DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für einen Beschluss des Rates über den Zugang der für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Prävention, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten (KOM(2005)600 endg.)

(2006/C 97/03)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 286286,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr,

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, insbesondere auf Artikel 41,

gestützt auf das am 29. November 2005 eingegangene Ersuchen der Kommission um Stellungnahme nach Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG

1.1. Vorbemerkungen

Die Kommission hat dem Europäischen Datenschutzbeauftragten (EDPS) den Vorschlag für einen Beschluss des Rates über den Zugang der für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Prävention, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten (im Folgenden „der Vorschlag") mit Schreiben vom 24. November 2005 übermittelt. Der Europäische Datenschutzbeauftragte betrachtet dieses Schreiben als Ersuchen um Beratung der Organe und Einrichtungen der Gemeinschaft nach Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001. Nach Auffassung des Datenschutzbeauftragten sollte in der Präambel des Beschlusses auf die vorliegende Stellungnahme verwiesen werden.

Der Europäische Datenschutzbeauftragte hält es für wichtig, zu diesem sensiblen Thema Stellung zu nehmen, da dieser Vorschlag unmittelbar an die Errichtung des VIS anschließt, das seiner Kontrolle unterliegen wird und zu dem er am 23. März 2005 seine Stellungnahme abgegeben hat ([1]). In dieser Stellungnahme wurde die Möglichkeit eines Zugangs von Strafverfolgungsbehörden bereits in Betracht gezogen (siehe unten); die Einführung neuer VIS-Zugangsrechte hat datenschutzrechtlich erhebliche Auswirkungen auf das System. Eine Stellungnahme zu dem vorliegenden Vorschlag ist daher ein unerlässlicher Folgeschritt zur ersten Stellungnahme.

1.2. Bedeutung des Vorschlags

a) *Kontext*

Der vorliegende Vorschlag hat nicht nur für sich betrachtet schon große Bedeutung, sondern ist auch wichtig, weil er der allgemeinen Tendenz folgt, Strafverfolgungsbehörden Zugang zu verschiedenen groß angelegten Informations- und Identifizierungssystemen zu gewähren. Dies wird unter anderem in der Mitteilung der Kommission vom 24. November 2005 über die Verbesserung der Effizienz der europäischen Datenbanken im Bereich Justiz und Inneres und die Steigerung ihrer Interoperabilität sowie der Synergien zwischen ihnen ([2]), insbesondere unter Nummer 4.6 dargelegt: *„Mit Blick auf das Ziel der Bekämpfung von Terrorismus und Kriminalität stellt der Rat nunmehr fest, dass der Umstand, dass die für die innere Sicherheit zuständigen Behörden keinen Zugang zu den Daten des VIS haben, einen Mangel darstellt. Das Gleiche ließe sich für alle einwanderungsbezogenen Daten des SIS II und die Eurodac-Daten feststellen."*

Der vorliegende Vorschlag könnte daher als Vorläufer für ähnliche Rechtsakte betrachtet werden, die im Zusammenhang mit anderen Datenbanken ausgearbeitet werden, und es ist außerordentlich wichtig, von Anfang an zu bestimmen, in welchen Fällen dieser Zugang zulässig sein könnte.

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

([2]) KOM(2005)597 endg.

b) *Auswirkungen eines neuen Zugangs zum VIS*

Der Europäische Datenschutzbeauftragte erkennt durchaus an, dass die Strafverfolgungsbehörden über die bestmöglichen Instrumente verfügen müssen, um Personen identifizieren zu können, die terroristische oder sonstige schwerwiegende Straftaten begehen. Er ist sich auch bewusst, dass VIS-Daten unter bestimmten Umständen für diese Behörden eine wesentliche Informationsquelle bilden können.

Es ist jedoch alles andere als belanglos, wenn Strafverfolgungsbehörden der Zugang zu im Rahmen der ersten Säule genutzten Datenbanken gewährt wird — auch wenn dies unter dem Gesichtspunkt der Terrorismusbekämpfung gerechtfertigt sein mag. Es darf nicht außer Acht gelassen werden, dass das VIS ein Informationssystem darstellt, das mit Blick auf die Umsetzung der europäischen Visumpolitik und nicht als Instrument der Strafverfolgung entwickelt wurde. Ein Routinezugang wäre ein schwerwiegender Verstoß gegen den Grundsatz der Zweckbeschränkung. Er hätte einen unverhältnismäßigen Eingriff in die Privatsphäre von Reisenden zur Folge, die zwecks Erlangung eines Visums der Verarbeitung ihrer Daten zugestimmt haben und davon ausgehen, dass ihre Daten nur zu diesem Zweck erfasst, abgefragt und übermittelt werden.

Da Informationssysteme für einen bestimmten Zweck eingerichtet werden und auf diesen Zweck ausgerichtete Schutzmaßnahmen, Sicherheitsvorkehrungen und Zugangsbedingungen vorgesehen werden, würde mit der Gewährung eines systematischen Zugangs zu einem anderen als den ursprünglich vorgesehenen Zweck, nicht nur gegen den Grundsatz der Zweckbeschränkung verstoßen, sondern dies könnte auch dazu führen, dass die vorgenannten Regelungen nicht mehr angemessen oder ausreichend sind.

Unter dem gleichen Gesichtspunkt betrachtet könnte eine derartige einschneidende Änderung des Systems die Ergebnisse der Folgenabschätzung (die sich nur mit dem Einsatz des Systems für den ursprünglich vorgesehenen Zweck befasste) hinfällig machen. Das gleiche gilt auch für die Stellungnahmen der Datenschutzbehörden. Es könnte geltend gemacht werden, dass der neue Vorschlag die Voraussetzungen für die von ihnen erstellte Analyse hinsichtlich der Einhaltung der Rechtsvorschriften ändert.

c) *Strikte Beschränkung dieses Zugangs*

Angesichts der obigen Ausführungen möchte der Europäische Datenschutzbeauftragte hervorheben, dass den Strafverfolgungsbehörden nur unter bestimmten Umständen und fallweise Zugang zum VIS gewährt werden kann und dass dies mit strengen Schutzmaßnahmen verbunden sein muss. Mit anderen Worten: Der Zugriff von Strafverfolgungsbehörden muss durch angemessene technische und rechtliche Mittel auf spezielle Fälle beschränkt werden.

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

Infolgedessen können die zentralen Anforderungen wie folgt zusammengefasst werden:

— Es sollte kein systematischer Zugang gewährt werden: In dem Beschluss muss sichergestellt werden, dass stets fallweise geprüft wird, ob der Zugang von im Rahmen der dritten Säule tätigen Behörden notwendig und verhältnismäßig ist. In dieser Hinsicht ist eine präzise Formulierung des Rechtsakts von höchster Bedeutung, damit kein Spielraum für eine extensive Auslegung bleibt, die wiederum zu einem Routinezugang führen würde.

— In den Fällen, in denen Zugang gewährt wird, müssen angesichts des sensiblen Charakters dieses Zugangs angemessene Schutzmaßnahmen und Bedingungen einschließlich einer umfassenden Datenschutzregelung für die Verwendung der Daten auf nationaler Ebene beschlossen werden.

1.3. **Erste Anmerkungen**

Der Europäische Datenschutzbeauftragte erkennt an, dass dem Datenschutz in dem vorgeschlagenen Rechtsakt große Aufmerksamkeit geschenkt wird, wobei insbesondere der Zugang auf bestimmte Fälle beschränkt und nur im Rahmen der Bekämpfung schwerwiegender Straftaten vorgesehen ist [1].

Als weitere positive Elemente sind speziell folgende zu nennen:

— Beschränkung auf bestimmte Arten von Straftaten, auf die im Europol-Übereinkommen Bezug genommen wird;

— Verpflichtung der Mitgliedstaaten, eine Liste der zugangsberechtigten Behörden zu erstellen und diese Listen zu veröffentlichen;

— eine zentrale Zugangsstelle pro Mitgliedstaat (und eine Spezialeinheit innerhalb von Europol), wodurch das Filtern der Anträge auf Zugang erleichtert und eine bessere Kontrolle ermöglicht wird;

— strenge Regeln für die Weitergabe von Daten nach Artikel 8 Absatz 5 des Vorschlags;

— Verpflichtung der Mitgliedstaaten und von Europol, Aufzeichnungen über die für Datenabfragen verantwortlichen Personen zu führen.

2. **ANALYSE DES VORSCHLAGS**

2.1. **Vorbemerkung**

Damit Behörden im Rahmen der dritten Säule Zugang gewährt werden kann, sollte der in den Bereich der ersten Säule fallende Hauptvorschlag zum VIS eine Überleitungsklausel enthalten, in der der mögliche Inhalt eines Rechtsakts der dritten Säule wie dieses Vorschlags im Wesentlichen festgelegt wird. Zu dem Zeitpunkt, als der Europäische Datenbeauftragte seine Stellungnahme zum VIS abgab, war noch keine Überleitungsklausel vorgesehen, so dass er sich dazu nicht äußern konnte. Daher gilt für alle nachstehenden Bemerkungen ein Vorbehalt bezüglich des Inhalts der Überleitungsklausel.

[1] Dies steht auch im Einklang mit den Schlussfolgerungen des Rates vom März und vom Juli 2005, in denen gefordert wurde, dass den für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten der Zugang zum VIS *„nur unter strikter Einhaltung der Vorschriften für den Schutz personenbezogener Daten"* gewährt wird.

2.2. **Zweck des Zugangs**

Die Bedingungen für den Zugang zum VIS müssen sorgfältig bestimmt werden, damit eine angemessene Beschränkung des Zugangs sichergestellt werden kann. Es ist zu begrüßen, dass nicht nur in dem vorgeschlagenen Beschluss selbst, sondern auch in der Begründung und in den Erwägungsgründen (siehe insbesondere Erwägungsgrund 7) deutlich herausgestellt wird, dass nur auf Einzelfallbasis Zugang gewährt werden soll.

Zu Artikel 5 des Vorschlags kann eine Anmerkung gemacht werden, die bei der Auslegung dieses Artikels als Orientierungshilfe dienen soll.

Artikel 5 beschränkt die Reichweite des Zugangs durch grundsätzliche Bedingungen:

b) Der Zugang zwecks Datenabfrage ist für die Prävention, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerwiegender Straftaten erforderlich;

c) der Zugang zwecks Datenabfrage ist in einem spezifischen Einzelfall erforderlich (…), und

d) aufgrund der vorliegenden tatsächlichen Anhaltspunkte bestehen berechtigte Gründe zu der Annahme, dass die Abfrage von VIS-Daten zur Prävention, Aufdeckung oder Untersuchung einer der genannten Straftaten beitragen würde.

Diese Bedingungen sind kumulativer Art, wobei die unter Buchstabe b aufgeführte Bedingung eher eine Definition des sachlichen Anwendungsbereichs darstellt. In der Praxis bedeutet dies, dass die um Zugang ersuchende Behörde mit einer schwerwiegenden Straftat nach Buchstabe b des Vorschlags befasst sein muss; es muss ein spezifischer Einzelfall nach Buchstabe c vorliegen. Darüber hinaus muss die Behörde gemäß Buchstabe d nachweisen können, dass in diesem spezifischen Einzelfall die Abfrage von VIS-Daten zur Prävention, Aufdeckung oder Untersuchung dieser Straftat beitragen wird.

Auch bei dieser Auslegung des Artikels 5 ist der Europäische Datenbeauftragte über die flexible Formulierung von Buchstabe d besorgt: „beitragen" ist eher zu weit gefasst. Es gibt zahlreiche Fälle, in denen VIS-Daten zur Prävention oder Untersuchung einer schwerwiegenden Straftat „beitragen" könnten. Der Europäische Datenbeauftragte ist der Auffassung, dass diese Abfrage „wesentlich" zur Prävention, Aufdeckung oder Untersuchung der betreffenden schwerwiegenden Straftat „beitragen" sollte, und schlägt vor, Artikel 5 dementsprechend zu ändern, um einen Zugang zu VIS-Daten in Abweichung vom Grundsatz der Zweckbeschränkung zu rechtfertigen.

Gemäß Artikel 10 sollte aus den Aufzeichnungen genau hervorgehen, zu welchem Zweck die Datenabfrage erfolgt. Die Angaben zum „Zweck" sollten auch die Elemente umfassen, aufgrund deren die VIS-Abfrage im Sinne von Artikel 5 Absatz 1 Buchstabe d erforderlich war. Dies würde dazu beitragen, dass bei allen Abfragen des VIS deren Notwendigkeit geprüft und das Risiko von Routinezugriffen verringert wird.

2.3. **Suchbegriffe in der VIS-Datenbank**

In Artikel 5 Absätze 2 und 3 ist ein zweistufiger Zugang zu VIS-Daten vorgesehen, bei dem ein Datensatz nur zugänglich wird, wenn auf der Grundlage des ersten Datensatzes ein Treffer erzielt worden ist. Der erste Datensatz ist jedoch sehr weit gefasst. Insbesondere kann die Relevanz von Daten wie der in Artikel 5 Absatz 2 Buchstaben e und i genannten Daten für den ersten Datensatz in Frage gestellt werden:

— Der „Zweck der Reise" scheint ein sehr allgemeiner Suchbegriff für eine effiziente Abfrage des Systems zu sein. Darüber hinaus besteht die Gefahr, dass ein Profil von Reisenden auf der Grundlage dieses Kriteriums erstellt wird.

— Was „Lichtbilder" anbelangt, so ist die Möglichkeit, eine derart umfangreiche Datenbank auf der Grundlage von Lichtbildern abzufragen, beschränkt; die mit solchen Abfragen erzielten Resultate weisen beim gegenwärtigen Stand der Technik eine unannehmbare Fehlerquote auf. Eine falsche Identifizierung hat für die betroffene Person äußerst schwerwiegende Folgen.

Daher fordert der Europäische Datenbeauftragte, dass die Daten nach Artikel 5 Absatz 2 Buchstaben e und i als ergänzende Informationen betrachtet werden, die erst zugänglich werden, wenn sich aus der ersten Abfrage ergibt, dass das System bereits Daten enthält, und dass sie in Artikel 5 Absatz 3 aufgenommen werden.

Alternativ könnte der beratende Ausschuss eine Beurteilung der Technologie für die Abfrage der Datenbank anhand von Lichtbildern vornehmen, und diese würde erst dann eingesetzt, wenn sie ausgereift ist und als hinreichend zuverlässig betrachtet werden kann.

2.4. **Anwendung auf Mitgliedstaaten, für die die VIS-Verordnung nicht gilt**

Die für die innere Sicherheit zuständigen Behörden von Mitgliedstaaten, die nicht am VIS beteiligt sind, können Zugang zum VIS zur Datenabfrage erhalten. Diese Behörden müssen die Abfrage über einen beteiligten Mitgliedstaat unter Einhaltung der Bedingungen nach Artikel 5 Absatz 1 Buchstaben b bis d (d.h. auf Einzelfallbasis) vornehmen und einen hinreichend begründeten schriftlichen Antrag vorlegen.

Der Europäische Datenschutzbeauftragte möchte darauf hinweisen, dass einige Bedingungen für die Verarbeitung über die Abfrage hinaus festgelegt werden müssen. Für die am VIS beteiligten Mitgliedstaaten gilt die Regelung, dass aus dem VIS abgerufene Daten im Einklang mit dem Rahmenbeschluss über den Datenschutz im Rahmen der dritten Säule verarbeitet werden müssen (siehe im Folgenden). Diese Bedingung sollte auch für die Mitgliedstaaten gelten, auf die die VIS-Verordnung nicht anwendbar ist, die jedoch die entsprechenden Daten abfragen. Das gleiche sollte auch hinsichtlich der Führung von Aufzeichnungen für künftige Kontrollen gelten. Der Europäische Datenschutzbeauftragte empfiehlt daher, in Artikel 6 des Vorschlags einen Absatz aufzunehmen, wonach Artikel 8 und 10 des Beschlusses auch für Mitgliedstaaten gelten, auf die die VIS-Verordnung nicht anwendbar ist.

2.5. **Datenschutzregelung**

a) *Anwendung des Rahmenbeschlusses über Datenschutz im Rahmen der dritten Säule*

Da der Zugang von für die innere Sicherheit zuständigen Behörden von der Zweckbestimmung des VIS abweicht, sollte er einer kohärenten Datenschutzregelung unterworfen werden, mit der ein hohes Maß an Schutz für die Daten gewährleistet wird, die aus dem VIS abgerufen und von nationalen Behörden oder Europol verarbeitet werden.

Nach Artikel 8 des Vorschlags erfolgt die Verarbeitung personenbezogener Daten im Sinne dieses Beschlusses nach Maßgabe des Rahmenbeschlusses des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (im Folgenden „der Rahmenbeschluss"). Hinsichtlich des Datenschutzes sollte der vorliegende Vorschlag also als *lex specialis* betrachtet werden, das das *lex generalis* (d.h. den Rahmenbeschluss) ergänzt oder präzisiert. So sind beispielsweise die Bestimmungen über die Weitergabe von Daten in diesem Vorschlag strenger und sollten eingehalten werden. Das gleiche gilt für die Gründe für den Zugang zu den Daten.

b) *Anwendungsbereich*

Der Europäische Datenschutzbeauftragte begrüßt es, dass die Datenschutzregelung des Rahmenbeschlusses für jede Verarbeitung von personenbezogenen Daten nach Maßgabe der vorgeschlagenen Verordnung gilt. Dies bedeutet, dass unabhängig davon, welche Behörden das VIS abfragen, das gleiche Datenschutzniveau gewährleistet ist.

Da in Artikel 2 ein funktionelles Kriterium herangezogen wird, um diese Behörden zu bestimmen („die Behörden der Mitgliedstaaten, welche für die Prävention, Aufdeckung oder Untersuchung von terroristischen Straftaten oder sonstigen schwerwiegenden Straften verantwortlich sind"), könnte diese Definition sowohl Nachrichtendienste als auch Strafverfolgungsbehörden umfassen. Nachrichtendienste, die das VIS abfragen, unterliegen daher grundsätzlich den gleichen datenschutzrechtlichen Verpflichtungen, was durchaus als positiv zu bewerten ist.

Da jedoch Zweifel an dieser Auslegung hinsichtlich der Anwendbarkeit des Rahmenbeschlusses auf Nachrichtendienste bei deren Zugang zu VIS-Daten auftreten könnten, schlägt der Europäische Datenschutzbeauftragte folgende Alternativformulierung vor:

„In den Fällen, in denen der Rahmenbeschluss (…) nicht anwendbar ist, stellen die Mitgliedstaaten ein Datenschutzniveau sicher, das zumindest dem durch den Rahmenbeschluss gewährleisteten Niveau entspricht".

c) *Kontrolle*

Was die Formulierung von Artikel 8 anbelangt, so sollte klargestellt werden, dass Absatz 1 die Verarbeitung von Daten im Hoheitsgebiet der Mitgliedstaaten betrifft. Die Absätze 2 und 3 enthalten genaue Angaben über ihren Anwendungsbereich (Datenverarbeitung durch Europol und durch die Kommission), und es sollte ausdrücklich angegeben werden, dass mit Absatz 1 ein anderer Fall geregelt wird.

Die Aufteilung der Kontrollkompetenzen entsprechend den jeweiligen Aktivitäten der verschiedenen Beteiligten folgt einem vernünftigen Ansatz. Es fehlt jedoch ein Aspekt, nämlich die Notwendigkeit eines koordinierten Ansatzes bei der Kontrolle. Der Europäische Datenschutzbeauftragte hat bereits in seiner Stellungnahme zum VIS Folgendes gestellt: *„Was die Kontrolle des VIS anbelangt, so sei ferner betont, dass die Kontrolltätigkeiten der nationalen Kontrollstellen und des EDPS bis zu einem gewissen Grad koordiniert werden sollten (…). In der Tat sind eine Harmonisierung in Bezug auf die Durchführung der Verordnung sowie die Ausarbeitung eines gemeinsamen Konzepts zur Lösung gemeinsamer Probleme unerlässlich.*

Artikel 35 [des VIS-Vorschlags] sollte daher eine entsprechende Bestimmung enthalten, wonach der EDPS mindestens einmal jährlich eine Sitzung mit allen nationalen Kontrollstellen einberuft."

Das Gleiche gilt auch für diese besondere Nutzung des VIS-Systems (in diesem Falle auch unter Einbeziehung der gemeinsamen Kontrollinstanz von Europol). Die Kontrolle sollte mit der Kontrolle des „VIS der ersten Säule" vollständig im Einklang stehen, da es sich um dasselbe System handelt. Darüber hinaus wird auch im Rahmen der Kontrolle anderer groß angelegter Informationssysteme wie Eurodac so verfahren, dass Koordinierungssitzungen mit allen an der Kontrolle Beteiligten abgehalten werden, die vom Europäischen Datenschutzbeauftragten einberufen werden.

Dem Europäischen Datenschutzbeauftragten ist bewusst, dass in dem Vorschlag, in dem auf die Rolle der künftigen, nach Artikel 31 des vorgeschlagenen Rahmenbeschlusses einzusetzenden Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten Bezug genommen wird, ein gewisses Maß an Koordinierung vorgesehen ist. Es ist jedoch nochmals darauf hinzuweisen, dass die Kontrolle selbst nicht unter das Mandat dieses beratenden Gremiums fällt.

Der Europäische Datenschutzbeauftragte schlägt vor, zusätzlich eine Bestimmung vorzusehen, wonach das vom Europäischen Datenschutzbeauftragten im Rahmen der Kontrolle des „VIS der ersten Säule" einberufene Koordinierungsgremium auch für gemäß dem vorliegenden Vorschlag verarbeitete Daten zuständig ist und dass zu diesem Zweck darin auch die gemeinsame Kontrollinstanz von Europol vertreten sein sollte.

2.6. **Eigenkontrolle**

Artikel 12 des Vorschlage sieht Überwachungssysteme für das VIS vor. Der Europäische Datenschutzbeauftragte ist der Auffassung, dass sich diese Überwachung nicht nur auf die Ergebnisse, Kostenwirksamkeit und Qualität des Dienstes, sondern auch auf die Einhaltung der Rechtsvorschriften insbesondere im Bereich des Datenschutzes erstrecken sollte. Artikel 12 sollte dementsprechend geändert werden.

Damit diese Eigenkontrolle im Hinblick auf die Rechtmäßigkeit der Verarbeitung ausgeübt werden kann, sollte es der Kommission ermöglicht werden, die nach Artikel 10 des Vorschlags geführten Aufzeichnungen zu verwenden. Dementsprechend sollte in Artikel 10 vorgesehen werden, dass diese Aufzeichnungen nicht nur zur Überwachung des Datenschutzes und zur Gewährleistung der Datensicherheit, sondern auch zu regelmäßigen Eigenkontrollen des VIS gespeichert werden sollten. Die Berichte über die Eigenkontrolle werden zur Wahrnehmung der Kontrollaufgaben des Europäischen Datenschutzbeauftragten und anderer Kontrollbeauftragter beitragen, denen die Auswahl ihrer vorrangigen Kontrollbereiche erleichtert wird.

3. SCHLUSSFOLGERUNG

Angesichts der obigen Ausführungen hebt der Europäische Datenschutzbeauftragte hervor, dass es von entscheidender Bedeutung ist, dass den für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten und Europol nur auf Einzelfallbasis und unter strengen Schutzmaßnahmen Zugang gewährt wird. Dieses Ziel wird im Vorschlag zwar auf insgesamt zufrieden stellende Weise erreicht, jedoch können — wie in dieser Stellungnahme vorgeschlagen — einige Verbesserungen vorgenommen werden:

— Eine Bedingung für den Zugang zum VIS nach Artikel 5 sollte sein, dass die Abfrage „wesentlich" zur Prävention, Aufdeckung und Untersuchung einer schwerwiegenden Straftat beiträgt und dass die nach Artikel 10 vorgeschriebenen Aufzeichnungen eine Bewertung dieser Bedingung in jedem Einzelfall ermöglichen sollten.

— Zwei der in Artikel 5 Absatz 2 genannten Suchbegriffe für den Zugang zum VIS, nämlich „Zweck der Reise" und „Lichtbilder", sollten nochmals geprüft werden und als ergänzende Information im Falle eines Treffers zugänglich gemacht werden.

— Unabhängig davon, welche Behörden VIS-Daten abfragen, sollte über die Abfrage hinaus das gleiche Datenschutzniveau gewährleistet sein. Artikel 8 und 10 sollten auch für Mitgliedstaaten gelten, auf die die VIS-Verordnung nicht anwendbar ist.

— Ein koordinierter Kontrollansatz sollte auch im Hinblick auf den in diesem Vorschlag vorgesehenen Zugang zum VIS gewährleistet sein.

— Die Bestimmungen über Überwachungssysteme sollten auch eine Eigenkontrolle der Einhaltung der Datenschutzanforderungen sicherstellen.

Geschehen zu Brüssel, am 20. Januar 2006

Peter HUSTINX

Europäischer Datenschutzbeauftragter