Klarheit und Transparenz die Auffassung, dass jeglicher Eingriff in das Recht auf Achtung des Privatlebens angemessen begründet und klar und allgemein verständlich formuliert werden muss, da mit dem betreffenden Verordnungsentwurf verbindliche Regeln eingeführt werden, die bestimmte Rechte einschränken.

Daher sollten alle Bestimmungen, die die Datenqualität, die Verhältnismäßigkeit der Maßnahmen und die Garantien für den Einzelnen betreffen, direkt in der VIS-Verordnung festgelegt werden. Dies gilt insbesondere für die Bestimmungen, die Folgendes betreffen: Kategorien personenbezogener Daten, die in das C-VIS einzugeben sind; Kategorien von Personen, die zur Abgabe von Fingerabdrücken verpflichtet sind bzw. die von dieser Pflicht befreit sind; Höchst- bzw. Mindestalter der Antragsteller; bestimmte Alternativverfahren; Identitätsmissbrauch und ungenaue Identifizierung aufgrund technischer Mängel; Speicherung der Daten; Garantien zugunsten der Personen, bei denen eine Abnahme von Fingerabdrücken physisch nicht möglich ist.

Außerdem muss die Abnahme der Fingerabdrücke transparent erfolgen, und der Betreffende muss entsprechend informiert werden, damit er sein Auskunftsrecht wahrnehmen kann.

b) Pflicht zur Abnahme von Fingerabdrücken: Erfassungsphase

Die Datenschutzgruppe weist darauf hin, dass präzise und verlässliche Rahmenbedingungen für die Entgegennahme der Anträge und die Erfassung der biometrischen Identifikatoren geschaffen werden müssen.

Dies ist vor allem von Bedeutung, wenn das betreffende Verfahren – wie im Vorschlag vorgesehen – im Rahmen der Kolokation oder der Zusammenarbeit mit externen Dienstleistern (Outsourcing) durchgeführt wird. In jedem Fall muss sichergestellt werden, dass die Identität jeder in einer Auslandsvertretung vorstelligen Person ordnungsgemäß festgestellt wird, bevor deren Fingerabdrücke abgenommen und den Identifizierungsdaten zugeordnet werden.

In diesem Zusammenhang ist hervorzuheben, dass Artikel 1 Absatz 1 nur allgemein auf die Beachtung der „einschlägigen Datenschutz- und Sicherheitsvorschriften“ Bezug nimmt; es ist jedoch wichtig, dass die Umstände, unter denen die Fingerabdrücke abgenommen werden, eine hundertprozentige Zuverlässigkeit garantieren.

Zu bedenken sind die möglichen Konsequenzen einer falschen Zuordnung der Identifizierungsdaten und der Fingerabdrücke bei der Erfassung der Fingerabdruckdaten, die bewusst herbeigeführt werden könnte, wenn die Person, deren Fingerabdrücke digital erfasst wurden, ihre tatsächliche Identität ansonsten nicht preisgibt. In einem solchen Fall würde die gestohlene Identität stets mit den betreffenden digitalen Fingerabdrücken in Verbindung gebracht werden.

Daher sollten unbedingt nur entsprechend geschulte und absolut verlässliche Mitarbeiter mit der Durchführung der oben genannten Maßnahmen betraut werden, die in jedem Fall unter der Aufsicht und Verantwortung des diplomatischen Personals des Mitgliedstaats, der den Visumantrag entgegennimmt, vorzunehmen sind.

c) Befreiung von der Pflicht zur Abgabe von Fingerabdrücken

c1) Alter der Visumantragsteller

Kinder unter sechs Jahren werden von der Pflicht zur Abgabe von Fingerabdrücken befreit sein; dagegen wurde nicht festgelegt, dass ältere Menschen ab einem bestimmten Alter von dieser Pflicht befreit sind. Die einschlägigen wichtigen Bestimmungen sind in der GKI-Verordnung als rein technische Vorgabe enthalten; sie sollten jedoch die Grundlage einer breiten politischen Debatte bilden. Die Aufnahme eines Verweises auf das Übereinkommen über die Rechte des Kindes ist als unerlässliche Voraussetzung dafür anzusehen, dass geprüft werden kann, ob die Würde des Kindes im Zusammenhang mit der genannten Pflicht gewahrt wird; ein solcher Verweis sollte nicht nur als Verwaltungsrichtschnur für das Erfassungsverfahren gelten.

Die Datenschutzgruppe ist der Ansicht, dass die Erfassung und die Verarbeitung der Fingerabdrücke – im Interesse der Würde des Betroffenen und der Zuverlässigkeit des Verfahrens – bei Kindern und älteren Menschen eingeschränkt werden sollten und dass die Altersgrenzen den für andere große biometrische Datenbanken der EU (insbesondere Eurodac) geltenden Altersgrenzen entsprechen sollten.

Es ist zu bedenken, dass in keiner wissenschaftlichen Literatur schlüssig nachgewiesen wird, dass die Fingerabdrucktechnologie bei Kindern oder älteren Menschen ausreichend zuverlässig ist.

Es sollte auch festgelegt werden, welche Fehlerspanne nach Aussage der Hersteller bei den in dem System (für die Dauer von fünf Jahren) gespeicherten Fingerabdrücken einzukalkulieren ist und welche Kontrollen (Treffer/kein Treffer) in den fünf Jahren (oder 48 Monaten), während der die betreffenden Fingerabdrücke gespeichert werden, durchzuführen sind. Dies gilt insbesondere für Kinder unter einem bestimmten Alter und für andere Personen, die an bestimmten Krankheiten leiden und/oder deren Zustand sich allmählich verschlechtert, da in diesen Fällen die Wahrscheinlichkeit einer falschen Zuordnung mit der Zeit zunimmt. Außerdem sollte festgelegt werden, wie in diesen Fällen die Achtung der Menschenwürde und der Grundfreiheiten gewährleistet wird.

Wegen unzureichender diesbezüglicher Untersuchungen und wegen fehlender verbindlicher Angaben der Hersteller zu den Stabilitäts- und Qualitätsniveaus, die eine zuverlässige Zuordnung zu C-VIS-Fingerabdrücken bei Kindern unter einem bestimmten Alter und/oder bei älteren Menschen über einem bestimmten Alter gewährleisten, ist die Datenschutzgruppe der Auffassung, dass die Festlegung neuer, anderer Altersgrenzen für die Befreiung von der Pflicht zur Abgabe von Fingerabdrücken nicht gerechtfertigt ist, dass sie die Würde der betroffenen Personen beeinträchtigt und dass sie angesichts des geringen Risikos im Zusammenhang mit den genannten Personengruppen und angesichts der Zwecke, für die das VIS konzipiert wurde, unnötig ist.

Der Entwurf sieht vor, dass die Abdrücke aller zehn Finger der Hände des Antragstellers abzunehmen sind, was zweifelsohne eine hohe Identifizierungsqualität gewährleistet; in diesem Zusammenhang sollte jedoch daran erinnert werden, dass in Eurodac – entsprechend dem für dieses System geltenden Kriterium für die Eingabe von Fingerabdruckdaten – lediglich Fingerabdrücke von Personen, die mindestens 14 und höchstens 80 Jahre alt sind, gespeichert werden.

Aufgrund der mangelnden Zuverlässigkeit der Fingerabdrücke sollten diese vorzugsweise ausschließlich zur Überprüfung der Identität erfasst werden, wobei die Möglichkeit der Erfassung solcher Daten (im Einklang mit den Verfahren und Garantien, die das innerstaatliche Recht vorsieht) im Bedarfsfall, zum Beispiel zur Verhinderung von Identitätsdiebstahl, unberührt bleibt. Insbesondere die unzuverlässigen Fingerabdruckdaten von Kindern unter 14 Jahren können nicht

zum Zwecke der Identifizierung verwendet werden; daher darf der Zugriff auf Daten, die gemäß Artikel 17 des VIS-Verordnungsvorschlags zum Zwecke der Identifizierung bereitgestellt werden, nicht genehmigt werden, was ausdrücklich festzulegen ist.

c2) Fälle, in denen keine Erfassung möglich ist

Ein weiterer wichtiger Aspekt ist die Festlegung der Kategorien von Personen, die von der Pflicht zur Abgabe von Fingerabdrücken und damit von der Verpflichtung zur Einhaltung der entsprechenden rechtlichen Bestimmungen befreit sein werden.

Wie das Europäische Parlament in seinem Bericht von 2005 und der Europäische Datenschutzbeauftragte in seiner Stellungnahme im Zusammenhang mit den Fällen, in denen eine Abnahme von Fingerabdrücken physisch unmöglich ist, bereits erwähnt haben, ist in verschiedenen Studien aufgezeigt worden, dass bei einem Bevölkerungsanteil von schätzungsweise bis zu 5 % keine Erfassung möglich ist (weil die Fingerabdrücke nicht lesbar sind oder weil die Betroffenen in einer Form behindert sind, die eine Erfassung ausschließt). Geht man davon aus, dass jährlich ungefähr 20 Millionen Visumanträge gestellt werden, so werden bis zu eine Million Personen nicht nach dem üblichen Verfahren erfasst werden können.

Die Datenschutzgruppe ist der Ansicht, dass einer derart großen Bevölkerungsgruppe angemessen Rechnung getragen werden sollte.

Sie ist außerdem der Auffassung, dass diese Personen nicht Opfer eines mangelhaften technischen Systems sein dürfen; zudem ist es verwerflich, dass sie stigmatisiert werden, weil ihre Fingerabdrücke unlesbar sind, und somit das Risiko besteht, dass ihr Visumantrag abgelehnt wird.

Als Alternativverfahren dürfte die Erfassung von Nachnamen, Geburtsnamen (früher verwendeten Nachnamen) und Vornamen sowie Angaben zum Geschlecht, Geburtsdatum, -ort und -land ausreichend sein, um den Erfordernissen gerecht zu werden. Daher sollte, wie bereits dargelegt, vorzugsweise die VIS-Verordnung um Ad-hoc-Bestimmungen ergänzt werden.

Die Datenschutzgruppe schlägt vor, dass statistisch ausgewertet werden sollte, wie viele Visumanträge nur deshalb abgelehnt wurden, weil eine Erfassung der betreffenden Personen nicht möglich war; außerdem sollte die Zahl der aus diesem Grund erfolgten Antragsablehnungen der Gesamtzahl der Ablehnungen aus anderen Gründen gegenübergestellt werden. Dies könnte in dem von der Kommission vorzulegenden Zweijahresbericht geschehen.

5. Sonstige besondere Garantien

Der GKI-Vorschlag muss den Anforderungen der EU-Datenschutzrichtlinie (95/46/EG) genügen, auch was die Transparenz, Kontrolle und Bewertung anbelangt.

Entsprechende Bestimmungen sind in dem GKI-Vorschlag und in der VIS-Verordnung enthalten.

Erwägungsgrund 14 des GKI-Vorschlags sieht Folgendes vor: „Die Kommission sollte zwei Jahre nach Inkrafttreten dieser Verordnung einen Bericht über deren Durchführung vorlegen, der sich mit der Umsetzung der Erfassung biometrischer Identifikatoren, dem Grundsatz des „Erstantrags“ und der Organisation der Entgegennahme und Bearbeitung von Visumanträgen befasst.“

Die vorstehende Bestimmung scheint lediglich eine technische Bewertung vorzusehen, während gemäß dem aktuellen VIS-Verordnungsentwurf (Artikel 34) die nationalen Datenschutz-Kontrollstellen und der Europäische Datenschutzbeauftragte im Rahmen der ihnen übertragenen Kontrollbefugnisse „sich gegenseitig bei Überprüfungen und Inspektionen [unterstützen], ...

Schwierigkeiten bei der Auslegung oder Anwendung dieser Verordnung [prüfen], ... harmonisierte Vorschläge im Hinblick auf gemeinsame Lösungen für etwaige Probleme aus[arbeiten] und ... erforderlichenfalls die Sensibilisierung für die Datenschutzrechte [fördern]“ (Artikel 35a).

Daher weist die Datenschutzgruppe nachdrücklich darauf hin, dass die Kohärenz gewahrt werden muss, und schlägt vor, den GKI-Vorschlag um eine Bestimmung mit folgendem Wortlaut zu ergänzen:

- **Erwägungsgrund 14a:** Die Kontrolle, Überwachung und Bewertung der Erfassung biometrischer Identifikatoren sollten nach Maßgabe der Artikel 34 und 35a der VIS-Verordnung betreffend die Überwachungstätigkeiten der nationalen Datenschutz-Kontrollstellen und des Europäischen Datenschutzbeauftragten erfolgen.

- **Artikel 1 Absatz 2 Nummer 1.2 Buchstabe a:** Am Ende dieses Absatzes sollte auf die Aufgaben Bezug genommen werden, die den nationalen Kontrollstellen gemäß Artikel 28 der EG-Richtlinie und gemäß Artikel 34 der VIS-Verordnung sowie im Rahmen der koordinierten Überwachung zukommen, mit der die nationalen Kontrollstellen und der Europäische Datenschutzbeauftragte gemeinsam betraut wurden, um die Rechtmäßigkeit der Verarbeitung personenbezogener Daten im Zusammenhang mit der Erfassung und Verwendung biometrischer Identifikatoren durch Überprüfungen, Inspektionen und Prüfung von Problemen bei der Ausübung der Rechte betroffener Personen und der Datenschutzrechte zu kontrollieren.

Die Datenschutzgruppe weist erneut darauf hin, dass für die Entgegennahme und Bearbeitung von Visumanträgen ein eindeutiges Regelwerk festgelegt werden sollte, insbesondere wenn es um die Verarbeitung biometrischer Daten geht. Die Grundsätze der Richtlinie 95/46/EG müssen in Bezug auf die Haftung bei der Datenverarbeitung uneingeschränkt Beachtung finden, vor allem wenn auf zwischenstaatlicher Ebene zusammengearbeitet werden soll und/oder private Stellen in Drittländern für die Wahrnehmung derart sensibler Tätigkeiten in Anspruch genommen werden.

Gemäß **Artikel 23 Absatz 2** des Verordnungsentwurfs werden „die Daten ... im VIS im Namen der Mitgliedstaaten verarbeitet“, und gemäß 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“. Der aktuelle Vorschlag sieht Folgendes vor: „Für die Organisation der Entgegennahme und Bearbeitung von Visumanträgen sind die einzelnen Mitgliedstaaten zuständig.“

Mit dem aktuellen Vorschlag soll daher ein Rechtsrahmen für die Organisation der Auslandsvertretungen der Mitgliedstaaten zum Zwecke der Anwendung des Visa-Informationssystems (für Tätigkeiten, die in der Praxis bereits teilweise durchgeführt werden) festgelegt werden.

Drei Möglichkeiten sind vorgesehen: Kolokation, gemeinsame Visumsantragstellen und Zusammenarbeit mit externen Dienstleistern. Die Datenschutzgruppe möchte vor allem zu den letzten beiden Optionen Empfehlungen aussprechen.

a) Zusammenarbeit mit externen Dienstleistern

Die Datenschutzgruppe schließt sich uneingeschränkt dem Standpunkt des Europäischen Datenschutzbeauftragten an, der nachdrücklich von einem Outsourcing an externe Dienstleister abgeraten und die begrenzten akzeptablen Optionen dargelegt hat.

Entsprechend der Organisation der Auslandsvertretungen sollte diese Möglichkeit als letzte Option angesehen werden. Sie dürfte zu viele Risiken in sich bergen, wenn sie nicht unter den

diplomatenstatusbedingten Schutz und die volle Verantwortung des betreffenden Mitgliedstaats fällt.

Es muss präzisiert werden, welche Stelle als für die Datenverarbeitung Verantwortlicher fungiert und welche rechtlichen Auflagen dem (den) Outsourcing-Anbieter(n) vorgeschrieben werden können, sofern Letzterer (Letztere) für die Verarbeitung zuständig und in einem Drittland niedergelassen ist (sind). Es bedarf besonderer Garantien in Bezug auf die Identifizierung der Antragsteller und die Abnahme der Fingerabdrücke, die nur in Gegenwart ausreichend qualifizierter Bediensteter der zuständigen Visumbehörden vorgenommen werden dürfen.

Daher sollte durch ein rechtliches Verbot sichergestellt werden, dass erfasste Daten nicht kopiert, in heruntergeladener Form gespeichert oder anderweitig von dem Dienstleister aufbewahrt werden. Außerdem sollten Bestimmungen zur Rückgabe der in Papierform erhobenen Daten an die jeweiligen Behörden festgelegt werden.

Der Vorschlag zur Änderung der GKI sollte ferner die Rechte der Visumantragsteller gegenüber den ausgelagerten Dienstleistern regeln und Bestimmungen über die Informationen enthalten, die die Dienstleister und Konsularbehörden den Antragstellern zur Verfügung stellen müssen.

Über die von den einzelnen Dienstleistern vorgelegten Anträge sollte Buch geführt werden, damit objektive Informationen vorliegen, die über die Zuverlässigkeit der Dienstleister Aufschluss geben.

b) Gemeinsame Visumsantragstellen

Auch in diesem Fall sollten klare Verfahren festgelegt werden, um den für die Verarbeitung Verantwortlichen zu ermitteln, um sicherzustellen, dass die Daten nach ihrer Erhebung nicht in der Visumsantragstelle verbleiben, sondern unverzüglich an die zuständigen nationalen Behörden zurückgehen, um das Verfahren zur Erfassung und Identifizierung der Antragsteller zu verbessern, damit gewährleistet ist, dass die Fingerabdrücke den richtigen Identifizierungsdaten zugeordnet werden, um wirksame Garantien für den Fall vorzusehen, dass bestimmte Maßnahmen getroffen werden müssen, und um zu ermöglichen, dass bei einem Identitätsmissbrauch die Daten des betreffenden Antragstellers und die Zuordnung zwischen seinen alphanumerischen Daten und den biometrischen Informationen sofort berichtigt und geändert werden.

Außerdem sollten geeignete Datenschutzmaßnahmen getroffen werden, um einen unbefugten Datenzugriff, das Duplizieren von Daten und sonstige unrechtmäßige Datenverarbeitungsvorgänge zu verhindern.

6. Schlussfolgerungen

Die Datenschutzgruppe empfiehlt Folgendes:

1. Grundsätzlich sollten die Kategorien von Daten, die in die zentrale Datenbank (C-VIS) eingegeben werden müssen, einer sorgfältigen Bewertung unterzogen werden. Nach Inkrafttreten des Visakodexes der Gemeinschaft muss ermittelt werden, welche Daten in das zentrale System C-VIS einzugeben sind, da viele von ihnen dann nicht mehr unbedingt erforderlich sind. Die VIS-Verordnung muss daher überprüft und die Verarbeitung personenbezogener Daten auf die Daten beschränkt werden, die für den Zweck, für den das VIS konzipiert wurde, unbedingt benötigt werden. Dies gilt insbesondere für die Grundsätze und Bedingungen, die die Erhebung von Fingerabdruckdaten regeln, da es sich hierbei um sensible Informationen handelt. Nach Auffassung der Datenschutzgruppe sollten die entsprechenden Bestimmungen der VIS-Verordnung (Artikel 6) dahingehend geändert werden, dass eine Einschränkung bezüglich der erhobenen und in das C-VIS eingegebenen personenbezogenen Daten festgelegt wird. So würden durch die Formulierung „*Ausschließlich die folgenden Daten werden in das C-VIS eingegeben: ...*“ weitere Änderungen des VIS nach Inkrafttreten des Visakodexes der Gemeinschaft vermieden.
2. Der Verordnungsentwurf sollte Vorschriften zur ordnungsgemäßen Anwendung dieser Grundsätze enthalten und die praktischen Aspekte der Verarbeitung biometrischer Daten regeln.
3. Bei der Aufnahme biometrischer Daten und der möglichen Verwendung von Fingerabdrücken im Zusammenhang mit Visumanträgen sollte den diesbezüglichen Auswirkungen auf die Menschenwürde und die Grundrechte Rechnung getragen werden.
4. Alle Entscheidungen über die auf den Standardvordrucken für Visumanträge zu erfassenden Kategorien von Daten sollten zusammen mit den Entscheidungen über die in das C-VIS einzugebenden Daten getroffen werden.
5. Um einen Missbrauch des Systems zu verhindern, sollte die Verwendung biometrischer Daten zum Zwecke der Identifizierung im Wege der Datensparsamkeit und der Verhältnismäßigkeit selektiv eingeschränkt werden.
6. Präzise und verlässliche Rahmenbedingungen sollten für die Entgegennahme der Anträge und die Erfassung der biometrischen Identifikatoren geschaffen werden.
7. Bei Kindern und älteren Menschen sollte die Erfassung und Verarbeitung der Fingerabdrücke eingeschränkt werden, und die Altersgrenzen sollten den für andere große biometrische Datenbanken der EU (wie Eurodac) geltenden Altersgrenzen angepasst werden.
8. Es sollte statistisch ausgewertet werden, wie viele Visumanträge nur deshalb abgelehnt wurden, weil eine Erfassung der betreffenden Personen nicht möglich war; die entsprechenden Statistiken sollten regelmäßig von der Kommission überprüft werden.
9. Im Einklang mit den einschlägigen Bestimmungen der VIS-Verordnung sollten, insbesondere durch Einfügung des Erwägungsgrunds 14a und Änderung von Artikel 1 Absatz 2 des Verordnungsentwurfs, eine angemessene Überwachung und Kontrolle gewährleistet werden.
10. Die Beauftragung privater Stellen (Outsourcing) mit der Bearbeitung von Visumanträgen sollte grundsätzlich vermieden werden; hiervon ausgenommen sind Call-Center-Aufgaben. Es bedarf besonderer Garantien, die im Falle einer Auslagerung der Erfassungsaufgaben gewährleisten,

dass die Haftung bei den zuständigen Visumbehörden in den Mitgliedstaaten verbleibt und die Verarbeitung unter strenger Aufsicht erfolgt.

Die Datenschutzgruppe ist davon überzeugt, dass die in ihrer Stellungnahme dargelegten Erwägungen angemessen berücksichtigt und in den Rechtsetzungsprozess einfließen werden, damit sichergestellt ist, dass die erwähnten Garantien vor Annahme der betreffenden Rechtsakte geschaffen werden.

Im Rahmen einer geeigneten Informationskampagne sollte die Öffentlichkeit über die betreffenden Themen informiert werden. Die Datenschutzgruppe ist bereit, hierzu in der für angemessen erachteten Weise beizutragen.

Brüssel, den 1. März 2007

Für die Datenschutzgruppe
Der Vorsitzende
Peter SCHAAR