DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten zu dem

— Vorschlag für einen Beschluss des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (KOM(2005)230 endg.),

— Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (KOM(2005)236 endg.) und

— Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den Zugang von für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständigen Dienststellen der Mitgliedstaaten zum Schengener Informationssystem der zweiten Generation (SIS II) (KOM(2005)237 endg.).

(2006/C 91/11)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

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

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

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

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

gestützt auf das am 17. Juni 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. Hintergrund

Das Schengener Informationssystem (SIS) ist ein EU-weites IT-System, das als Ausgleichsmaßnahme infolge der Abschaffung der Kontrollen an den Binnengrenzen im Schengen-Raum eingerichtet wurde. Das SIS ermöglicht den zuständigen Behörden in den Mitgliedstaaten den Austausch von Daten für die Durchführung von Personen- und Sachkontrollen an den Außengrenzen oder in ihrem Hoheitsgebiet sowie für die Erteilung von Visa und Aufenthaltsgenehmigungen.

Das Schengener Durchführungsübereinkommen ist 1995 als zwischenstaatliches Abkommen in Kraft getreten. Das SIS als Bestandteil des Schengener Durchführungsübereinkommens wurde später durch den Amsterdamer Vertrag in den EU-Rahmen einbezogen.

Ein neues Schengener Informationssystem der zweiten Generation (SIS II) wird das derzeitige System ersetzen und damit die Erweiterung des Schengen-Raums auf die neuen EU-Mitgliedstaaten ermöglichen. Mit ihm werden auch neue Funktionalitäten in das System eingeführt. Die im zwischenstaatlichen Rahmen erarbeiteten Schengen-Bestimmungen werden in vollem Umfang in „klassische“ EU-Rechtsakte umgesetzt.

Die Europäische Kommission hat am 1. Juni 2005 drei Vorschläge für die Einrichtung des SIS II vorgelegt. Dazu gehören

— ein auf Titel IV des EG-Vertrags (Visa, Asyl, Einwanderung und andere Politiken betreffend den freien Personenverkehr) gestützter Verordnungsvorschlag, der die Aspekte der ersten Säule (Einwanderung) des SIS II regelt, nachstehend „Verordnungsvorschlag“ genannt;

— ein auf Titel VI des EU-Vertrags (polizeiliche und justizielle Zusammenarbeit in Strafsachen) gestützter Beschlussvorschlag, der die Nutzung des SIS für Zwecke der dritten Säule regelt, nachstehend „Beschlussvorschlag“ genannt;

— ein auf Titel V (Verkehr) gestützter Verordnungsvorschlag, der speziell den Zugang zum SIS durch Kfz-Zulassungsstellen betrifft; dieser Vorschlag wird gesondert behandelt (siehe Punkt 4.6).

In diesem Zusammenhang sei erwähnt, dass die Kommission in den kommenden Monaten eine Mitteilung zur Interoperabilität und Verbesserung der Synergien zwischen den einzelnen EU-Informationssystemen (SIS, VIS, Eurodac) vorlegen wird.

Das SIS II besteht aus einer zentralen Datenbank, dem so genannten „zentralen Schengener Informationssystem“ (CS-SIS), für dessen Betriebsmanagement die Kommission sorgt und das mit den von jedem Mitgliedstaat festgelegten nationalen Zugangsstellen (NI-SIS) verbunden ist. Die SIRENE-Behörden gewährleisten den Austausch von Zusatzinformationen (Informationen, die mit SIS-II-Ausschreibungen im Zusammenhang stehen, jedoch nicht im SIS II gespeichert sind).

Die Mitgliedstaaten liefern an das SIS II Daten über Personen, die zur Verhaftung, Übergabe oder Auslieferung ausgeschrieben sind, im Rahmen eines Gerichtsverfahrens oder zwecks verdeckter Registrierung oder gezielter Kontrolle gesucht werden oder denen an den Außengrenzen die Einreise verweigert werden soll, sowie über abhanden gekommene oder gestohlene Sachen. Ein im SIS II gespeicherter Datensatz, eine so genannte „Ausschreibung“, erlaubt den zuständigen Behörden die Identifizierung einer Person oder Sache.

Das SIS II weist neue Merkmale auf:) (für Europol, Eurojust, Staatsanwälte der Mitgliedstaaten, Kfz-Zulassungsstellen), Verknüpfungen zwischen Ausschreibungen, Aufnahme neuer Datenkategorien, einschließlich biometrischer Daten (Fingerabdrücke und Lichtbilder) sowie eine technische Plattform, die gemeinsam mit dem Visa-Informationssystem genutzt werden soll. Diese zusätzlichen Möglichkeiten haben jahrelang für Diskussionen über eine Verlagerung des Verwendungszwecks des SIS von einem Kontrollinstrument zu einem Melde- und Fahndungssystem gesorgt.

1.2. **Allgemeine Bewertung der Vorschläge**

1. Der Europäische Datenschutzbeauftragte (EDPS) begrüßt es, dass er auf der Grundlage von Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 konsultiert wurde. Angesichts des obligatorischen Charakters des Artikels 28 Absatz 2 sollte die vorliegende Stellungnahme in der Präambel der Rechtsakte erwähnt werden.

2. Die Vorschläge werden vom EDPS aus mehreren Gründen begrüßt. Die Umwandlung einer zwischenstaatlichen Struktur in europäische Rechtsinstrumente hat mehrere positive Auswirkungen: Der rechtliche Status der SIS-II-Vorschriften wird geklärt, dem Gerichtshof werden Zuständigkeiten für die Auslegung des Rechtsakts der ersten Säule übertragen und das Europäische Parlament wird — wenn auch ein bisschen spät — zumindest teilweise in den Prozess einbezogen.

3. Zudem ist ein Großteil der Bestimmungen in den Vorschlägen dem Datenschutz gewidmet, von denen einige willkommene Verbesserungen im Vergleich zur derzeitigen Situation darstellen. Genannt seien insbesondere die Maßnahmen zum Schutz der Opfer von Identitätsdiebstahl, die Ausweitung des Anwendungsbereichs der Verordnung 45/2001 auf Datenverarbeitungstätigkeiten der Kommission im Rahmen der Maßnahmen nach Titel VI sowie eine genauere Definition der Gründe für eine Ausschreibung von Personen zum Zwecke der Einreiseverweigerung.

4. Auch ist unverkennbar, dass auf die Formulierung der Vorschläge große Sorgfalt verwandt wurde; sie sind vielschichtig und spiegeln die ganze Komplexität des von ihnen geregelten Systems wider. Mit den meisten der in dieser Stellungnahme enthaltenen Bemerkungen wird bezweckt, bestimmte Vorschriften klarer zu gestalten oder zu ergänzen, ohne dass dabei eine komplette redaktionelle Überarbeitung erforderlich wäre.

Gleichwohl sind trotz dieser insgesamt positiven Beurteilung einige Vorbehalte angebracht; sie betreffen insbesondere folgende Punkte:

1. Es ist in vielerlei Hinsicht schwer zu erkennen, welche Absicht sich hinter dem Text verbirgt; in diesem Zusammenhang ist das Fehlen einer Begründung äußerst bedauerlich. Angesichts des sehr komplexen Charakters der Texte wäre dies eine wesentliche Voraussetzung gewesen kompliziert. Da sie fehlt, ist der Leser auf reine Vermutungen angewiesen.

2. Ferner ist zu bedauern, dass keine Studie zur Folgenabschätzung vorliegt. Der Umstand, dass die erste Version des Systems bereits funktioniert, ist dabei keine Rechtfertigung, da es zwischen beiden Systemen erhebliche Unterschiede gibt. Unter anderem hätten die Auswirkungen der Aufnahme biometrischer Daten stärker bedacht werden müssen.

3. Der Rechtsrahmen für den Datenschutz ist sehr komplex; er stützt sich auf die kombinierte Anwendung der *lex generalis* und der *lex specialis*. Es sollte dafür gesorgt werden, dass selbst im Falle der Erarbeitung spezifischer Rechtsvorschriften der bestehende Datenschutzrahmen der Richtlinie 95/46/EG und der Verordnung 45/2001 weiter in vollem Umfang gilt. Die kombinierte Anwendung mehrerer Rechtsinstrumente darf weder zu Widersprüchen zwischen einzelstaatlichen Regelungen in grundlegenden Fragen noch zur Schwächung des derzeitigen Datenschutzniveaus führen.

4. Der Zugang vieler neuer Behörden, die in keinerlei Bezug zu dem ursprünglichen „Zweck der Personen- und Sachkontrollen“ stehen, sollte an strengere Schutzklauseln gebunden sein.

5. Die Vorschläge stützen sich zu einem erheblichen Teil auf andere Rechtsinstrumente, die sich noch in der Vorbereitung befinden (teilweise liegen sogar noch keine Vorschläge vor). Der EDPS ist sich der Schwierigkeiten bewusst, die ein Rechtsetzungsprozess unter komplizierten, sich ständig verändernden Bedingungen mit sich bringt, doch hält er diesen Umstand angesichts der Folgen für die Betroffenen und der dadurch entstehenden Rechtsunsicherheit nicht hinnehmbar.

6. Die Aufteilung der Zuständigkeiten zwischen den Mitgliedstaaten und der Kommission ist ein wenig verschwommen. Hier ist größte Klarheit geboten, und zwar nicht nur für das reibungslose Funktionieren des Systems, sondern auch für seine umfassende Überwachung.

1.3. **Struktur der Stellungnahme**

Die Stellungnahme ist wie folgt strukturiert: Zunächst wird der für das SIS II geltende Rechtsrahmen geklärt. Anschließend werden die Zweckbestimmung des SIS II und die signifikanten Abweichungen vom derzeitigen System behandelt. Nummer 5 enthält Bemerkungen zu den jeweiligen Aufgaben der Kommission und der Mitgliedstaaten in Bezug auf den Betrieb des SIS II. In Nummer 6 geht es um die Rechte der Personen, deren Daten verarbeitet werden („Datensubjekte"), in Nummer 7 um die Überwachung auf nationaler Ebene und auf Ebene des EDPS sowie um die Zusammenarbeit zwischen den Kontrollinstanzen. Nummer 8 enthält einige Bemerkungen und Änderungsvorschläge in Bezug auf Sicherheitsfragen; in den Nummern 9 und 10 geht es um das Ausschussverfahren und die Interoperabilität. Abschließend werden die wichtigsten Schlussfolgerungen aus den einzelnen Punkten in einem Fazit zusammengefasst.

2. **EINSCHLÄGIGER RECHTSRAHMEN**

2.1. **Einschlägiger Datenschutzrahmen für das SIS II**

Als Rechtsrahmen für den Datenschutz werden in den Vorschlägen die Richtlinie 95/46/EG, das Übereinkommen Nr. 108 und die Verordnung (EG) Nr. 45/2001 herangezogen. Ferner sind noch andere Rechtsakte hier maßgeblich.

Um diesen Zusammenhang zu klären und nochmals auf die wichtigsten Bezugspunkte zurückzukommen, von denen wir bei unserer Prüfung ausgegangen sind, sei auf Folgendes verwiesen:

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

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

— In jüngerer Zeit wurden das Recht auf Achtung des Privatlebens und der Schutz personenbezogener Daten in Artikel 7 bzw. 8 der Charta der Grundrechte der Europäischen Union festgeschrieben. Nach Artikel 52 der Charta können diese Rechte Einschränkungen unterliegen, vorausgesetzt dass ähnliche Bedingungen erfüllt sind wie unter Artikel 8 EMRK.

— Artikel 6 Absatz 2 des EU-Vertrags bestimmt, dass die Union die Grundrechte achtet, wie sie in der EMRK gewährleistet sind.

Explizit gelten für die SIS-II-Vorschläge folgende drei Rechtsakte:

— Das Übereinkommen Nr. 108 des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (nachstehend *„Übereinkommen Nr. 108"*) enthält Grundprinzipien für den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Alle Mitgliedstaaten haben das Übereinkommen Nr. 108 ratifiziert. Es findet auch auf Tätigkeiten in den Bereichen Polizei und Justiz Anwendung. Derzeit bildet das Übereinkommen Nr. 108 zusammen mit der Empfehlung R (87) 15 des Ministerausschusses des Europarates über die Nutzung personenbezogener Daten im Polizeibereich vom 17. September 1987 die Datenschutzregelung für das SIS-Übereinkommen;

— 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 (ABl. L 281, S. 31) (nachstehend *„Richtlinie 95/46/EG"*). Es sei erwähnt, dass die nationalen Rechtsvorschriften zur Umsetzung der Richtlinie in den meisten Mitgliedstaaten auch die Datenverarbeitungstätigkeiten im Polizei- und Justizbereich erfassen.

— 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 (ABl. L 8, S. 1) (nachstehend *„Verordnung 45/2001"*).

Bei der Auslegung der Richtlinie 95/46/EG und der Verordnung 45/2001 muss teilweise die einschlägige Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte im Einklang mit der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) zugrunde gelegt werden. Das bedeutet, dass die Richtlinie und die Verordnung, soweit sie die Verarbeitung personenbezogener Daten regeln, bei der die Gefahr der Verletzung von Grundrechten und insbesondere eines Eingriffs in die Privatsphäre besteht, unter Berücksichtigung der Grundrechte ausgelegt werden müssen. Dies ergibt sich auch aus der Rechtsprechung des Europäischen Gerichtshofs. ([1])

([1]) In diesem Zusammenhang sei auf das Urteil des Gerichtshofs in der Rechtssache Österreichischer Rundfunk und andere (verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, Urteil vom 20. Mai 2003, Plenum, Slg. 2003 I-4989) verwiesen. Der Gerichtshof war mit einem österreichischen Gesetz befasst, das die Weitergabe von Einkommensdaten von Angestellten des öffentlichen Sektors an den Rechnungshof und ihre anschließende Veröffentlichung regelt. In seinem Urteil stellt der Hof einige aus Artikel 8 EMRK abgeleitete Kriterien auf, die bei der Anwendung der Richtlinie 95/46/EG herangezogen werden sollten, soweit diese Richtlinie bestimmte Einschränkungen des Rechts auf Privatsphäre vorsieht.

Am 4. Oktober 2005 hat die Kommission einen „Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden [1]“ (nachstehend „*Rahmenbeschlussentwurf*“) vorgelegt. Dieser Rahmenbeschluss soll das Übereinkommen Nr. 108 als Referenzrechtsakt für den SIS-II-Beschlussentwurf ersetzen, was sich voraussichtlich auf die einschlägige Datenschutzregelung auswirken wird (siehe Nummer 2.2.5).

2.2. **SIS II-Datenschutzregelung**

2.2.1. *Allgemeine Bemerkungen*

Die für das SIS II notwendige Rechtsgrundlage besteht aus unterschiedlichen Rechtsinstrumenten; gleichwohl — wie in den Erwägungsgründen festgestellt — „stellt das SIS II ein einziges Informationssystem dar, das auch als solches zu betreiben ist. Einige Bestimmungen dieser Rechtsinstrumente sind daher identisch.“

Die Struktur der beiden Dokumente ist im Wesentlichen gleich; in beiden Vorschlägen sind die Kapitel I-III nahezu identisch. Der Umstand, dass das SIS II als ein einziges Informationssystem mit zwei verschiedenen Rechtsgrundlagen zu betrachten ist, spiegelt sich auch in der — recht komplexen — Datenschutzregelung wider.

Die Datenschutzregelung wird zum Teil in den Vorschlägen selbst als eine „*lex specialis*“ festgelegt, die für jeden Bereich (Kommission, Mitgliedstaaten in Bezug auf die erste Säule, Mitgliedstaaten in Bezug auf die dritte Säule) durch ein gesondertes Referenzrecht („*lex generalis*“) ergänzt wird.

Angesichts dieser Struktur stellt sich die Frage, wie mit einem speziellen Regelwerk in seinem Verhältnis zur *lex generalis* zu verfahren ist. Hier sieht der EDPS in der *lex specialis* einen Anwendungsfall der *lex generalis*. Demzufolge muss die *lex specialis* stets mit der *lex generalis* im Einklang stehen; sie führt die *lex generalis* näher aus (bzw. konkretisiert oder ergänzt sie), ist aber nicht als Ausnahmeregelung für die *lex generalis* gedacht.

Was die Frage anbelangt, welches Recht auf spezifische Fälle angewendet werden soll, so gilt grundsätzlich, dass der *lex specialis* Vorrang einzuräumen ist. Sollte sie jedoch keine oder nur unklare Regelungen enthalten, so wäre die *lex generalis* heranzuziehen.

Nach dieser Struktur gibt es drei verschiedene Möglichkeiten der Kombination der *lex generalis* und der *lex specialis*. Sie lassen sich wie folgt beschreiben.

2.2.2. *Für die Kommission geltende Regelung*

Ist die Kommission beteiligt, so gilt die Verordnung 45/2001, auch in Bezug auf die Rolle des EDPS, sofern Tätigkeiten im Rahmen der ersten (Verordnungsvorschlag) oder der dritten Säule (Beschlussvorschlag) durchgeführt werden. Im Erwägungsgrund 21 des Beschlussvorschlags heißt es: „Die Verordnung (EG) Nr. 45/2001 (…) gilt für die Verarbeitung personenbezogener Daten durch die Europäische Kommission, wenn die Verarbeitung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise unter Gemeinschaftsrecht fallen. Die Verarbeitung personenbezogener Daten im SIS II fällt teilweise unter Gemeinschaftsrecht.“

Dafür gibt es praktische Gründe: Was die Kommission angeht, ließe sich nämlich nur sehr schwer bestimmen, ob die Daten im Rahmen von Tätigkeiten verarbeitet werden, die unter die Rechtsvorschriften der ersten oder der dritten Säule fallen.

Zudem ist die Anwendung eines einzigen Rechtsinstruments auf alle Tätigkeiten der Kommission im Zusammenhang mit SIS II nicht nur aus praktischer Sicht sinnvoller, sie sorgt auch für mehr Kohärenz (und gewährleistet damit nach Erwägungsgrund 21 des Verordnungsvorschlags eine „konsequente und einheitliche Anwendung von Vorschriften zum Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten“). Der EDPS begrüßt daher, dass die Kommission anerkannt hat, dass die Verordnung 45/2001 auf alle von der Kommission im SIS II durchgeführten Datenverarbeitungstätigkeiten anzuwenden ist.

2.2.3. *Für die Mitgliedstaaten geltende Regelung*

Was die Mitgliedstaaten betrifft, so ist die Situation komplexer. Die Verarbeitung personenbezogener Daten in Anwendung des Verordnungsvorschlags ist sowohl im Verordnungsvorschlag selbst als auch in der Richtlinie 95/46/EG geregelt. Aus dem Erwägungsgrund 14 des Verordnungsvorschlags geht eindeutig hervor, dass die Richtlinie als *lex generalis*, die SIS-II-Verordnung hingegen als *lex specialis* zu betrachten ist. Das hat eine Reihe von Auswirkungen, die nachstehend ausführlich dargelegt sind.

Für den Beschlussvorschlag gilt als Referenzregelwerk (*lex generalis*) das Übereinkommen Nr. 108, was in einigen Punkten zu erheblichen Unterschieden zwischen den Datenschutzregelungen für Aspekte der ersten und der dritten Säule führen kann.

2.2.4. *Auswirkung auf das Datenschutzniveau*

Zu dieser Regelung des Datenschutzes weist der EDPS generell auf Folgendes hin:

— Die Anwendung des Verordnungsvorschlags als *lex specialis* für die Richtlinie 95/46/EG (und analog dazu des Beschlussvorschlags als *lex specialis* für das Übereinkommen Nr. 108) darf auf keinen Fall zu einer Schwächung des im Rahmen der Richtlinie oder des Übereinkommens gewährleisteten Datenschutzniveaus führen. Der EDPS wird hierzu entsprechende Empfehlungen abgeben (siehe zum Beispiel: das Recht, Rechtsbehelfe einzulegen).

[1] (KOM(2005) 475 endg.).

— Ebenso wenig darf die kombinierte Anwendung von Rechtsinstrumenten dazu führen, dass das durch das geltende Schengener Durchführungsübereinkommen gewährleistete Datenschutzniveau sinkt (siehe zum Beispiel nachstehende Bemerkungen zu Artikel 13 der Richtlinie 95/46/EG).

— Durch die aufgrund der Struktur des EU-Rechts notwendige Anwendung zweier verschiedener Rechtsinstrumente darf es nicht dazu kommen, dass es je nach Art der betreffend eine Person verarbeiteten Daten zu ungerechtfertigten datenschutzrechtlichen Unterschieden kommt. Das muss so weit wie möglich verhindert werden. Die nachstehenden Empfehlungen sollen ebenfalls dazu beitragen, die Kohärenz so weit wie möglich zu verbessern (siehe zum Beispiel: die Befugnisse der nationalen Kontrollinstanzen).

— Der Rechtsrahmen ist so komplex, dass er bei der praktischen Anwendung höchstwahrscheinlich zu Verwirrungen führen wird. In bestimmten Fällen ist die Wechselwirkung von *lex generalis* und *lex specialis* schwer zu erkennen; es wäre daher nützlich, diesen Aspekt in den Vorschlägen klarzustellen. Zudem ist der Vorschlag der GK- Schengen in ihrer Stellungnahme vom 27. September 2005, zu der für das SIS II vorgeschlagenen Rechtsgrundlage ein „Vademecum" zu erarbeiten, das alle im Zusammenhang mit dem SIS II bestehenden Rechte aufführt und eine eindeutige Rangfolge der anwendbaren Rechtsvorschriften vorgibt, in diesem komplexen rechtlichen Umfeld sehr hilfreich.

Die vorliegende Stellungnahme soll also dazu beitragen, ein hohes Maß an Datenschutz, Kohärenz und Klarheit zu gewährleisten, um dem Datensubjekt die erforderliche Rechtssicherheit zu geben.

2.2.5. *Auswirkungen des Rahmenbeschlussentwurfs auf den Datenschutz im Rahmen der dritten Säule*

Das Übereinkommen Nr. 108, das als Datenschutz-Referenzregelwerk für den SIS-II-Beschlussentwurf gilt, wird durch den Rahmenbeschlussentwurf über den Datenschutz im Rahmen der dritten Säule ersetzt werden. ([1]) Dies wird nicht im Vorschlag erwähnt, ergibt sich jedoch aus dem vorgeschlagenen Rahmenbeschlussentwurf. Dort heißt es in Artikel 34 Absatz 2: „Bezugnahmen auf das Übereinkommen Nr. 108 des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten sind als Bezugnahmen auf diesen Rahmenbeschluss zu verstehen." Der EDPS wird im Laufe der nächsten Wochen eine Stellungnahme zu dem Rahmenbeschlussentwurf vorlegen, wird darauf in dieser Stellungnahme inhaltlich jedoch nicht näher eingehen. Für die Fall, dass die Anwendung des Rahmenbeschlusses jedoch ernsthafte Auswirkungen auf die SIS-II-Datenschutzregelung hätte, würde in der Stellungnahme darauf hingewiesen.

2.2.6. *Anwendung von Artikel 13 der Richtlinie 95/46/EG und von Artikel 9 des Übereinkommens Nr. 108*

Aufgrund von Artikel 13 der Richtlinie 95/46/EG und Artikel 9 des Übereinkommens Nr. 108 haben die Mitgliedstaaten die Möglichkeit, Rechtsvorschriften zu erlassen, um die darin vorgesehenen Pflichten und Rechte zu beschränken, sofern eine solche Beschränkung zur Wahrung anderer wichtiger Interessen (z.B. Sicherheit des Staates, Landesverteidigung, öffentliche Sicherheit) notwendig ist. ([2])

In den Erwägungsgründen des Verordnungs- und des Beschlussvorschlags wird darauf hingewiesen, dass diese Möglichkeit von den Mitgliedstaaten bei der Anwendung der vorgeschlagenen Rechtsakte auf innerstaatlicher Ebene genutzt werden könnte. In diesem Falle sollte eine doppelte Voraussetzung erfüllt sein: Die Anwendung von Artikel 13 der Richtlinie 95/46/EG muss im Einklang mit Artikel 8 EMRK erfolgen und darf nicht zu einer Schwächung des bestehenden Datenschutzniveaus führen.

Dies ist noch wichtiger im Falle des SIS II, da das System verlässlich sein muss. Da die Mitgliedstaaten die Daten gemeinsam nutzen, muss es eine Möglichkeit geben, hinreichende Klarheit darüber zu erlangen, wie diese auf nationaler Ebene verarbeitet werden.

In diesem Zusammenhang gibt insbesondere ein Element Anlass zu Besorgnis; dies hängt damit zusammen, dass die Vorschläge zu einer Schwächung des bestehenden Datenschutzniveaus führen könnten. Nach Artikel 102 des Schengener Durchführungsübereinkommens ist ein System zu schaffen, bei dem die Nutzung von Daten — sogar in den einzelstaatlichen Rechtsvorschriften — streng geregelt und scharf begrenzt ist („Jede Nutzung der Daten, die den Absätzen 1 bis 4 nicht entspricht, wird nach dem nationalen Recht der Vertragspartei als Zweckentfremdung bewertet."). Sowohl in der Richtlinie 95/46/EG als auch im Übereinkommen Nr. 108 ist jedoch vorgesehen, dass Ausnahmen beispielsweise vom Grundsatz der Zweckbindung in das einzelstaatliche Recht aufgenommen werden können. Würde dies getan, so ergäbe sich daraus ein Widerspruch zur derzeitigen Regelung im Schengener Durchführungsübereinkommen, wonach das einzelstaatliche Recht nicht vom Kerngrundsatz der Zweckbindung und der Nutzungsbeschränkung abweichen darf.

Die Annahme des Rahmenbeschlusses würde nichts an der folgenden Feststellung ändern: Das Problem besteht weniger darin sicherzustellen, dass die Daten im Einklang mit dem Rahmenbeschluss verarbeitet werden, als darin, den Grundsatz der Zweckbindung für die Verarbeitung von SIS-II-Daten weiterhin strikt zu wahren.

([1]) Er wird ferner die allgemeine Datenschutzregelung des Schengener Durchführungsübereinkommens (Artikel 126 bis 130) ersetzen. Diese Regelung gilt nicht für das SIS.

([2]) Ein Mitgliedstaat, der von dieser Möglichkeit der Beschränkung von Rechten Gebrauch macht, muss dabei - wie bereits zuvor erwähnt - die Bestimmungen von Artikel 8 EMRK einhalten.

Der EDPS schlägt vor, in die SIS-II-Vorschläge (nämlich in Artikel 21 des Verordnungsvorschlags und in Artikel 40 des Beschlussvorschlags) eine Bestimmung mit derselben Wirkung wie der derzeitige Artikel 102 Absatz 4 des Schengener Durchführungsübereinkommens aufzunehmen, mit der die Möglichkeiten der Mitgliedstaaten, nicht in den SIS-II-Regelungen vorgesehene Daten zu nutzen, eingeschränkt werden. Eine andere Möglichkeit besteht darin, das Ausmaß der Ausnahmen, die nach Artikel 13 der Richtlinie oder nach Artikel 9 des Übereinkommens in Anspruch genommen werden können, im Beschluss- und im Verordnungsvorschlag ausdrücklich zu begrenzen, indem beispielsweise festgelegt wird, dass die Mitgliedstaaten nur das Auskunfts- und Informationsrecht, nicht aber die Grundsätze der Datenqualität einschränken können.

3. **ZIEL**

Nach Artikel 1 beider Dokumente („Einrichtung und allgemeines Ziel des SIS II") besteht das Ziel der Errichtung des SIS II darin, „den zuständigen Behörden der Mitgliedstaaten die Zusammenarbeit durch Austausch von Informationen zum Zwecke von Personen- und Sachkontrollen zu ermöglichen", was „zur Wahrung eines hohen Maßes an Sicherheit in einem Raum ohne Binnengrenzkontrollen zwischen den Mitgliedstaaten beiträgt".

Das Ziel des SIS II ist ziemlich allgemein formuliert; die vorgenannten Bestimmungen enthalten keine konkrete Aussage darüber, was mit diesem Ziel abgedeckt (gemeint) ist.

Das Ziel des SIS II ist offenbar viel weiter gefasst als beim derzeitigen SIS, wie in Artikel 92 des Schengener Durchführungsübereinkommens dargelegt; darin wird nämlich speziell auf Ausschreibungen für die Suche nach Personen und Sachen, für Grenzkontrollen, sonstige polizeiliche und zollrechtliche Überprüfungen (…) sowie (bei Ausschreibungen nach Artikel 96) für Zwecke des Sichtvermerksverfahrens sowie der Erteilung der Aufenthaltstitel und der Handhabung des Ausländerrechts Bezug genommen.

Dieses umfassendere Ziel ergibt sich auch daraus, dass für das SIS II neue Funktionalitäten und Zugriffsmöglichkeiten vorgesehen wurden, die weniger dem ursprünglichen Zweck der Durchführung von Personen- und Sachkontrollen, sondern eher dem eines Ermittlungsinstruments entsprechen. Insbesondere ist der Zugriff für solche Behörden vorgesehen, die die SIS-II-Daten für eigene Zwecke und nicht für SIS-II-Zwecke nutzen werden (siehe unten). Die Verknüpfung von Ausschreibungen wird verallgemeinert werden, da dies ein typisches Merkmal eines Instruments für polizeiliche Ermittlungen darstellt.

Ferner gibt es Fragen in Bezug auf die in den nächsten Jahren zu entwickelnde biometrische Suchmaschine, mit der Abfragen im System ermöglicht werden sollen, die die Anforderungen eines Kontrollsystems übersteigen.

Zusammenfassend kann festgestellt werden, dass der Anwendungsbereich der Vorschläge gegenüber dem bestehenden Rechtsrahmen stark erweitert wurde. Daher sind zusätzliche Schutzgarantien erforderlich. Diesbezüglich wird der EDPS den Schwerpunkt seiner Analyse weniger auf die breit gefasste Zielsetzung in Artikel 1, sondern vielmehr auf die Funktionalitäten und die anderen Bestandteile des SIS II legen.

4. **WESENTLICHE ÄNDERUNGEN IM SIS II**

Den Schwerpunkt in diesem Kapitel bilden zunächst die neuen Elemente im SIS II, d.h. die Aufnahme biometrischer Daten, das neue Konzept für den Zugang — mit besonderer Aufmerksamkeit für den Zugang für Europol und Eurojust sowie für die Kfz-Zulassungsstellen –, die Verknüpfung von Ausschreibungen und der Zugang verschiedener Behörden zu Einwanderungsdaten.

4.1. **Biometrische Daten**

Mit den SIS-II-Vorschlägen wird die Möglichkeit der Verarbeitung einer neuen Datenkategorie eingeführt, die besondere Beachtung verdient, nämlich der biometrischen Daten. Wie der EDPS bereits in seiner Stellungnahme zum Visa-Informationssystem ([1]) betont hat, erfordert der sensible Charakter, der den biometrischen Daten inhärent ist, spezielle Schutzgarantien, die die SIS-II-Vorschläge jedoch nicht enthalten.

Allgemein ist festzustellen, dass es in EU-weit genutzten Informationssystemen (VIS, EURODAC, Führerschein-Informationssystem usw.) einen stetigen Aufwärtstrend bei der Nutzung biometrischer Daten gibt, die damit verbundenen Risiken und erforderlichen Schutzgarantien aber keine gebührende Berücksichtigung finden.

Auf die Notwendigkeit, gründlichere Überlegungen hierüber anzustellen, wurde auch in der Resolution über biometrische Daten hingewiesen, die auf der Internationalen Konferenz der Datenschutzbeauftragten in Montreux ([2]) verabschiedet wurde. Bislang stand bei der Frage, welchen Zusatznutzen die Aufstellung von Normen bringt, nur die zunehmende Interoperabilität zwischen den Systemen, nicht aber die Qualitätsverbesserung bei der Verarbeitung biometrischer Daten im Mittelpunkt.

([1]) Stellungnahme des Europäischen Datenschutzbeauftragten vom 23. März 2005 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, Nummer 3.4.2.

([2]) 27. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre, Montreux, 16. September 2005, Resolution über die Verwendung von biometrischen Daten in Reisepässen, Identitätskarten und Reisedokumenten.

Es wäre zweckmäßig, eine Reihe gemeinsamer Verpflichtungen oder Anforderungen, die dem spezifischen Charakter dieser Daten gerecht werden, sowie eine gemeinsame Methodik für deren Anwendung zu erarbeiten. Diese gemeinsamen Anforderungen könnten insbesondere die folgenden Elemente beinhalten (ihre Notwendigkeit wurde in den SIS-II-Vorschlägen erläutert):

— **Gezielte Folgenabschätzung:** Es sei hervorgehoben, dass die Vorschläge nicht Gegenstand einer Folgenabschätzung hinsichtlich der Nutzung biometrischer Daten waren. ([1])

— **Verstärkte Beachtung des Erfassungsverfahrens:** Die Quelle der biometrischen Daten und die Methode ihrer Erfassung sind nicht näher angegeben. Die Erfassung ist ein kritischer Schritt im gesamten Verfahren der biometrischen Identifizierung; sie lässt sich nicht einfach in Anhängen regeln oder im Rahmen von Untergruppensitzungen festlegen, denn von ihr hängt das Endergebnis des Prozesses, d.h. die Höhe der Falschrückweisungsrate oder der Falschakzeptanzrate unmittelbar ab.

— **Schwerpunkt Genauigkeitsgrad:** Die Verwendung biometrischer Daten zur Identifizierungszwecke (Abgleich „eins zu vielen"), die im Vorschlag als künftige Einsatzmöglichkeit einer „biometrischen Suchmaschine" vorgestellt wird, ist problematischer, weil der Genauigkeitsgrad der Ergebnisse dieses Prozesses geringer ist als bei einer Verwendung zur Authentikation oder Kontrolle (Abgleich „eins zu eins"). Eine Identifizierung anhand biometrischer Daten sollte daher nicht die einzige Methode der Identifizierung oder der einzige Schlüssel für den Zugang zu weiteren Informationen sein.

— **Ausweichverfahren:** Es sollten jederzeit verfügbare Ausweichverfahren (*fallback procedures*) eingeführt werden, um die Würde der Personen, die irrtümlicherweise identifiziert worden sein könnten, zu wahren und zu vermeiden, dass sie unter den Mängeln des Systems zu leiden haben.

Die Nutzung biometrischer Daten ohne angemessene vorherige Folgenabschätzung zeigt auch, dass die Zuverlässigkeit der Biometrik überschätzt wird. Biometrische Daten sind „lebendig" und ändern sich mit der Zeit; die in der Datenbank gespeicherten Muster sind lediglich Momentaufnahmen eines dynamischen Merkmals. Sie sind nicht dauerhaft unveränderlich und müssen daher überprüft werden. Die Genauigkeit biometrischer Daten muss stets im Verhältnis zu anderen Merkmalen gesehen werden, denn sie hat niemals absoluten Charakter.

Die mögliche Nutzung von SIS-II-Daten zu Ermittlungszwecken birgt erhebliche Risiken für das Datensubjekt, wenn man sich vorwiegend auf biometrische Daten als Beweismaterial verlässt oder deren Rolle überschätzt, wie in früheren Fällen aufgezeigt wurde ([2]).

Daher sollte in den Vorschlägen die tatsächliche Aussagekraft der Biometrik für Identifizierungszwecke realistisch bewertet und das Bewusstsein für diese Problematik geschärft werden.

4.2. **Zugang zu SIS-II-Daten**

4.2.1 *Ein neues Konzept für den Zugang zu den Daten*

Für jede Ausschreibung wird bestimmt, welche Behörden Zugang zu SIS-II-Daten haben. Grundsätzlich gilt für die Gewährung des Zugriffs auf SIS-II-Daten eine doppelte Voraussetzung: Der Zugang muss den Behörden im vollen Einklang mit dem allgemeinen Zweck des SIS und mit dem speziellen Zweck jeder einzelnen Ausschreibung gewährt werden.

Dies ergibt sich aus der im Verordnungs- und im Beschlussvorschlag enthaltenen Bestimmung des Begriffs Ausschreibung (Nach Artikel 3 Nummer 1 Buchstabe a beider Rechtsakte bedeutet *„Ausschreibung" einen im SIS II gespeicherter Datensatz, der den zuständigen Behörden die Identifizierung einer Person oder Sache im Hinblick auf eine spezifische zu ergreifende Maßnahme ermöglicht*). In Artikel 39 Absatz 3 des Beschlussvorschlags wird dies noch deutlicher; hier heißt es nämlich: *„Die in Absatz 1 genannten Daten werden ausschließlich zur Identifizierung einer Person im Hinblick auf eine spezifische zu ergreifende Maßnahme gemäß diesem Beschluss verwendet"*. In dieser Hinsicht weist das SIS II immer noch die Merkmale eines „Treffer/kein Treffer"-Systems auf, in das jede Ausschreibung zu einem speziellen Zweck eingegeben wird (Übergabe, Einreiseverweigerung, usw.).

Für Behörden, die Zugriff auf SIS-Daten haben, wird die Nutzung dieser Daten de facto beschränkt, da sie grundsätzlich nur Zugriff auf die Daten zur Durchführung einer spezifischen Maßnahme erhalten.

Doch entziehen sich einige der in den neuen Vorschlägen vorgesehenen Zugriffsmöglichkeiten dieser Logik, denn ihr Zweck besteht nicht etwa darin, der Behörde die Identifizierung einer Person und die Durchführung der in der Ausschreibung vorgesehenen Maßnahme zu ermöglichen, sondern darin, sie mit Informationen zu versorgen.

([1]) Grundlage für die Folgenabschätzung könnten die so genannten sieben Säulen der biometrischen Weisheit sein; diese finden sich in der Veröffentlichung „Biometrics at the frontiers: Assessing the impact on Society", Institut für Technologische Zukunftsforschung, GD Gemeinsame Forschungsstelle, EUR 21585 EN, Abschnitt 1.2, Seite 32.

([2]) Im Juni 2004 wurde ein Rechtsanwalt aus Portland (USA) zwei Wochen lang in Haft gehalten, weil das FBI festgestellt hatte, dass sein Fingerabdruck zu einem anderen passte, der bei den Bombenanschlägen von Madrid (auf dem Plastikbeutel, der den Zünder enthielt) gefunden worden war. Schließlich konnte nachgewiesen werden, dass der Abgleich fehlerhaft war und zu einem falschen Auswertungsergebnis geführt hatte.

Konkret betrifft dies:

— den Zugriff der Asylbehörden auf Einwanderungsdaten;

— den Zugriff der für die Zuerkennung der Flüchtlingseigenschaft zuständigen Behörden auf Einwanderungsdaten;

— den Zugriff von Europol auf Ausschreibungen von Personen zwecks Auslieferung, verdeckter Registrierung oder auf Sachfahndungsausschreibungen zur Sicherstellung;

— den Zugriff von Eurojust auf Auslieferungsdaten und Angaben zum Aufenthalt.

Für all diese Behörden gilt in Bezug auf die SIS-II-Daten übereinstimmend Folgendes:

Sie können nicht die spezifische Maßnahme ergreifen, wie sie in der Definition des Begriffs Ausschreibung erwähnt wird. Der Zugang wird ihnen zur Informationsbeschaffung für ihre eigenen Zwecke gewährt.

Sogar bei diesen Behörden muss ferner unterschieden werden zwischen denen, die Zugriff auf Daten für ihre eigenen Zwecke haben, wenn auch mit einem eher spezifischen Ziel, und jenen (nämlich Europol und Eurojust), bei denen überhaupt kein konkreter Zugriffszweck festgelegt ist. So haben Asylbehörden Zugriff zu einem spezifischen Zweck, selbst wenn es sich dabei nicht um den in der Ausschreibung genannten Zweck handelt. Ihnen kann der Zugriff auf Einwanderungsdaten gewährt werden, „damit sie bestimmen können, ob sich ein Asylbewerber illegal in einem anderen Mitgliedstaat aufgehalten hat". Europol und Eurojust hingegen wird Zugriff auf die in bestimmten Ausschreibungskategorien enthaltenen Daten „zur Erfüllung ihrer Aufgaben" gewährt.

Kurz gesagt wird der Zugriff auf SIS-II-Daten in drei Fällen gewährt:

— für die Durchführung der in der Ausschreibung vorgesehenen Maßnahme;

— für SIS-II-fremde Zwecke, die in den Vorschlägen eindeutig spezifiziert sind;

— für SIS-II-fremde Zwecke, die nicht genau beschrieben sind.

Der EDPS vertritt die Ansicht, dass die einzuführenden Schutzgarantien umso strikter sein sollten, je allgemeiner der Zweck des Zugriffs ist. Die allgemeinen Schutzgarantien werden nachstehend aufgeführt; anschließend wird auf den besonderen Status von Europol und Eurojust eingegangen.

4.2.2 *Bedingungen für die Gewährung des Zugangs*

1. In vielen Fällen kann der Zugang nur gewährt werden, wenn er mit dem allgemeinen Zweck des SIS II und mit dessen Rechtsgrundlage vereinbar ist.

   Dies bedeutet in der Praxis, dass der Zugriff auf Einwanderungsdaten nach dem Verordnungsvorschlag der Umsetzung der Maßnahmen im Zusammenhang mit dem den Personenverkehr betreffenden Teil des Schengen-Besitzstands dienen soll.

   Analog dazu soll der Zugriff auf die im Beschluss genannten Ausschreibungen zur Förderung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen beitragen.

   In diesem Zusammenhang verweist der EDPS auf das Kapitel, in dem die Frage des Zugangs von für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständigen Dienststellen zum SIS-II behandelt wird (siehe nachstehenden Punkt 4.6).

2. Die Notwendigkeit des Zugriffs auf SIS-II-Daten muss nachgewiesen werden, ebenso wie der Umstand, dass die Daten nicht oder nur unter großen Schwierigkeiten auf anderem, mit geringeren Eingriffen verbundenen Wege beschafft werden können. Darauf hätte in einer Begründung eingegangen werden müssen; dass sie fehlt, ist — wie bereits gesagt — sehr bedauerlich.

3. Die Nutzung der Daten muss ausdrücklich und restriktiv begrenzt sein.

   So haben Asylbehörden Zugriff auf Einwanderungsdaten, „damit sie bestimmen können, ob sich ein Asylbewerber illegal in einem anderen Mitgliedstaat aufgehalten hat". Europol und Eurojust hingegen wird der Zugriff auf die in bestimmten Kategorien von Ausschreibung enthaltenen Daten gewährt, da „dies zur Erfüllung ihrer Aufgaben nötig ist". Hierzu werden keine ausreichenden Erläuterungen gegeben (siehe unten).

4. Die Zugriffsbedingungen müssen genau definiert und begrenzt sein. Insbesondere dürften nur die Dienststellen innerhalb dieser Organisationen, die SIS-II-Daten verarbeiten müssen, zugangsberechtigt sein. Diese in Artikel 40 des Beschlussvorschlags und in Artikel 21 Absatz 2 des Verordnungsvorschlags genannte Bedingung sollte um eine Verpflichtung ergänzt werden, wonach die nationalen Behörden verpflichtet sind, eine aktuelle Liste der Personen mit Zugangsberechtigung zum SIS II zu führen. Gleiches sollte für Europol und Eurojust gelten.

5. Die Tatsache, dass diese Behörden Zugriff auf SIS-II-Daten gewährt wird, darf nicht als Grund dafür dienen, dass Daten in das System eingegeben werden oder dort gespeichert bleiben, wenn sie für die spezifische Ausschreibung, zu der sie gehören, ohne Nutzen sind. Neue Datenkategorien dürfen nicht deshalb vorgesehen werden, weil sie für andere Informationssysteme nützlich sein könnten. So sieht Artikel 39 des Beschlussvorschlags die Aufnahme von Angaben zur ausschreibenden Behörde in die Ausschreibungen vor. Diese Angaben sind für die Durchführung einer Maßnahme (Verhaftung, verdeckte Registrierung, usw.) nicht nötig; als einziger Grund für ihre Aufnahme wäre denkbar, dass sie Europol oder Eurojust von Nutzen sind. Es müsste also eine klare Begründung für die Verarbeitung dieser Daten genannt werden.

6. Die Speicherfrist der Daten darf nicht verlängert werden, wenn dies für den Zweck, für den die Daten eingegeben wurden, nicht erforderlich ist. Dies bedeutet, dass selbst die Tatsache, dass Europol oder Eurojust Zugriff auf diese Daten hat, kein ausreichender Grund für ihre weitere Speicherung im System ist (so sollten nach der Auslieferung einer Person die entsprechenden Daten gelöscht werden, auch wenn sie für Europol noch von Nutzen sein könnten). Auch hier ist eine sorgfältige Überwachung nötig, um sicherzustellen, dass die nationalen Behörden dem nachkommen.

4.2.3. *Zugang durch Europol und Eurojust*

a. *Gründe für den Zugang*

Der Zugriff von Europol und Eurojust auf bestimmte SIS-Daten wurde bereits diskutiert, bevor sie durch den Ratsbeschluss von 24. Februar 2005 [1] die Zugangsberechtigung erhielten. Von allen Behörden, die für ihre eigenen Zwecke Zugang zu den Daten haben, haben sie die umfangreichsten Zugriffsmöglichkeiten. Auch wenn die Nutzung dieser Daten in Kapitel XII des Beschlusses beschrieben ist, wird auf die Gründe für die Gewährung des Zugangs an sich überhaupt nicht hinreichend eingegangen. Diese Bemerkung trifft umso mehr zu, wenn man bedenkt, dass sich die Aufgaben von Europol und Eurojust voraussichtlich im Laufe der Zeit noch entwickeln werden.

Der EDPS ruft die Kommission dringend dazu auf, die Aufgaben, für deren Durchführung der Zugang durch Europol und Eurojust gerechtfertigt wäre, genau abzugrenzen.

b. *Beschränkung des Zugangs zu den Daten*

Um „Ausforschungen" durch Europol und Eurojust zu verhindern und sicherzustellen, dass sie nur Zugriff auf die zur Erfüllung ihrer Aufgaben notwendigen Daten erhalten, hat die GK Schengen in ihrer Stellungnahme vom 27. September 2005 über die SIS-II-Vorschläge angeregt, den Zugriff von Europol und Eurojust auf die Daten zu Personen zu beschränken, deren Namen bereits in ihren Dateien erscheinen. So wäre gewährleistet, dass nur Ausschreibungen abgefragt werden, die für sie relevant sind. Der EDPS unterstützt diese Empfehlung.

c. *Sicherheitsaspekte*

Der EDPS begrüßt die Verpflichtung zur Protokollierung aller durch Europol und Eurojust getätigte Vorgänge sowie das Verbot des Kopierens oder Herunterladens von Teilen des Systems.

In Artikel 56 des Beschlussvorschlags sind „eine oder zwei" Zugangsstellen für Europol und Eurojust vorgesehen. So verständlich es sein mag, dass ein Mitgliedstaat wegen der dezentralisierten Struktur seiner zuständigen Behörden mehr als eine Zugangsstelle benötigt, rechtfertigen der Status und die Tätigkeiten von Europol und Eurojust diesen Wunsch allerdings nicht. Es sei ferner darauf hingewiesen, dass unter dem Aspekt der Sicherheit die Einrichtung mehrerer Zugangsstellen die Gefahr von Missbräuchen erhöht und diese daher durch triftige Gründe besser gerechtfertigt werden sollte. In Ermangelung überzeugender Argumente schlägt der EDPS daher vor, Europol und Eurojust nur eine Zugangsstelle zu gewähren.

4.3. **Verknüpfungen zwischen Ausschreibungen**

Nach Artikel 26 der Verordnung bzw. nach Artikel 46 des Beschlusses kann ein Mitgliedstaat nach Maßgabe des innerstaatlichen Rechts Ausschreibungen miteinander verknüpfen, um zwei oder mehr Ausschreibungen miteinander zu verbinden.

So nützlich Verknüpfungen zwischen Ausschreibungen für Kontrollzwecke auch sein mögen (so kann ein Haftbefehl in Bezug auf einen gesuchten Autodieb mit einer Ausschreibung eines gestohlenen Kraftfahrzeugs verknüpft werden), sind Verknüpfungen zwischen Ausschreibungen doch ein sehr typisches Leistungsmerkmal eines Instruments für polizeiliche Ermittlungen.

Verknüpfungen zwischen Ausschreibungen können sich erheblich auf die Rechte der betroffenen Person auswirken, da diese nicht länger ausschließlich anhand der auf sie zutreffenden Daten, sondern anhand ihrer möglichen Verbindung zu anderen Personen überprüft wird. Personen, deren Daten mit denen von Kriminellen oder gesuchten Personen in Verbindung gebracht werden, sind voraussichtlich einem größeren Verdacht ausgesetzt als andere. Die Verknüpfung von Ausschreibungen kommt zudem einer Ausweitung der Ermittlungsmöglichkeiten des SIS gleich, denn es ermöglicht die Erfassung mutmaßlicher krimineller Banden oder Netze (wenn beispielsweise Daten über illegale Einwanderer mit denen von Schleusern verknüpft werden). Da die Herstellung von Verknüpfungen nach Maßgabe des innerstaatlichen Rechts erfolgt, ergibt sich schließlich als eine mögliche Konsequenz daraus, dass Verknüpfungen, die in einem Mitgliedstaat rechtswidrig sind, in einem anderen Mitgliedstaat hergestellt und somit „illegale" Daten in das System eingegeben werden können.

[1] Beschluss 2005/211/JI des Rates vom 24. Februar 2005 über die Einführung neuer Funktionen für das Schengener Informationssystem, auch im Hinblick auf die Terrorismusbekämpfung (ABl. L 68 vom 15.3.2005, S. 44).

In den Schlussfolgerungen des Rates vom 14. Juni 2004 zu den funktionellen Anforderungen an das SIS II wird festgestellt, dass jede Verknüpfung durch eindeutige operative Erfordernisse begründet sein, auf einen eindeutig definierten Sachzusammenhang gestützt werden und im Einklang mit dem Grundsatz der Verhältnismäßigkeit stehen muss. Zudem darf sie die Zugriffsrechte nicht beeinträchtigen. Da die Verknüpfung von Ausschreibungen einen Verarbeitungsvorgang darstellt, muss sie auf jeden Fall mit den für die Umsetzung der Richtlinie 95/46/EG und/oder des Übereinkommens Nr. 108 erlassenen nationalen Rechtsvorschriften im Einklang stehen.

In den Vorschlägen wird immer wieder darauf hingewiesen, dass bestehende Verknüpfungen nichts an den Zugriffsrechten ändern dürfen (sonst würde dadurch der Zugang zu Daten ermöglicht, deren Verarbeitung nach nationalem Recht unzulässig wäre, was ein Verstoß gegen Artikel 6 der Richtlinie darstellen würde).

Der EDPS betont, wie wichtig es ist, Artikel 26 des Verordnungsvorschlags und Artikel 46 des Beschlussvorschlags strikt auszulegen. Dies lässt sich unter anderem gewährleisten, indem eindeutig festgelegt wird, dass Behörden, die kein Recht auf Zugang zu bestimmten Datenkategorien haben, nicht nur der Zugang zu Verknüpfungen zu solchen Datenkategorien verwehrt wird, sondern dass sie nicht einmal von der Existenz solcher Verknüpfungen Kenntnis erhalten sollten. Verknüpfungen dürfen nicht sichtbar gemacht werden, wenn kein Recht auf Zugang zu verknüpften Daten besteht.

Darüber hinaus möchte der EDPS zu den technischen Maßnahmen, mit denen dies gewährleistet werden soll, konsultiert werden.

4.4. **Ausschreibungen zum Zwecke der Einreiseverweigerung**

4.4.1. *Gründe für die Aufnahme*

Die Nutzung von „Ausschreibungen von Drittstaatsangehörigen zur Einreiseverweigerung“ (Artikel 15 der Verordnung) hat schwer wiegende Auswirkungen auf die Freiheiten des Einzelnen, denn wer nach Maßgabe dieser Bestimmung ausgeschrieben wurde, darf auf Jahre nicht mehr in den Schengen-Raum einreisen. Gemessen an der Zahl der Betroffenen, handelt es sich hier um die am häufigsten eingegebene Ausschreibung. In Anbetracht der Konsequenzen, die eine solche Ausschreibung hat, muss sie mit besonderer Sorgfalt konzipiert und angewendet werden. Zwar gilt dies auch für andere Ausschreibungen, dennoch möchte der EDPS dieser Ausschreibungsart ein gesondertes Kapitel widmen, weil sie hinsichtlich der Gründe für ihre Aufnahme besondere Probleme aufwirft.

Die neue Ausschreibung zur Einreiseverweigerung bringt Verbesserungen gegenüber der derzeitigen Situation, ist jedoch nicht völlig zufrieden stellend, da sie sich weitgehend auf Rechtsinstrumente stützt, die noch nicht erlassen wurden oder noch nicht einmal als Vorschläge vorliegen.

Die Verbesserungen liegen in einer präziseren Beschreibung der Gründe für die Aufnahme der Daten in das System. Aufgrund des jetzigen Wortlauts des Schengener Durchführungsübereinkommens gibt es erhebliche Unterschiede zwischen den Mitgliedstaaten, was die Zahl der nach Artikel 96 des Übereinkommens ausgeschriebenen Personen anbelangt. Die GK-Schengen hat eine umfassende Studie ([1]) zu diesem Problem durchgeführt und angeregt, dass die politischen Entscheidungsträger prüfen sollten, ob die Gründe für die Aufnahme von Ausschreibungen in den einzelnen Schengen-Staaten nicht vereinheitlicht werden könnten.

Der vorgeschlagene Artikel 15 ist detaillierter formuliert, was begrüßenswert ist.

Zudem enthält Artikel 15 Absatz 2 eine Liste von Fällen, in denen die Personen nicht ausgeschrieben werden können, weil sie sich unter dem Schutz des einen oder anderen Rechtsstatus rechtmäßig im Hoheitsgebiet eines Mitgliedstaats aufhalten. Zwar lässt sich dies auch aus dem Schengener Durchführungsübereinkommen in seiner derzeitigen Fassung herleiten, doch hat sich in der Praxis gezeigt, dass auch diese Regelung in den Mitgliedstaaten unterschiedlich gehandhabt wird. Diese Klarstellung ist somit begrüßenswert.

Doch gibt es auch herbe Kritik an dieser Bestimmung, weil sie sich weitgehend auf einen noch nicht erlassenen Rechtsakt, nämlich die „Rückführungsrichtlinie“ stützt.

Seit der Annahme der SIS-II-Vorschläge hat die Kommission (am 1. September 2005) den Vorschlag für eine „Richtlinie über gemeinsame Normen und Verfahren in den Mitgliedstaaten zur Rückführung illegal aufhältiger Drittstaatsangehöriger“ vorgelegt; solange der Text jedoch nicht endgültig verabschiedet wurde, kann er nicht als triftige Begründung für die Aufnahme von Daten in ein System herangezogen werden. Er stellt insbesondere einen Verstoß gegen Artikel 8 EMRK dar, da ein Eingriff in die Privatshäre von Personen unter anderem durch klare und zugängliche Rechtsvorschriften begründet werden sollte.

Deshalb fordert der EDPS die Kommission dringend auf, diese Bestimmung entweder zurückzuziehen oder sie auf der Grundlage bestehender Rechtsvorschriften so umzuformulieren, dass Einzelpersonen genau wissen können, welche Maßnahmen von den Behörden ihnen gegenüber ergriffen werden können.

4.4.2. *Zugriff auf Ausschreibungen nach Artikel 15*

In Artikel 18 ist festgelegt, welche Behörden auf diese Ausschreibungen Zugriff haben und welchen Zweck der Zugriff zu verfolgen hat. In Artikel 18 Absätze 1 und 2 ist vorgesehen, welche Behörden auf der Grundlage der Rückführungsrichtlinie zugriffsberechtigt sind. Hierzu gelten die gleichen Bemerkungen wie oben.

([1]) Bericht der GK-Schengen zu einer Überprüfung der Nutzung von Ausschreibungen gemäß Artikel 96 im Schengener Informationssystem, Brüssel, 20. Juni 2005.

Nach Artikel 18 Absatz 3 des Verordnungsvorschlags erhalten die für die Zuerkennung der Flüchtlingseigenschaft zuständigen Behörden Zugriff auf Ausschreibungen auf der Grundlage einer Richtlinie, die noch nicht einmal als Vorschlag vorliegt. Da bislang kein Text verfügbar ist, muss der EDPS seine vorstehenden Bemerkungen bekräftigen.

4.4.3. *Erfassungsdauer von Ausschreibungen nach Artikel 15*

Ausschreibungen dürfen nach Artikel 20 Absatz 1 nur für die Dauer der Einreiseverweigerung, die in der Abschiebungsanordnung oder der Rückführungsentscheidung angegeben ist, gespeichert werden. Diese Regelung steht mit den Datenschutzvorschriften in Einklang. Außerdem werden die Ausschreibungen automatisch nach fünf Jahren gelöscht, sofern der Mitgliedstaat, der die Daten in das SIS II eingegeben hat, nichts anderes entscheidet.

Durch eine angemessene Überwachung auf nationaler Ebene sollte sichergestellt werden, dass ohne triftigen Grund keine automatische Verlängerung der Erfassungsdauer erfolgt und dass die Mitgliedstaaten die Daten vor Ablauf der Fünfjahresfrist löschen, wenn die Dauer des Einreiseverbots kürzer sein sollte.

4.5. **Erfassungsdauer**

Zwar bleibt der Grundsatz in Bezug auf die Erfassung unverändert (generell sind Ausschreibungen aus dem SIS II zu löschen, sobald die mit der Ausschreibung beantragte Maßnahme durchgeführt ist), doch ergibt sich aus den Vorschlägen, dass die Erfassungsdauer der Ausschreibungen generell verlängert wurde.

Nach dem Schengener Durchführungsübereinkommen ist die Erforderlichkeit der weiteren Speicherung der Daten spätestens drei Jahre nach ihrer Einspeicherung (bzw. nach einem Jahr im Falle von Daten, die zur verdeckten Registrierung aufgenommen wurden) zu prüfen. In den neuen Vorschlägen ist eine automatische Löschung von Einwanderungsdaten nach 5 Jahren, von Personenfahndungsausschreibungen zwecks Verhaftung, Ausschreibungen von Vermissten und von Personen, die im Hinblick auf ein Gerichtsverfahren gesucht werden, nach 10 Jahren sowie von Personenfahndungsausschreibungen zwecks verdeckter Registrierung nach 3 Jahren vorgesehen, wobei der ausschreibende Mitgliedstaat Einspruch erheben kann.

Wenngleich die Mitgliedstaaten grundsätzlich verpflichtet sind, die Daten zu löschen, sobald der Zweck der Ausschreibung erreicht ist, kommt diese Neuregelung doch einer deutlichen Verlängerung (in den meisten Fällen einer Verdreifachung) der maximalen Erfassungsdauer gleich, ohne dass die Kommission dies in irgendeiner Weise begründet. Im Falle der Einwanderungsdaten kann man nur mutmaßen, dass die Erfassungsdauer von 5 Jahren mit der Dauer des Einreiseverbots, wie sie in der Rückführungsrichtlinie vorgeschlagen wird, zusammenhängt. Für alle anderen Fälle liegt nach Wissen des EDPS keine Begründung vor.

Die möglichen Auswirkungen auf die im SIS ausgeschriebenen Datensubjekte können sich erheblich auf das Leben der Betroffenen auswirken. Besonderen Anlass zur Besorgnis geben hier Fahndungsausschreibungen zwecks verdeckter Registrierung oder gezielter Kontrolle, da sie aufgrund von Verdachtsmomenten in das System aufgenommen werden können.

Der EDPS würde es begrüßen, wenn eine stichhaltige Begründung für die Verlängerung der Frist für die Speicherung der Daten vorgelegt wird. Sollte es keine überzeugenden Gründe geben, so empfiehlt er, diese Frist auf ihre derzeitige Dauer zurückzuführen, wofür er insbesondere bei den Fahndungsausschreibungen zwecks verdeckter Registrierung oder gezielter Kontrolle plädiert.

4.6. **Zugriff für Behörden, die für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständig sind**

Das Hauptproblem liegt in der Wahl einer mehr als bedenklichen Rechtsgrundlage. Der Kommission gelingt es nicht, überzeugend zu begründen, warum sie eine Rechtsgrundlage aus der ersten Säule „Verkehr" für eine Maßnahme wählt, mit der Verwaltungsbehörden der Zugriff auf das SIS zum Zwecke der Prävention und Bekämpfung der Kriminalität (Schmuggel gestohlener Fahrzeuge) gewährt würde. Die Notwendigkeit einer triftigen Begründung und einer tragfähigen Rechtsgrundlage für die Gewährung des Zugriffs auf das SIS II wurde in Nummer 4.2.2 dieser Stellungnahme bereits ausführlich dargelegt.

Der EDPS verweist auf die diesbezüglichen Bemerkungen der GK-Schengen in ihrer Stellungnahme über die für das SIS II vorgeschlagene Rechtsgrundlage. Insbesondere sollte die Anregung der GK-Schengen, den Beschlussvorschlag zu ändern, um auch diese Zugriffsmöglichkeit darin aufzunehmen, aufgegriffen werden.

5. **ROLLE DER KOMMISSION UND DER MITGLIEDSTAATEN**

Eine klare Beschreibung und Aufteilung der Zuständigkeiten im Zusammenhang mit SIS II ist von größter Bedeutung, und zwar nicht nur für das reibungslose Funktionieren des Systems, sondern auch für die Zwecke der Überwachung. Die Aufteilung der Überwachungsbefugnisse ergibt sich aus der Beschreibung der Zuständigkeiten, weshalb absolute Klarheit unerlässlich ist.

5.1. **Rolle der Kommission**

Der EDPS begrüßt das in beiden Vorschlägen enthaltene Kapitel III, in dem die Rolle und die Zuständigkeiten der Kommission im Rahmen des SIS II (Zuständigkeit für das „Betriebsmanagement") beschrieben werden. Im VIS-Vorschlag fehlte diese Klarheit. Doch wird in dem genannten Kapitel allein die Rolle der Kommission nicht erschöpfend beschrieben. Wie in Kapitel 9 dieser Stellungnahme dargelegt, ist die Kommission im Wege des Ausschussverfahrens nämlich auch an der Einrichtung und der Verwaltung des Systems beteiligt.

In Bezug auf den Datenschutz hat die Kommission eine Rolle, die ihr bereits bei den Systemen VIS und Eurodac zuerkannt wurde, nämlich die Zuständigkeit für das Betriebsmanagement. Zusammen mit ihrer führenden Rolle bei Entwicklung und Wartung des Systems sollte dies als eine Kontrollaufgabe sui generis betrachtet werden. Wie bereits in der Stellungnahme des EDPS zum VIS festgehalten, umfasst diese Kontrollaufgabe zum einen viel mehr als eine Verarbeitungsaufgabe, zum anderen ist sie aber eingeschränkter als die einer gewöhnlichen Kontrollstelle, da die Kommission keinen Zugang zu den im SIS II verarbeiteten Daten hat.

Da das SIS II auf komplexe Systemen gestützt sein wird, von denen einige auf neu entstehenden Technologien beruhen, betont der EDPS nachdrücklich, dass die Kommission verstärkt dafür zuständig sein soll, die Systeme auf dem neuesten Stand zu halten und hierfür auf die besten verfügbaren Sicherheits- und Datenschutztechnologien zurückzugreifen.

Daher sollte in Artikel 12 der Vorschläge jeweils hinzugefügt werden, dass die Kommission regelmäßig die Anwendung neuer Technologien vorschlagen sollte, die dem Stand der Technik auf diesem Gebiet entsprechen und das Niveau des Datenschutzes und der Sicherheit erhöhen und die Aufgaben der nationalen Behörden, die Zugang zu diesen Daten haben, erleichtern werden.

5.2. **Rolle der Mitgliedstaaten**

Die Lage der Mitgliedstaaten ist nicht eindeutig geklärt, da es schwierig ist, in Erfahrung zu bringen, welche Behörde(n) für die Datenkontrolle zuständig sein wird (werden).

Die Vorschläge sehen eine Rolle für das nationale SIS-II-Büro (zur Gewährleistung des Zugangs der zuständigen Behörden zum SIS II) sowie für die SIRENE-Behörden (zur Gewährleistung des Austauschs aller Zusatzinformationen) vor. Ferner obliegt es den Mitgliedstaaten, für den Betrieb und die Sicherheit ihres jeweiligen nationalen Systems (NS) zu sorgen. Es ist nicht klar, ob dafür eine der vorgenannten Behörden zuständig sein soll. Dies muss auf jeden Fall präzisiert werden.

Was den Datenschutz anbelangt, so sollten die Kommission und die Mitgliedstaaten als gemeinsame Kontrollinstanzen mit jeweils besonderen Zuständigkeiten betrachtet werden. Nur wenn anerkannt wird, dass diese Aufgaben sich gegenseitig ergänzen, kann gewährleistet werden, dass kein Bereich der SIS-II-Tätigkeiten ohne Aufsicht bleibt.

6. **RECHTE DER DATENSUBJEKTE**

6.1. **Information**

6.1.1. *Verordnungsvorschlag*

Nach Artikel 28 der vorgeschlagenen Verordnung wird den Datensubjekten ein im Wesentlichen an Artikel 10 der Richtlinie 95/46/EG angelehntes Recht auf Information eingeräumt. Gegenüber der derzeitigen Lage, wonach im Übereinkommen ein Recht auf Information nicht ausdrücklich vorgesehen ist, ist dies eine begrüßenswerte Verbesserung. In den nachstehenden Punkten sind aber noch weitere Verbesserungen möglich.

Die Aufzählung sollte um einige Informationen ergänzt werden, da dies zur Gewährleistung einer fairen Behandlung der Datensubjekte beitragen würde ([1]). Diese Informationen sollten Folgendes betreffen: die für die Daten geltende Speicherungsfrist, das Bestehen des Rechts, eine Überprüfung zu beantragen oder Widerspruch gegen eine Ausschreibung einzulegen (in einigen Fällen siehe Artikel 15 Absatz 3 der vorgeschlagenen Verordnung), die Möglichkeit der Unterstützung durch die Datenschutzbehörde und die Möglichkeit, Rechtsmittel einzulegen.

In der vorgeschlagenen Verordnung findet sich kein Verweis auf den Zeitpunkt, zu dem die Information bereitgestellt werden sollte. Dies könnte den Datensubjekten die Ausübung ihrer Rechte unmöglich machen. Um diesen Rechten Wirkung zu verleihen, sollte in der Verordnung der genaue Zeitpunkt angegeben werden, zu dem die Informationen — je nachdem, welche Behörde die Ausschreibung eingegeben hat — bereitzustellen sind.

In der Praxis könnte die Lösung darin bestehen, bereits in die Entscheidung, die der Ausschreibung zugrunde liegt, Informationen über die Ausschreibung aufzunehmen: dies wäre eine mit einer Bedrohung der öffentlichen Sicherheit begründete Gerichts- oder Verwaltungsentscheidung oder eine Rückführungsentscheidung oder eine mit dem Verbot der Wiedereinreise verbundene Abschiebungsanordnung. Diese Angaben sollten in Artikel 28 der Verordnung aufgenommen werden.

6.1.2. *Beschlussvorschlag*

In Artikel 50 des Beschlusses ist vorgesehen, dass die Datensubjekte auf Antrag Informationen erhalten können, und es werden ferner die Gründe angeführt, aus denen die Informationserteilung verweigert werden darf. Die Beschränkungen des Rechts auf Auskunft sind in Anbetracht der Art der Daten und des Zusammenhangs, in dem sie verarbeitet werden, selbstverständlich nachvollziehbar.

Das Recht auf Information sollte jedoch nicht von einem Antrag des Datensubjekts abhängen (dies wäre nämlich eher die Definition eines Antrags auf Auskunft). Es kann davon ausgegangen werden, dass das Bedürfnis der „Stellung eines Antrags“ auf Information in den Fällen gerechtfertigt ist, in denen die Datensubjekte nicht unterrichtet werden können, da ihr Aufenthaltsort nicht bekannt ist.

Dies könnte besser geregelt werden, indem eine Ausnahme vom Recht auf Information für die Fälle hinzugefügt wird, in denen die Informationserteilung sich als unmöglich erweist oder nur mit unverhältnismäßigem Aufwand möglich wäre. Artikel 50 des Beschlusses sollte entsprechend geändert werden.

([1]) Siehe hierzu auch die Stellungnahme des EDPS zum Visa-Informationssystem (VIS), Nummer 3.10.1.

Diese Lösung wäre auch mit der Anwendung des Rahmenbeschlusses über den Datenschutz im Bereich der dritten Säule vereinbar.

6.2. **Auskunft**

Sowohl im Verordnungs- als auch im Beschlussvorschlag werden Fristen für die Beantwortung von Ersuchen um Auskunft vorgegeben; dies ist eine positive Entwicklung. Da das Verfahren für die Inanspruchnahme des Rechts auf Auskunft auf nationaler Ebene festgelegt ist, stellt sich jedoch die Frage, wie die in den Vorschlägen vorgegebenen Fristen mit den bestehenden Verfahren harmonieren können; dies gilt besonders, wenn in den Mitgliedstaaten für die Beantwortung von Ersuchen um Auskunft kürzere Fristen gelten. Es sollte präzisiert werden, dass die für das Datensubjekt jeweils günstigste Frist gelten soll.

6.2.1. *Verordnungsvorschlag*

Es sei darauf hingewiesen, dass die Beschränkungen des Rechts auf Auskunft („…unterbleibt, wenn dies zur Durchführung einer rechtmäßigen Aufgabe im Zusammenhang mit" der Ausschreibung „zum Schutz der Rechte und Freiheiten der betroffenen Person oder eines Dritten unerlässlich ist"), die sich derzeit im Schengener Durchführungsübereinkommen finden, in der vorgeschlagenen Verordnung fehlen.

Dies hängt vermutlich mit der Anwendbarkeit der Richtlinie 95/46/EG zusammen, in der (in Artikel 13) vorgesehen ist, dass in den nationalen Rechtsvorschriften Beschränkungen angewendet werden können. Es sollte auf jeden Fall darauf hingewiesen werden, dass der Rückgriff auf Artikel 13 in den nationalen Rechtsvorschriften zur Beschränkung des Rechts auf Auskunft stets mit Artikel 8 EMRK im Einklang stehen muss und nur in Ausnahmefällen zulässig ist.

6.2.2. *Beschlussvorschlag*

In dem vorgeschlagenen Beschluss werden die Beschränkungen des Rechts auf Auskunft aus dem Schengener Durchführungsübereinkommen übernommen. Der vorgeschlagene Rahmenbeschluss enthält im Wesentlichen die gleichen Beschränkungen des Rechts auf Auskunft, so dass die Annahme dieses Rechtsakts diesbezüglich keine wesentliche Veränderung bewirken würde.

Da in einigen Mitgliedstaaten der Zugang zu Strafverfolgungsdaten „mittelbar" erfolgt (d.h. über die nationale Datenschutzbehörde), wäre es sicherlich sinnvoll, eine Verpflichtung aufzunehmen, wonach die Datenschutzbehörden bei der Inanspruchnahme des Rechts auf Auskunft aktiv zusammenarbeiten.

6.3. **Recht auf Überprüfung der Entscheidung zur Eingabe einer Ausschreibung oder auf Widerspruch gegen diese Entscheidung**

In Artikel 15 Absatz 3 der Verordnung ist bestimmt, dass der Betroffene eine von einer Verwaltungtsbehörde getroffene Ausschreibungsentscheidung von einer Justizbehörde überprüfen lassen oder bei einer Justizbehörde ein Rechtsmittel dagegen einlegen kann. Dies ist gegenüber dem derzeitigen Schengener Durchführungsübereinkommen eine zu begrüßende Neuerung.

Damit wird unterstrichen, dass die Datensubjekte — wie in Nummer 6.1 ausgeführt — vollständig und rechtzeitig zu unterrichten sind. Ohne diese Information hätte dieses neue Recht einen rein virtuellen Charakter.

6.4. **Rechtsbehelfe**

In Artikel 30 der vorgeschlagenen Verordnung und Artikel 52 des vorgeschlagenen Beschlusses ist vorgesehen, dass das Datensubjekt das Recht hat, vor einem Gericht eines Mitgliedstaats Klage zu erheben oder eine Beschwerde einzulegen, wenn ihm das Recht auf Erteilung von Auskunft über die es betreffenden Daten, das Recht auf Berichtigung oder Löschung solcher Daten oder das Recht auf Information oder Schadenersatz verweigert wird.

Aufgrund der Formulierung („jede im Hoheitsgebiet eines Mitgliedstaats aufhältige Person") ist davon auszugehen, dass der Beschwerdeführer physisch im Hoheitsgebiet anwesend sein muss, um bei Gericht Klage zu erheben. Diese territoriale Beschränkung ist nicht gerechtfertigt und könnte das Recht, einen Rechtsbehelf einzulegen, unwirksam machen, da in sehr vielen Fällen der Beschwerdeführer gerade deshalb Klage erheben dürfte, weil ihm die Einreise ins Schengen-Gebiet verweigert wird. Ferner muss hinsichtlich der vorgeschlagenen Verordnung Artikel 22 der Richtlinie, die die *lex generalis* ist, berücksichtigt werden; dort ist vorgesehen, dass „jede Person" ungeachtet ihres Aufenthaltsortes das Recht hat, bei Gericht einen Rechtsbehelf einzulegen. Auch der vorgeschlagene Rahmenbeschluss enthält keine territoriale Beschränkung. Der EDPS schlägt vor, die territoriale Beschränkung in Artikel 30 der Verordnung und Artikel 52 des Beschlusses zu streichen.

7. **ÜBERWACHUNG**

7.1. **Einleitende Bemerkung: Aufteilung der Zuständigkeiten**

In den Vorschlägen wird die Aufgabe der Überwachung zwischen den nationalen Kontrollbehörden ([1]) und dem EDPS für ihren jeweiligen Bereich aufgeteilt. Dies entspricht dem mit den Vorschlägen verfolgten Ansatz in Bezug auf das geltende Recht und die Zuständigkeiten für Betrieb und Nutzung des SIS II sowie der Notwendigkeit einer wirksamen Überwachung.

Daher begrüßt der EDPS diesen in Artikel 31 des Verordnungsvorschlags und in Artikel 53 des Beschlussvorschlags enthaltenen Ansatz. Der EDPS schlägt zum besseren Verständnis und zur Präzisierung der jeweiligen Aufgaben jedoch vor, jeden Artikel in mehrere Bestimmungen aufzuteilen, wobei jede Bestimmung einem Überwachungsniveau entspricht, wie dies sachgemäß im VIS-Vorschlag gehandhabt wurde.

([1]) Die für Europol und Eurojust zuständigen Aufsichtsbehörden sind, wenn auch in geringerem Maße, ebenfalls beteiligt.

7.2. **Überwachung durch die nationalen Datenschutzbehörden**

Nach Artikel 31 der vorgeschlagenen Verordnung und Artikel 53 des vorgeschlagenen Beschlusses gewährleistet jeder Mitgliedstaat, dass eine unabhängige Behörde die Rechtmäßigkeit der Verarbeitung personenbezogener SIS-II-Daten kontrolliert.

In Artikel 53 des vorgeschlagenen Beschlusses wird jeder Einzelperson zusätzlich das Recht eingeräumt, von der Aufsichtsbehörde die Überprüfung der Rechtmäßigkeit der Verarbeitung der diese Person betreffenden Daten zu verlangen. In die Verordnung wurde keine entsprechende Bestimmung übernommen, da hier die Richtlinie als *lex generalis* gilt. Daher ist zu berücksichtigen, dass die nationalen Datenschutzbehörden in Bezug auf das SIS II alle ihnen mit Artikel 28 der Richtlinie 95/46/EG verliehenen Befugnisse — einschließlich der Überprüfung der Rechtmäßigkeit der Datenverarbeitung — ausüben können. Mit Artikel 31 Absatz 1 der Verordnung werden ihre Aufgaben präzisiert; er kann aber keine Begrenzung dieser Befugnisse darstellen. Die Anerkennung dieser Befugnisse sollte im Text der vorgeschlagenen Verordnung präziser zum Ausdruck kommen.

Was den vorgeschlagenen Beschluss anbelangt, so weist er den nationalen Kontrollbehörden umfassendere Aufgaben zu, da ihm eine andere *lex generalis* zugrunde liegt. Eine Situation, in der die Aufsichtsbehörden je nach Kategorie der verarbeiteten Daten unterschiedliche Aufgaben und Zuständigkeiten haben, ist nicht vernünftig und in der Praxis nur schwer handhabbar. Daher sollte dies vermieden werden, indem entweder diesen Behörden im Text des Beschlussvorschlags selbst oder durch Bezugnahme auf eine andere *lex generalis* (nämlich den Rahmenbeschluss über den Datenschutz im Bereich der dritten Säule) den Datenschutzbehörden mehr Befugnisse eingeräumt werden.

7.3. **Überwachung durch den EDPS**

Der EDPS wacht darüber, dass die Datenverarbeitungstätigkeiten der Kommission entsprechend den Vorschlägen durchgeführt werden. Desgleichen sollte der EDPS in der Lage sein, alle ihm nach der Verordnung (EG) Nr. 45/2001 zustehenden Befugnisse auszuüben, wobei jedoch die begrenzten Befugnisse der Kommission in Bezug auf die Daten selbst zu berücksichtigen sind.

Sinnvollerweise sei darauf hingewiesen, dass der EDPS nach Artikel 46 Buchstabe f der Verordnung (EG) Nr. 45/2001 „mit den einzelstaatlichen Kontrollstellen“ zusammenarbeitet, „soweit dies zur Erfüllung der jeweiligen Pflichten erforderlich ist“. Die Zusammenarbeit mit den Mitgliedstaaten bei der Überwachung des SIS II geht also nicht nur auf die Vorschläge, sondern auch auf die Verordnung (EG) Nr. 45/2001 zurück.

7.4 **Gemeinsame Kontrolle**

In den Vorschlägen wird eingeräumt, dass die Kontrolltätigkeiten der einzelnen beteiligten Behörden koordiniert werden müssen. In Artikel 31 der vorgeschlagenen Verordnung und in Artikel 53 des vorgeschlagenen Beschlusses ist bestimmt, dass „die nationalen Kontrollstellen und der Europäische Datenschutzbeauftragte“ aktiv zusammenarbeiten und der Europäische Datenschutzbeauftragte „zu diesem Zweck“ „mindestens einmal jährlich eine Zusammenkunft“ einberuft.

Der EDPS begrüßt diesen Vorschlag, der im Wesentlichen die erforderlichen Elemente für die Entwicklung der — wirklich unverzichtbaren — Zusammenarbeit zwischen den Behörden, die auf nationaler und auf europäischer Ebene mit der Überwachung betraut sind, enthält. Es sei darauf hingewiesen, dass in den Vorschlägen mindestens eine jährliche Zusammenkunft vorgesehen ist, dies jedoch als absolutes Minimum betrachtet werden soll.

Es wäre nützlich, in den betreffenden Bestimmungen (Artikel 31 der vorgeschlagenen Verordnung und Artikel 53 des vorgeschlagenen Beschlusses) den Inhalt dieser Koordinierung klarzustellen. Die bestehende Gemeinsame Kontrollinstanz (GK) ist für Probleme mit der Auslegung oder Anwendung des Übereinkommens, die Prüfung von Schwierigkeiten mit der Ausübung der unabhängigen Überwachung oder des Rechts auf Auskunft und die Ausarbeitung harmonisierter Vorschläge für die gemeinsame Lösung bestehender Probleme zuständig.

Die neuen Vorschläge dürfen nicht zu einer Verwässerung des derzeitigen Anwendungsbereichs der gemeinsamen Überwachung führen. Wenn davon ausgegangen wird, dass die Datenschutzbehörden in Bezug auf SIS II alle Kontrollbefugnisse ausüben können, mit denen sie nach der Richtlinie betraut sind, kann die Zusammenarbeit zwischen diesen Behörden breite Aspekte der Überwachung des SIS II abdecken; hierzu gehören auch die Aufgaben der bestehenden GK nach Maßgabe des Artikels 115 des Schengener Durchführungsübereinkommens.

Damit dies jedoch vollkommen klar wird, wäre es sinnvoll, es in den Vorschlägen auch ausdrücklich zu bekräftigen.

8. **SICHERHEIT**

Die Handhabung und die Wahrung eines optimalen Sicherheitsniveaus für das SIS II ist eine Grundvoraussetzung für die Gewährleistung eines angemessenen Schutzes der in der Datenbank gespeicherten Daten. Um ein derartiges ausreichendes Schutzniveau zu erreichen, bedarf es geeigneter Maßnahmen, um die potenziellen Gefahren im Zusammenhang mit der Infrastruktur des Systems und den daran beteiligten Personen abzuwenden. Dieses Thema wird nunmehr in Bezug auf verschiedene Teile der Vorschläge dargelegt; hier bedarf es einiger Verbesserungen.

Die Artikel 10 und 13 der Vorschläge enthalten verschiedene Maßnahmen zur Datensicherheit; ferner werden die verschiedenen Arten von Missbräuchen angegeben, die zu verhindern sind. Der EDPS begrüßt es, dass Bestimmungen über die systematische (Eigen-)Kontrolle der Sicherheitsmaßnahmen in diese Artikel aufgenommen wurden.

Artikel 59 des vorgeschlagenen Beschlusses und Artikel 34 der vorgeschlagenen Verordnung, in denen es um Kontrolle und Bewertung geht, sollten jedoch nicht nur auf die Aspekte Leistung, Kostenwirksamkeit und Dienstqualität abstellen, sondern auch auf die Einhaltung rechtlicher Anforderungen, insbesondere auf dem Gebiet des Datenschutzes. Daher empfiehlt der EDPS, dass der Anwendungsbereich dieser Artikel auf die Kontrolle der Rechtmäßigkeit der Verarbeitung und auf die entsprechende Berichterstattung ausgedehnt wird.

Ferner sollten Artikel 10 Absatz 1 Buchstabe f oder Artikel 18 des vorgeschlagenen Beschlusses und Artikel 17 der vorgeschlagenen Verordnung, in denen es um das zum Zugriff auf die Daten berechtigte Personal geht, dahingehend ergänzt werden, dass die Mitgliedstaaten (sowie Europol und Eurojust) sicherstellen sollten, dass genaue Benutzerprofile vorhanden sind (die für die nationalen Überwachungsbehörden für Überprüfungszwecke bereit gehalten werden sollten). Neben diesen Benutzerprofilen müssen die Mitgliedstaaten eine vollständige Liste der Benutzeridentitäten erstellen und ständig auf dem neuesten Stand halten. Das Gleiche gilt sinngemäß für die Kommission.

Diese Sicherheitsmaßnahmen werden durch Kontrollmaßnahmen und organisatorische Maßnahmen ergänzt. In Artikel 14 der Vorschläge ist jeweils festgelegt, unter welchen Bedingungen und für welche Zwecke Aufzeichnungen über alle Datenverarbeitungsvorgänge aufbewahrt werden müssen. Diese Aufzeichnungen sind nicht nur zur Datenschutzkontrolle und zur Gewährleistung der Datensicherheit aufzubewahren, sondern dienen auch zur Konsolidierung der in Artikel 10 vorgeschriebenen regelmäßigen Eigenkontrolle des SIS II. Die Berichte über die Eigenkontrolle werden zur wirksamen Abwicklung der Aufgaben der Aufsichtsbehörden beitragen; diese können dadurch nämlich die größten Schwachstellen ermitteln und sich bei ihren eigenen Kontrollverfahren darauf konzentrieren.

Wie in dieser Stellungnahme bereits erwähnt, muss eine Erhöhung der Zahl der Zugangsstellen des Systems sorgfältig begründet werden, da damit die Gefahr von Missbräuchen automatisch zunimmt. Daher sollte in beiden Vorschlägen in Artikel 4 Absatz 1 Buchstabe b vorgesehen werden, dass die Notwendigkeit einer zweiten Zugangsstelle konkret zu begründen ist.

In den Vorschlägen wird die Notwendigkeit der Erstellung nationaler Kopien des zentralen Systems nicht genau dargelegt, was Anlass zu ernsten Bedenken in Bezug auf das gesamte Gefährdungs- und Sicherheitsniveau des Systems gibt; hier wäre Folgendes zu nennen:

— Die Existenz weiterer Kopien erhöht die Gefahr von Missbräuchen (insbesondere in Anbetracht der Existenz neuer Daten wie etwa biometrischer Daten);

— es ist nicht genau bestimmt, welche Daten von diesen Kopien betroffen sind;

— die in Artikel 9 festgelegten Anforderungen an Genauigkeit, Qualität und Verfügbarkeit der Daten stellen große technische Herausforderungen dar und erhöhen somit je nach Stand der verfügbaren Technik die Kosten;

— die Überwachung der betreffenden Kopien durch die nationalen Behörden erfordert zusätzliches Personal und zusätzliche Mittel, die möglicherweise nicht immer zur Verfügung stehen.

In Anbetracht der möglichen Risiken ist der EDPS weder von der Notwendigkeit (unter Berücksichtigung der verfügbaren Technik) noch vom Zusatznutzen nationaler Kopien überzeugt. Er empfiehlt, dass auf die Möglichkeit, dass die Mitgliedstaaten nationale Kopien verwenden, verzichtet wird.

Für den Fall, dass die nationalen Kopien doch erstellt werden sollen, erinnert der EDPS daran, dass für ihre einzelstaatliche Verwendung der Grundsatz der Zweckbindung strikt eingehalten werden muss. Analog hierzu dürfen die nationalen Kopien niemals auf andere Art und Weise als die zentrale Datenbank abgefragt werden.

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten beruht auf der strikten Wahrung der Datensicherheit und der Datenintegrität. Der EDPS wird die betreffenden Vorgänge dann effizient überwachen können, wenn er mittels einer Analyse der verfügbaren Protokolle nicht nur die Sicherheit der Daten, sondern auch ihre Integrität kontrollieren kann. Daher muss die „Datenintegrität“ in Artikel 14 Absatz 6 aufgenommen werden.

9. **AUSSCHUSSVERFAHREN**

In den Vorschlägen sind für mehrere Fälle, in denen technische Entscheidungen über die Verwaltung des SIS II getroffen werden müssen, Ausschussverfahren vorgesehen. Wie aus ähnlichen Gründen in der Stellungnahme zum VIS ausgeführt wurde, werden sich diese Entscheidungen wesentlich auf die ordnungsgemäße Anwendung des Grundsatzes der Zweckbindung und des Verhältnismäßigkeitsprinzips auswirken.

Der EDPS empfiehlt, dass Entscheidungen mit wesentlichen Auswirkungen auf den Datenschutz — wie etwa Entscheidungen über den Zugang zu und die Eingabe von Daten, den Austausch von Zusatzinformationen, die Qualität der Daten und die Vereinbarkeit zwischen Ausschreibungen, die technische Übereinstimmung der nationalen Kopien usw. — im Wege einer Verordnung oder eines Beschlusses vorzugsweise im Wege eines Mitentscheidungsverfahren [1] getroffen werden sollten.

[1] Siehe hierzu auch die Stellungnahme des EDPS zum Visa-Informationssystem (Nummer 3.12) und die Stellungnahme des EDPS vom 26. September 2005 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden (Nummer 60).

In allen anderen Fällen, die sich auf den Datenschutz auswirken, sollte dem EDPS die Möglichkeit eingeräumt werden, die betreffenden Ausschüsse bei ihren Entscheidungen zu beraten.

Die beratende Rolle des EDPS sollte in die Artikel 60 und 61 des Beschlusses sowie in Artikel 35 der Verordnung aufgenommen werden.

In dem spezielleren Fall der technischen Regeln für die Verknüpfung von Ausschreibungen (Artikel 26 der Verordnung und Artikel 46 des Beschlusses) ist zu erläutern, warum der Rückgriff auf unterschiedliche Ausschussverfahren (beratender Ausschuss bei dem Beschluss und Regelungsausschuss bei der Verordnung) notwendig ist.

10. **INTEROPERABILITÄT**

Da die Mitteilung der Kommission über die Interoperabilität der neu entstehenden EU-Systeme noch aussteht, lässt sich der mit den geplanten, aber noch nicht bestimmten Synergien verbundene Zusatznutzen nur schwer abschätzen.

In diesem Zusammenhang möchte der EDPS auch auf die Erklärung des Rates vom 25. März 2004 zum Kampf gegen den Terrorismus verweisen, in der die Kommission aufgefordert wird, Vorschläge zur Verbesserung der Interoperabilität europäischer Datenbanken vorzulegen und zu erkunden, welche Synergieeffekte zwischen bestehenden und künftigen Informationssystemen (SIS II, VIS und EURODAC) geschaffen werden können. Der EDPS möchte ferner auf die auf die laufenden Beratungen über die Frage verweisen, welche Stelle künftig mit der Verwaltung der verschiedenen Großsysteme betraut werden könnte (siehe auch Nummer 3.8. dieser Stellungnahme).

Der EDPS hat bereits in seiner Stellungnahme zum VIS-System erklärt, dass die Interoperabilität eine wichtige und entscheidende Voraussetzung für die Effizienz von IT-Großsystemen wie dem VIS ist. Sie ermöglicht es, die Gesamtkosten konsequent zu senken und eine etwaige naturgemäße Redundanz heterogener Elemente aufzufangen.

— Die Interoperabilität kann ferner dem Ziel einer gemeinsamen Visumpolitik dienen, in einem Raum ohne Kontrollen an den Binnengrenzen zwischen den Mitgliedstaaten ein hohes Maß an Sicherheit zu wahren, indem für alle Bestandteile dieser Politik dieselben Verfahrensstandards vorgesehen werden. Allerdings ist es äußerst wichtig, zwischen zwei verschiedenen Interoperabilitätsgraden zu unterscheiden:

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

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

Unter den Schutzmaßnahmen, die zur Zweckbindung des Systems und zur Vorbeugung eines „function creep“ (schleichende Ausweitung der Anwendung des Systems) zur Verfügung stehen, kann die Verwendung unterschiedlicher technologischer Standards einen Beitrag zu dieser Zweckbegrenzung leisten. Darüber hinaus sollte jede Form der Interaktion zwischen zwei verschiedenen Systemen eingehend dokumentiert werden. Die Interoperabilität darf keinesfalls dazu führen, dass eine Behörde, die nicht berechtigt ist, Zugang zu bestimmten Daten zu haben oder letztere zu verwenden, einen solchen Zugang über ein anderes Informationssystem erhalten kann. Soweit den Vorschlägen entnommen werden kann, wird das SIS II beispielsweise in den ersten Jahren nicht über ein automatisiertes Fingerabdruck-Identifizierungssystem (AFIS) verfügen; es wird lediglich auf eine künftige Suchmaschine für die Abfrage biometrischer Daten verwiesen. Für den Fall, dass erwogen wird, die Fingerabdruckidentifizierungstechnologie anderer EU-Systeme zu verwenden, sollte dies zusammen mit den für derartige Synergien erforderlichen Schutzmaßnahmen genau dokumentiert werden.

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

11. **FAZIT**

11.1. **Allgemeines**

1. Der EDPS begrüßt mehrere positive Aspekte dieser Vorschläge, die in einigen Punkten eine Verbesserung gegenüber der derzeitigen Lage darstellen. Er erkennt an, dass die den Datenschutz betreffenden Bestimmungen im Allgemeinen mit großer Sorgfalt formuliert worden sind.

2. Nach Meinung des EDPS sollte die neue rechtliche Regelung trotz ihrer Komplexität

   — ein hohes Maß an Datenschutz gewährleisten,

   — sowohl für die Bürger als auch für die am Datenaustausch beteiligten Behörden verlässlich sein und

   — in ihrer Anwendung auf verschiedene Zusammenhänge (erste oder dritte Säule) kohärent sein.

3. Ferner sollte die Aufnahme neuer Komponenten in das SIS II, die die möglichen Auswirkungen des Systems auf das Leben der Menschen erhöhen, durch die in der Stellungnahme dargelegten stringentere Schutzmechanismen flankiert werden. Insbesondere gilt Folgendes:

   — Der Zugang zu den SIS-II-Daten darf neuen Behörden nicht ohne Nachweis der absoluten Notwendigkeit eingeräumt werden. Der Zugang sollte ferner so weit wie möglich begrenzt werden, und zwar sowohl hinsichtlich der Daten, zu denen der Zugang besteht, als auch hinsichtlich der zugangsberechtigten Personen.

   — Die Verknüpfung von Ausschreibungen darf niemals, auch nicht mittelbar, zu einer Änderung der Zugangsrechte führen.

   — Noch nicht verabschiedete Rechtsvorschriften dürfen nicht als stichhaltige Begründung für die Eingabe von Daten in das SIS II herangezogen werden (Ausschreibungen für die Zwecke der Einreiseverweigerung).

   — Die Rechtsgrundlage für den Zugang der für die Ausstellung von Kraftfahrzeugzulassungsbescheinigungen zuständigen Dienststellen sollte erneut geprüft werden, da damit im Wesentlichen das Ziel der Kriminalitätsbekämpfung verfolgt wird.

   — Der EDPS räumt ein, dass die Nutzung biometrischer Daten die Leistungsfähigkeit des Systems verbessern und für die Opfer von Identitätsdiebstahl hilfreich sein kann. Die Auswirkungen der Aufnahme dieser Daten scheinen jedoch noch nicht gründlich genug überdacht worden zu sein, und die Zuverlässigkeit der Daten wird allem Anschein nach überbewertet.

11.2. **Spezifische Bemerkungen**

1. Der EDPS begrüßt es, dass die Kommission anerkannt hat, dass die Verordnung (EG) Nr. 45/2001 für alle Datenverarbeitungstätigkeiten der Kommission im Rahmen des SIS II gilt, da dies dazu beitragen wird, eine kohärente und einheitliche Anwendung der Bestimmungen über den Schutz der Grundrechte und -freiheiten des Menschen bei der Verarbeitung personenbezogener Daten zu gewährleisten.

2. Zur Gewährleistung einer strengen Zweckbindung auf nationaler Ebene empfiehlt der EDPS, in die SIS-II-Vorschläge (nämlich Artikel 21 der vorgeschlagenen Verordnung und Artikel 40 des vorgeschlagenen Beschlusses) eine Bestimmung mit gleicher Zielrichtung wie in den derzeitigen Artikel 102 Absatz 4 des Schengener Durchführungsübereinkommens aufzunehmen, wonach die Möglichkeit der Mitgliedstaaten, eine nicht in den SIS-II-Texten vorgesehene Nutzung der Daten vorzusehen, beschränkt wird.

3. Wenn einer Behörde der Zugang zum SIS II gewährt wird, sollten strenge Voraussetzungen gelten:

   — Der Zugang muss mit dem allgemeinen Zweck des SIS II vereinbar sein und mit dessen Rechtsgrundlage im Einklang stehen.

   — Die Notwendigkeit des Zugangs zum SIS II muss nachgewiesen werden.

   — Die Zwecke, zu denen die Daten verwendet werden dürfen, müssen ausdrücklich und restriktiv festgelegt werden.

   — Die Voraussetzungen für den Zugang müssen präzise definiert und beschränkt werden. Insbesondere sollte eine aktualisierte Liste der zum Zugang zum SIS II berechtigten Personen unter Einschluss von Europol und Eurojust erarbeitet werden.

   — Der Umstand, dass diesen Behörden der Zugang zu SIS-II-Daten gewährt wird, darf niemals als Begründung dafür vorgebracht werden, dass Daten ins System eingegeben oder dort gespeichert werden, wenn sie für die spezifische Ausschreibung, zu der sie gehören, nicht von Nutzen sind.

   — Die Frist für die Speicherung der Daten darf nicht verlängert werden, wenn dies für den Zweck, für den die Daten eingegeben wurden, nicht erforderlich ist.

4. Was speziell Europol und Eurojust anbelangt, so fordert der EDPS die Kommission nachdrücklich auf, die Aufgaben, für deren Erledigung der Zugang zu den Daten gerechtfertigt wäre, restriktiv zu bestimmen. Ferner sollte der Zugang von Europol und Eurojust auf die Daten zu Einzelpersonen beschränkt werden, deren Name bereits in ihren Dateien erscheint. Es wird ferner vorgeschlagen, Europol und Eurojust nur eine Zugangsstelle zu gewähren.

5. Was die Ausschreibungen zum Zwecke der Einreiseverweigerung anbelangt, so sollten die auf noch nicht verabschiedeten Rechtsgrundlagen beruhenden Bestimmungen entweder gestrichen oder — gestützt auf geltende Rechtsvorschriften — dahingehend umformuliert werden, dass die betroffene Person in Erfahrung bringen kann, welche Maßnahmen die Behörden in Bezug auf ihre Person genau treffen können.

6. Die Fristen für die Speicherung der Daten sind verlängert worden, ohne dass dies stichhaltig begründet worden ist. Wenn es keine stichhaltigen Gründe für die Verlängerung gibt, sollte die geltende Dauer beibehalten werden, insbesondere bei Ausschreibungen zur verdeckten Registrierung oder zur gezielten Kontrolle.

7. Gemäß der Beschreibung der Rolle der Kommission ist diese für das Betriebsmanagement zuständig. In Verbindung mit ihrer führenden Rolle bei der Entwicklung und Wartung des Systems sollte dies als eine Kontrollaufgabe sui generis betrachtet werden. Diese Kontrollaufgabe umfasst zwar mehr als die eine Verarbeitungsstelle, ist aber auch eingeschränkter als die einer gewöhnlichen Kontrollstelle, da die Kommission keinen Zugang zu den im SIS II verarbeiteten Daten hat.

   Aufgrund dieser Aufgabe sollte in Artikel 12 beider Vorschläge hinzugefügt werden, dass die Kommission regelmäßig die Anwendung neuer Technologien vorschlagen sollte, die dem Stand der Technik auf diesem Gebiet entsprechen und das Niveau des Datenschutzes und der Sicherheit erhöhen.

8. Zur Rolle der Mitgliedstaaten muss präzisiert werden, welche Behörden Kontrollbehörden sein werden.

9. In Bezug auf die Erteilung von Informationen an die Datensubjekte gilt Folgendes:

   — In der vorgeschlagenen Verordnung sollten einige Informationen zusätzlich in die Liste aufgenommen werden: die für die Daten geltende Speicherungsfrist, das Bestehen des Rechts, eine Überprüfung zu beantragen oder Widerspruch gegen eine Ausschreibung einzulegen, die Möglichkeit der Unterstützung durch die Datenschutzbehörde und die Möglichkeit, Rechtsmittel einzulegen.

   — In dem vorgeschlagenen Beschluss sollte Artikel 50 geändert werden, damit das Recht auf Auskunft nicht von einem Antrag des Datensubjekts abhängig gemacht wird.

10. Was die Fristen für die Beantwortung von Auskunftsersuchen anbelangt, so ist die Festlegung von Fristen in den Vorschlägen zu begrüßen. Es sollte präzisiert werden, dass in den Fällen, in denen auch die nationalen Rechtsvorschriften Fristen vorgeben, die für das Datensubjekt günstigsten Fristen gelten sollten.

    Ferner wäre es sinnvoll, die Datenschutzbehörden zur aktiven Zusammenarbeit in Bezug auf die Inanspruchnahme des Auskunftsrechts zu verpflichten.

11. Zu dem Recht, Rechtsbehelfe einzulegen, schlägt der EDPS vor, die territoriale Beschränkung in Artikel 30 bzw. Artikel 52 zu streichen.

12. Hinsichtlich der Befugnisse der nationalen Datenschutzbehörden gilt Folgendes:

    — Verordnung: Es ist in Betracht zu ziehen, dass die nationalen Datenschutzbehörden in Bezug auf das SIS II alle ihnen mit Artikel 28 der Richtlinie 95/46/EG verliehenen Befugnisse ausüben können; dies sollte im Text der vorgeschlagenen Verordnung präzisiert werden.

    — Beschluss: Den Aufsichtsbehörden sollten die gleichen Befugnisse wie nach der Verordnung/Richtlinie zuerkannt werden.

13. Was die Befugnisse des EDPS anbelangt, so sollte er in der Lage sein, alle ihm nach der Verordnung (EG) Nr. 45/2001 verliehenen Befugnisse auszuüben, wobei jedoch den begrenzten Befugnissen der Kommission in Bezug auf die Daten selbst Rechnung zu tragen ist.

14. Zur koordinierten Überwachung ist zu bemerken, dass in den Vorschlägen auch anerkannt wird, dass die Überwachungstätigkeiten der einzelnen beteiligten Behörden koordiniert werden müssen. Der EDPS begrüßt es, dass die Vorschläge im Großen und Ganzen die erforderlichen Elemente enthalten, um die Zusammenarbeit zwischen den auf nationaler und auf europäischer Ebene für die Überwachung zuständigen Behörden zu entwickeln. Es wäre jedoch nützlich, in die betreffenden Bestimmungen (Artikel 31 der vorgeschlagenen Verordnung und Artikel 53 des vorgeschlagenen Beschlusses) einige präzisere Angaben zum Inhalt dieser Koordinierung aufzunehmen.

15. Die Artikel 10 und 13 der Vorschläge enthalten verschiedene Maßnahmen zur Datensicherheit; die Aufnahme von Bestimmungen über die systematische (Eigen-)Kontrolle der Sicherheitsmaßnahmen in diese Artikel ist zu begrüßen.

    — Artikel 59 des vorgeschlagenen Beschlusses und Artikel 34 der vorgeschlagenen Verordnung, in denen es um Kontrolle und Bewertung geht, sollten jedoch nicht nur die Aspekte Leistung, Kostenwirksamkeit und Dienstqualität behandeln, sondern auch die Einhaltung rechtlicher Anforderungen, insbesondere auf dem Gebiet des Datenschutzes. Diese Bestimmungen sollten entsprechend geändert werden.

    — Ferner sollte in Artikel 10 Absatz 1 Buchstabe f oder in Artikel 18 des vorgeschlagenen Beschlusses und Artikel 17 der vorgeschlagenen Verordnung zusätzlich vorgesehen werden, dass die Mitgliedstaaten, Europol und Eurojust sicherstellen sollten, dass genaue Benutzerprofile vorhanden sind (die für die nationalen Kontrollbehörden für Überprüfungszwecke bereit gehalten werden sollten). Über diese Benutzerprofile hinaus müssen die Mitgliedstaaten eine vollständige Liste der Benutzeridentitäten aufstellen und ständig auf dem neuesten Stand zu halten. Das Gleiche gilt sinngemäß für die Kommission.

    — Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten beruht auf der strikten Wahrung der Datensicherheit und der Datenintegrität. Der EDPS sollte deshalb in der Lage sein, mittels einer Analyse der verfügbaren Protokolle nicht nur die Sicherheit der Daten, sondern auch ihre Integrität zu kontrollieren. Daher muss die „Datenintegrität“ in Artikel 14 Absatz 6 aufgenommen werden.

16. Die Verwendung nationaler Kopien kann viele zusätzliche Risiken nach sich ziehen. Der EDPS ist weder von der Notwendigkeit (in Anbetracht der verfügbaren Technik) noch vom Zusatznutzen der nationalen Kopien überzeugt. Er empfiehlt, dass auf die Möglichkeit, dass die Mitgliedstaaten nationale Kopien verwenden, verzichtet wird bzw. diese so weit wie möglich beschränkt wird. Für den Fall, dass die nationalen Kopien doch erstellt werden sollen, muss bei ihrer einzelstaatlichen Verwendung der Grundsatz der Zweckbindung strikt eingehalten werden. Analog hierzu dürfen die nationalen Kopien niemals auf andere Art und Weise als die zentrale Datenbank abgefragt werden.

17. Zum Ausschussverfahren wäre festzuhalten, dass Entscheidungen mit wesentlichen Auswirkungen auf den Datenschutz im Wege einer Verordnung oder eines Beschlusses getroffen werden sollten, vorzugsweise nach dem Mitentscheidungsverfahren. Wird tatsächlich ein Ausschussverfahren gewählt, so sollte die beratende Rolle des EDPS in die Artikel 60 und 61 des Beschlusses sowie in Artikel 35 der Verordnung aufgenommen werden.

18. Die Interoperabilität der Systeme darf nicht unter Verletzung des Grundsatzes der Zweckbindung umgesetzt werden, und alle einschlägigen Vorschläge sollten dem EDPS unterbreitet werden.

Geschehen zu Brüssel am 19. Oktober 2005

Peter HUSTINX

Der Europäische Datenschutzbeauftragte