# DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

## Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (KOM(2005) 475 endgültig)

(2006/C 47/12)

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 das Ersuchen um Stellungnahme nach Artikel 28 Absatz 2 der 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 —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

### I. VORBEMERKUNGEN

*Konsultation des EDPS*

1. Der Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, wurde dem EDPS von der Kommission mit Schreiben vom 4. Oktober 2005 übermittelt. Der EDPS versteht dieses Schreiben als Ersuchen um Beratung der Organe und Einrichtungen der Gemeinschaft nach Artikel 28 Absatz 2 der Verordnung Nr. 45/2001/EG. Dem EDPS zufolge sollte die vorliegende Stellungnahme in der Präambel des Rahmenbeschlusses erwähnt werden.

*Bedeutung des vorliegenden Vorschlags*

2. Der EDPS unterstreicht die Bedeutung des vorliegenden Vorschlags unter dem Gesichtspunkt, dass der Schutz personenbezogener Daten zu den Grundrechten und Grundfreiheiten natürlicher Personen zählt. Die Annahme dieses Vorschlags würde einen bedeutenden Fortschritt für den Schutz personenbezogener Daten in einem wichtigen Bereich bedeuten, in dem ein kohärenter und effizienter Mechanismus für den Schutz personenbezogener Daten auf EU-Ebene besonders notwendig ist.

3. Der EDPS unterstreicht in diesem Zusammenhang, dass die polizeiliche und justizielle Zusammenarbeit zwischen den Mitgliedstaaten als Element der fortschreitenden Schaffung eines Raums der Freiheit, der Sicherheit und des Rechts zunehmend an Bedeutung gewinnt. Mit dem Haager Programm wurde zur Verbesserung des grenzüberschreitenden Austauschs strafverfolgungsrelevanter Informationen zwischen den Mitgliedstaaten der Grundsatz der Verfügbarkeit eingeführt. Laut dem Haager Programm ([1]) sollte der bloße Umstand, dass Informationen Grenzen überschreiten, nicht länger von Bedeutung sein. Die Einführung des Grundsatzes der Verfügbarkeit spiegelt einen allgemeineren Trend zur Erleichterung des Austauschs strafverfolgungsrelevanter Informationen wider (siehe beispielsweise den von sieben Mitgliedstaaten unterzeichneten Prümer Vertrag ([2]) und den Vorschlag Schwedens für einen Rahmenbeschluss über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden ([3])). Unter demselben Gesichtspunkt kann die jüngst erfolgte Billigung einer Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten ([4]) durch das Europäische Parlament betrachtet werden. Diese Entwicklungen machen die Annahme eines Rechtsinstruments zur Gewährleistung eines wirksamen Schutzes personenbezogener Daten in allen EU-Mitgliedstaaten auf der Grundlage gemeinsamer Standards erforderlich.

([1]) Seite 18 des Programms.

([2]) Vertrag zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreich Spanien, der Französischen Republik, dem Großherzogtum Luxemburg, dem Königreich der Niederlande und der Republik Österreich über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration, Prüm (Deutschland) 27. Mai 2005.

([3]) Initiative des Königreichs Schweden im Hinblick auf die Annahme eines Rahmenbeschlusses über die Vereinfachung des Austauschs von Informationen und Geheimdienstinformationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, insbesondere in Bezug auf schwerwiegende Straftaten einschließlich terroristischer Handlungen (ABl. C 281 vom 18.11.2004).

([4]) Grundlage: Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM (2005) 438 endgültig).

4. Der EDPS weist darauf hin, dass der derzeitige allgemeine datenschutzrechtliche Rahmen in diesem Bereich unzulänglich ist. Zum einen ist die Richtlinie 95/46/EG nicht auf die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten anwendbar, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, wie dies bei Daten im Sinne von Titel VI EUV der Fall ist (Artikel 3 Absatz 2 der Richtlinie). Obwohl in den meisten Mitgliedstaaten der Anwendungsbereich der Umsetzungsbestimmungen breiter gefasst ist als die Richtlinie selbst dies fordert und eine Datenverarbeitung zum Zwecke der Strafverfolgung nicht ausschließt, gibt es erhebliche Unterschiede zwischen den einzelstaatlichen Rechtsvorschriften. Zum anderen wird in dem Übereinkommen Nr. 108 des Europarates ([1]), durch das alle Mitgliedstaaten gebunden sind, der Schutz nicht hinreichend präzisiert, wie dies bereits zum Zeitpunkt der Annahme der Richtlinie 95/46/EC konstatiert wurde. Drittens trägt keines dieser beiden Rechtsinstrumente den spezifischen Merkmalen des Austauschs von Daten durch Polizei- und Justizbehörden Rechnung ([2]).

*Ein Beitrag zum Erfolg der eigentlichen Zusammenarbeit*

5. Ein wirksamer Schutz personenbezogener Daten ist nicht nur für die betroffenen Personen wichtig, sondern trägt auch zum Erfolg der polizeilichen und justiziellen Zusammenarbeit an sich bei. In vielen Aspekten greifen beide öffentlichen Interessen eng ineinander.

6. Dabei ist zu berücksichtigen, dass die betreffenden personenbezogenen Daten häufig besonders schützenswert sind, und von den Polizei- und Justizbehörden im Rahmen von Personenermittlungen erlangt wurden. Die Bereitschaft, derartige Daten mit Behörden anderer Mitgliedstaaten auszutauschen, ist größer, wenn eine Behörde Gewissheit über das Schutzniveau in dem anderen Mitgliedstaat hat. Als datenschutzrelevante Elemente führt der EDPS die Vertraulichkeit und die Sicherheit der Daten sowie die Beschränkungen des Zugangs und der Weiterverwendung an.

7. Darüber hinaus kann ein hohes Datenschutzniveau Gewähr für die Richtigkeit und Zuverlässigkeit der personenbezogenen Daten bieten. Noch wichtiger sind Richtigkeit und Zuverlässigkeit dieser Daten, wenn sie zwischen Polizei- und/oder Justizbehörden ausgetauscht werden, insbesondere weil Daten nach mehreren Austauschen und Übermittlungen zwischen Strafverfolgungsbehörden schließlich weitab von ihrer Quelle und nicht mehr in dem Kontext, in dem sie ursprünglich erhoben und genutzt wurden, weiterverarbeitet werden. Den Empfängerbehörden liegen in der Regel keine Informationen zu den Begleitumständen vor, und sie müssen sich einzig und allein auf die Daten selbst verlassen.

8. Die Harmonisierung der einzelstaatlichen Rechtsvorschriften über personenbezogene Daten im Polizei- und Justizbereich — einschließlich angemessener Garantien für den Schutz dieser Daten — kann somit dem gegenseitigen Vertrauen und gleichzeitig der Wirksamkeit des eigentlichen Austauschs förderlich sein.

*Achtung der Datenschutzgrundsätze in Verbindung mit einem ergänzenden Normenwerk*

9. Bei mehreren Gelegenheiten wurde Nachdruck auf die Notwendigkeit und Bedeutung des vorliegenden Vorschlags gelegt. Die europäischen Datenschutzbehörden haben im April 2005 auf ihrer Frühjahrkonferenz in Krakau eine Erklärung verabschiedet und ein Positionspapier gebilligt, in denen sie zur Annahme eines für Tätigkeiten der dritten Säule geltenden neuen Rechtsrahmens für den Datenschutz aufriefen. Dieser neue Rahmen muss nicht nur die Datenschutzgrundsätze der Richtlinie 95/46/EC wahren (es ist wichtig, dass die Einheitlichkeit des Datenschutzes innerhalb der Europäischen Union gewährleistet ist), sondern auch ein ergänzendes Normenwerk vorsehen, das den Besonderheiten des Strafverfolgungsbereichs Rechnung trägt ([3]). Der EDPS begrüßt, dass diese Ausgangspunkte in dem vorliegenden Vorschlag berücksichtigt wurden: Der Vorschlag wahrt die Datenschutzgrundsätze der Richtlinie 95/46/EC und sieht ein ergänzendes Normenwerk vor.

10. In dieser Stellungnahme wird unter gebührender Berücksichtigung des besonderen Kontextes des Datenschutzes im Strafverfolgungsbereich analysiert, inwieweit das Ergebnis aus datenschutzrechtlicher Sicht annehmbar ist. Einerseits sind die betreffenden Daten relativ häufig besonders schützenswert (siehe Nummer 6 dieser Stellungnahme), andererseits wird massiver Druck dahin gehend ausgeübt, im Hinblick auf eine wirksame Strafverfolgung, wozu der Schutz des Lebens und der körperlichen Sicherheit von Personen zählen kann, Zugang zu diesen Daten zu erhalten. Nach Ansicht des EDPS sollten die Datenschutzbestimmungen auf die berechtigten Erfordernisse der Strafverfolgung eingehen, den Betroffenen aber auch vor ungerechtfertigter Verarbeitung und ungerechtfertigtem Zugriff schützen. Um mit dem Grundsatz der Verhältnismäßigkeit vereinbar zu sein, müssen die Überlegungen des europäischen Gesetzgebers der Achtung der beiden potenziell entgegen gesetzten öffentlichen Interessen Rechnung tragen. In diesem Zusammenhang weist der EDPS nochmals darauf hin, dass die beiden Interessen häufig ineinander greifen.

*Kontext des Titels VI des Vertrags über die Europäische Union (EUV)*

11. Schließlich ist noch zu erwähnen, dass dieser Vorschlag Teil von Titel VI des EU-Vertrags, der so genannten dritten Säule, darstellt. Das Tätigwerden des europäischen Gesetzgebers unterliegt präzisen Einschränkungen: Beschränkung der Gesetzgebungsbefugnisse der Union auf die in den Artikeln 30 und 31 genannten Angelegenheiten, Einschränkungen hinsichtlich des Gesetzgebungsverfahrens, an dem das Europäische Parlament nicht voll und ganz beteiligt ist, und Einschränkungen hinsichtlich der gerichtlichen Kontrolle, da die Zuständigkeiten des Europäischen Gerichtshofs nach Artikel 35 EUV nicht umfassend sind. Diese Einschränkungen machen eine noch sorgfältigere Analyse des Wortlauts des Vorschlags erforderlich.

([1]) Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.

([2]) 1987 hat der Europarat die Empfehlung Nr. R (87) 15 über die Nutzung personenbezogener Daten im Polizeibereich angenommen, die jedoch ihrem Wesen nach für die Mitgliedstaaten nicht bindend ist.

([3]) Siehe in diesem Sinne das auf www.edps.eu.int veröffentliche Strategiepapier vom 18. März 2005 „Der Europäische Datenschutzbeauftragte als Berater der Organe und Einrichtungen der Gemeinschaft im Zusammenhang mit Vorschlägen für Rechtsvorschriften und zugehörigen Dokumenten".

## II. KONTEXT: INFORMATIONSAUSTAUSCH NACH DEM GRUNDSATZ DER VERFÜGBARKEIT, VORRATSDATENSPEICHERUNG UND SPEZIFISCHE RAHMENBEDINGUNGEN DES SIS II UND DES VIS

### II.1. Grundsatz der Verfügbarkeit

12. Der vorliegende Vorschlag steht in engem Zusammenhang mit dem Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit (KOM(2005) 490 endgültig). Letzterer zielt auf die Einführung des Verfügbarkeitsgrundsatzes ab, wodurch gewährleistet werden soll, dass Informationen, die den zuständigen Behörden eines Mitgliedstaates zur Kriminalitätsbekämpfung vorliegen, den entsprechenden Behörden anderer Mitgliedstaaten zur Verfügung gestellt werden. Dadurch, dass der Informationsaustausch unionsweit einheitlichen Bedingungen unterworfen wird, sollen die Binnengrenzen für den Austausch solcher Informationen beseitigt werden.

13. Die enge Verknüpfung zwischen den beiden Vorschlägen ergibt sich daraus, dass es sich bei strafverfolgungsrelevanten Informationen weitgehend um personenbezogene Daten handelt. Rechtsvorschriften über den Austausch strafverfolgungsrelevanter Informationen können nur unter der Voraussetzung verabschiedet werden, dass für einen angemessenen Schutz personenbezogener Daten gesorgt wird. Führt ein Tätigwerden auf EU-Ebene zum Wegfall der Binnengrenzen für den Austausch dieser Informationen, so kann der Schutz personenbezogener Daten nicht mehr nur durch nationales Recht geregelt werden. Die Gewährleistung des Schutzes personenbezogener Daten im Unionsgebiet ohne Binnengrenzen ist zur Aufgabe der europäischen Organe geworden. Diese Aufgabe wird ausdrücklich in Artikel 30 Absatz 1 Buchstabe b EUV festgelegt und geht auf die Verpflichtung der Union zur Achtung der Grundrechte (Artikel 6 EUV) zurück. Hinzu kommt Folgendes:

— Artikel 1 Absatz 2 des vorliegenden Vorschlags besagt ausdrücklich, dass die Mitgliedstaaten den grenzüberschreitenden Informationstransfer nicht länger aus datenschutzrechtlichen Gründen einschränken oder untersagen dürfen.

— In dem Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit wird mehrmals auf den vorliegenden Vorschlag Bezug genommen.

14. Der EDPS weist darauf hin, dass ein Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit nur unter der Voraussetzung verabschiedet werden sollte, dass auch ein Rahmenbeschluss über den Schutz personenbezogener Daten angenommen wird. Dieser Vorschlag für einen Rahmenbeschluss des Rates über den Datenschutz hat jedoch seine eigenen Vorzüge und wird auch ohne Rechtsinstrument über die Verfügbarkeit benötigt. Dies wurde in Abschnitt I dieser Stellungnahme hervorgehoben.

15. Der EDPS wird die beiden Vorschläge daher in zwei getrennten Stellungnahmen analysieren. Dies hat auch praktische Gründe. Es gibt nämlich keine Gewähr dafür, dass die Vorschläge im Rat und im Europäischen Parlament gemeinsam und gleichermaßen zügig behandelt werden.

### II.2. Vorratsspeicherung von Daten

16. Der EDPS hat am 26. September 2005 seine Stellungnahme zu dem Vorschlag für eine Richtlinie über die Vorratsspeicherung von Kommunikationsdaten [1] vorgelegt. Er wies darin auf einige schwerwiegende Mängel des Vorschlags hin und schlug vor, dass der Richtlinie konkrete Bestimmungen über den Zugang der zuständigen Behörden zu den Verkehrs- und Standortdaten und über die Weiterverwendung der Daten sowie zusätzliche Datenschutzgarantien hinzugefügt werden. Der Wortlaut der vom Europäischen Parlament und vom Rat angenommenen Richtlinie enthält eine begrenzte — aber keineswegs ausreichende — Bestimmung über den Datenschutz und die Datensicherheit und umfasst eine noch unzulänglichere Bestimmung über den Zugang, wobei für das Ergreifen von Maßnahmen auf einzelstaatliches Recht vorbehaltlich der einschlägigen Bestimmungen des Unionsrechts bzw. des Völkerrechts verwiesen wird.

17. Aufgrund der Billigung der Richtlinie über die Vorratsspeicherung von Kommunikationsdaten ist es noch dringender erforderlich, dass ein Rechtsrahmen für den Datenschutz in der dritten Säule geschaffen wird. Durch die Annahme dieser Richtlinie erlegt der Gemeinschaftsgesetzgeber den Anbietern von Telekommunikations- und Internetdiensten die Verpflichtung zur Vorratsspeicherung von Daten zu Strafverfolgungszwecken auf, ohne die erforderlichen angemessenen Garantien für den Schutz der Betroffenen. Der Schutz ist allerdings in einem wichtigen Punkt weiterhin lückenhaft, da in der Richtlinie weder (in ausreichendem Maße) auf den Zugang zu den Daten eingegangen wird, noch auf deren Weiterverwendung, sobald sie von den für die Strafverfolgung zuständigen Behörden abgerufen wurden.

18. Mit dem vorliegenden Vorschlag wird diese Lücke größtenteils geschlossen, da er für die Weiterverwendung der von Strafverfolgungsbehörden abgerufenen Daten anwendbar ist. Der EDPS bedauert indes, dass weder in dem Vorschlag der Zugang zu diesen Daten behandelt wird. Im Gegensatz zu dem, was für die Systeme SIS II und VIS vorgesehen ist (siehe Abschnitt II.3 dieser Stellungnahme), bleibt dieser Aspekt den Nationalgesetzgebern überlassen.

### II.3. Verarbeitung im Rahmen des SIS II und des VIS

19. Die EU nutzt bzw. entwickelt zurzeit mehrere groß angelegte Informationssysteme (Eurodac, SIS II, VIS) und strebt Synergien zwischen diesen an. Die Tendenz geht auch zunehmend dahin, zu Strafverfolgungszwecken einen weiter gehenden Zugang zu diesen Systemen zu gewähren. Bei diesen weit reichenden Entwicklungen ist nach dem Haager Programm auch „dem Erfordernis, das richtige Verhältnis zwischen Strafverfolgungszwecken und der Wahrung der Grundrechte zu finden, Rechnung zu tragen".

[1] Stellungnahme des Europäischen Datenschutzbeauftragten 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, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005) 438 endg.), veröffentlicht unter www.edps.eu.int

20. Der EDPS hat in seiner Stellungnahme vom 19. Oktober 2005 zu dem Vorschlag für die zweite Generation des Schengener Informationssystems (SIS II) [1] einige Aspekte im Zusammenhang mit der gleichzeitigen Anwendung allgemeiner Bestimmungen (*lex generalis*) und speziellen Bestimmungen (*lex specialis)* über den Datenschutz hervorgehoben. Dieser Vorschlag kann als *lex generalis* betrachtet werden, der das Übereinkommen Nr. 108 im Rahmen der dritten Säule ersetzt [2].

21. Der EDPS hebt in diesem Zusammenhang hervor, dass der Vorschlag auch einen allgemeinen datenschutzrechtlichen Rahmen für spezifische Rechtsinstrumente wie den die dritten Säule betreffenden Teil des SIS II und den Zugang der Strafverfolgungsbehörden zum Visa-Informationssystem vorsieht [3].

## III. **KERNPUNKT DES VORSCHLAGS**

### III.1. **Für jede Verarbeitung geltende gemeinsame Standards**

*Ausgangspunkt*

22. Dieser Vorschlag zielt nach Artikel 1 Absatz 1 darauf ab, einheitliche Bestimmungen zum Schutz personenbezogener Daten im Rahmen von Maßnahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen festzulegen. Artikel 1 Absatz 1 ist in Verbindung mit Artikel 3 Absatz 1 zu lesen, wonach der Vorschlag für die (…) Verarbeitung personenbezogener Daten durch eine zuständige Behörde zum Zwecke der Verhütung, Ermittlung, Untersuchung und Verfolgung von Straftaten gilt.

23. Aus diesen Bestimmungen ergeben sich die zwei Hauptmerkmale des vorgeschlagenen Rahmenbeschlusses: Er legt gemeinsame Standards fest und gilt für jede Verarbeitung zum Zwecke der Durchsetzung strafrechtlicher Bestimmungen, selbst wenn die betreffenden Daten nicht von den zuständigen Behörden anderer Mitgliedstaaten übermittelt oder zur Verfügung gestellt wurden.

24. Der EDPS unterstreicht die Bedeutung dieser beiden Hauptmerkmale. Der Anspruch dieses Vorschlags sollte sein, einen Rahmen für den Datenschutz festzulegen, der den in der ersten Säule bereits bestehenden Rechtsrahmen umfassend ergänzt. Nur unter dieser Voraussetzung wird die EU ihrer Verpflichtung nach Artikel 6 Absatz 2 EUV vollauf gerecht, die Grundrechte, wie sie in der EMRK gewährleistet sind, zu achten.

*Gemeinsame Standards*

25. Zum ersten Merkmal: Mit diesem Vorschlag soll gewährleistet werden, dass die geltenden Datenschutzgrundsätze in der dritten Säule angewandt werden. Zudem sind darin gemeinsame Standards vorgesehen, die diese Grundsätze näher bestimmen, damit sie in diesem Bereich Anwendung finden können. Der EDPS hält diese Aspekte des Vorschlags für besonders wichtig. Sie spiegeln den spezifischen und sensitiven Charakter der Verarbeitung personenbezogener Daten in diesem Bereich wider. Der EDPS begrüßt insbesondere, dass ergänzend zu den bestehenden Datenschutzgrundsätzen der Grundsatz der Unterscheidung zwischen personenbezogenen Daten von verschiedenen Personengruppen als spezieller Datenschutzgrundsatz für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen eingeführt wird (Artikel 4 Absatz 4). Nach Ansicht des EDPS sollte der eigentliche Grundsatz und seine rechtlichen Folgen für den Betroffenen sogar *noch präziser* umrissen werden (siehe Nummern 88–92 dieser Stellungnahme).

26. Die Vorschriften müssen für unterschiedliche Situationen gelten und dürfen daher nicht zu detailliert sein. Andererseits müssen sie dem Bürger die nötige Rechtssicherheit sowie einen angemessenen Schutz der Daten zu seiner Person bieten. Nach Ansicht des EDPS stehen diesen beiden potenziell widersprüchlichen gesetzlichen Anforderungen in diesem Vorschlag in einem ausgewogenen Verhältnis zueinander. Die Bestimmungen belassen im Bedarfsfall Flexibilität, sind in den meisten Bereichen jedoch präzise genug, um den Bürger zu schützen.

27. In einigen Punkten ist der Vorschlag allerdings zu flexibel und bietet nicht die erforderlichen Garantien. In Artikel 7 Absatz 1 sieht der Vorschlag beispielsweise eine allgemeine Ausnahmeregelung zu den Garantien unter dem alleinigen Vorbehalt „sofern nicht durch innerstaatliche Rechtsvorschriften etwas anderes bestimmt wird“ vor. Der Umstand, dass ein derart weit gefasster Ermessensspielraum belassen wird, um die Daten länger als für den beabsichtigten Zweck zu speichern, wäre nicht nur mit dem Grundrecht auf Datenschutz unvereinbar, sondern würde sich auch nachteilig auswirken in Bezug auf den dringenden Bedarf an Harmonisierung auf dem Gebiet des Schutzes personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.

28. Ausnahmeregelungen sollten im Bedarfsfall auf Rechtsvorschriften — auf nationaler oder EU-Ebene — zum Schutz spezifischer öffentlicher Interessen beschränkt bleiben. Diese öffentlichen Interessen sollten in Artikel 7 Absatz 1 genannt werden.

29. Dies leitet zu einem weiteren Punkt über. Wann immer ein anderer spezifischer Rechtsakt nach Titel VI des EU-Vertrags präzisere Bedingungen oder Beschränkungen für die Verarbeitung von Daten oder den Zugang zu Daten vorsieht, sollten diese spezifischen Rechtsvorschriften als *lex specialis* gelten. Artikel 17 dieses Vorschlags sieht Ausnahmen von den Artikeln 12, 13, 14 und 15 vor, wenn in speziellen Vorschriften nach Titel VI besondere Bedingungen für die Übermittlung von Daten festgelegt sind. Dies zeigt, wie allgemein der Vorschlag gehalten ist (siehe vorstehende Erläuterungen), wobei jedoch nicht alle

[1] Nummer 2.2.4 der Stellungnahme.

[2] Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981.

[3] Vorschlag für einen Beschluss des Rates über den Zugang der für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Prävention, Ermittlung und Untersuchung terroristischer und sonstiger schwerwiegender Straftaten (KOM (2005) 600 endgültig) vom 24. November 2005. Der EDPS wird Anfang 2006 seine Stellungnahme hierzu abgeben.

Hypothesen abgedeckt sind. Nach Auffassung des EDPS sollte Artikel 17

— allgemeiner gefasst sein: Falls es spezifischere Rechtsvorschriften gibt, die irgendeinen Aspekt der Datenverarbeitung (nicht nur die Datenübermittlung) regeln, so gelten diese spezifischen Rechtsvorschriften;

— die Garantie vorsehen, dass das Schutzniveau nicht durch Ausnahmeregelungen gemindert werden darf.

*Anwendbar auf jede Verarbeitung*

30. Zum zweiten Merkmal: Das ideale Ergebnis wäre, jede Erhebung und Verarbeitung personenbezogener Daten im Rahmen der dritten Säule abzudecken.

31. Der Rahmenbeschluss muss zur Verwirklichung seines Ziels unbedingt alle polizeilichen und justiziellen Daten einbeziehen, selbst wenn diese nicht von den zuständigen Behörden anderer Mitgliedstaaten übermittelt oder zur Verfügung gestellt werden.

32. Dies ist umso wichtiger, da jegliche Beschränkung auf Daten, die an die zuständigen Behörden in anderen Mitgliedstaaten übermittelt oder diesen zur Verfügung gestellt werden, zu großer Ungewissheit und Unsicherheit bezüglich des Anwendungsbereichs des Rahmenbeschlusses führen würde, was dem grundlegenden Ziel des Rahmenbeschlusses zuwiderlaufen würde ([1]). Die Rechtssicherheit des Einzelnen wäre beeinträchtigt. Unter normalen Umständen steht — zum Zeitpunkt der Erhebung oder Verarbeitung personenbezogener Daten — nicht von vornherein fest, ob diese Daten für einen Austausch mit den zuständigen Behörden anderer Mitgliedstaaten von Belang sein werden. Der EDPS verweist in diesem Zusammenhang auf den Grundsatz der Verfügbarkeit und auf die Abschaffung der Binnengrenzen für den Austausch strafverfolgungsrelevanter Daten.

33. Schließlich stellt der EDPS fest, dass der Vorschlag nicht gilt für

— die Verarbeitung im Rahmen der zweiten Säule des EU-Vertrags (Gemeinsame Außen- und Sicherheitspolitik),

— die Verarbeitung von Daten durch Nachrichtendienste und den Zugriff dieser Dienste auf diese Daten, wenn diese durch die zuständigen Behörden oder andere Parteien verarbeitet werden (dies ergibt sich aus Artikel 33 EUV).

In diesen Bereichen müssen einzelstaatliche Rechtsvorschriften einen angemessenen Schutz für die Betroffenen vorsehen. Diese Schutzlücke auf EU-Ebene ist bei der Einschätzung des Vorschlags zu berücksichtigen ([2]): Da nicht sämtliche Verarbeitungsvorgänge im Strafverfolgungsbereich erfasst werden können, muss der Gesetzgeber einen umso wirksameren Schutz in den im Vorschlag tatsächlich abgedeckten Bereichen gewährleisten.

([1]) Der EDPS verweist auf die gleichlautende Argumentation des Gerichtshofs (unter anderem) in seinem Urteil in der Rechtssache Österreichischer Rundfunk und andere (Verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, Slg. 2003, I-4989).

([2]) Siehe in diesem Sinne 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, und zur Änderung der Richtlinie 2002/58/EG, Nummer 33.

III.2 **Rechtsgrundlage**

34. In den Erwägungsgründen des Vorschlags für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit ist eine spezifische Rechtsgrundlage angeführt, nämlich Artikel 30 Absatz 1 Buchstabe b. In dem vorliegenden Vorschlag ist dagegen nicht genau angegeben, welche Bestimmungen nach Artikel 30 oder Artikel 31 die Rechtsgrundlage bilden.

35. Obwohl es nicht Aufgabe des EDPS ist, als Berater bei der Gesetzgebung der Europäischen Union die Rechtsgrundlage eines Vorschlags zu wählen, wäre es sinnvoll davon auszugehen, dass auch für diesen Vorschlag Artikel 30 Absatz 1 Buchstabe b als Rechtsgrundlage herangezogen werden könnte. Zusätzlich könnte er auch auf Artikel 31 Absatz 1 Buchstabe c EUV gestützt werden und sollte auch uneingeschränkt für innerstaatliche Situationen Anwendung finden, falls dies zur Verbesserung der polizeilichen und justiziellen Zusammenarbeit zwischen den Mitgliedstaaten erforderlich ist. In diesem Zusammenhang betont der EDPS nochmals, dass alle zu Strafverfolgungszwecken erhobenen, gespeicherten, verarbeiteten oder analysierten personenbezogenen Daten insbesondere nach dem Grundsatz der Verfügbarkeit mit den zuständigen Behörden anderer Mitgliedstaaten ausgetauscht werden können.

36. Der EDPS teilt die Ansicht, dass Artikel 30 Absatz 1 Buchstabe b und Artikel 31 Absatz 1 Buchstabe c EUV eine Rechtsgrundlage für Bestimmungen über den Datenschutz bieten, die nicht auf den Schutz von personenbezogenen Daten beschränkt sind, welche tatsächlich zwischen den zuständigen Behörden der Mitgliedstaaten ausgetauscht werden, sondern auch auf innerstaatliche Situationen anwendbar sind. Insbesondere ist Folgendes zu bemerken:

— Artikel 30 Absatz 1 Buchstabe b, der als Rechtsgrundlage für Bestimmungen über das Einholen, Speichern, Verarbeiten, Analysieren und Austauschen wichtiger Informationen dienen kann, beschränkt sich nicht auf Informationen, die anderen Mitgliedstaaten zur Verfügung gestellt oder übermittelt wurden. Die einzige, von Artikel 30 Absatz 1 Buchstabe b auferlegte Einschränkung besteht in der Sachdienlichkeit der Informationen für die polizeiliche Zusammenarbeit.

— Was die justizielle Zusammenarbeit betrifft, so ist Artikel 31 Absatz 1 Buchstabe c noch expliziter, da ein gemeinsames Vorgehen „die Gewährleistung der Vereinbarkeit der jeweils geltenden Vorschriften der Mitgliedstaaten untereinander, soweit dies zur Verbesserung der Zusammenarbeit erforderlich ist“ einschließt.

— Aus der Rechtssache Pupino ([3]) ergibt sich, dass der Gerichtshof gemeinschaftsrechtliche Grundsätze auf Fragen der dritten Säule anwendet. Diese Rechtsprechung veranschaulicht die Entwicklung von einer reinen Zusammenarbeit zwischen den Behörden der Mitgliedstaaten im Rahmen der dritten Säule zu einem mit dem durch den EG-Vertrag geschaffenen Binnenmarkt vergleichbaren Raum der Freiheit, der Sicherheit und des Rechts.

([3]) Urteil des Gerichtshofs vom 16. Juni 2005 in der Rechtssache C-105/03, Pupino.

— Nach Ansicht des EDPS führt der Grundsatz der Effektivität dazu, dass der Vertrag nicht derart ausgelegt wird, dass die Organe der EU an der effektiven Durchführung ihrer Aufgaben gehindert werden. Dies schließt ihre Aufgabe ein, die Grundrechte zu schützen.

— Wie bereits erwähnt, würde durch eine Beschränkung auf grenzüberschreitende Sachverhalte den Auswirkungen des Grundsatzes der Verfügbarkeit nicht Rechnung getragen und die Rechtssicherheit des Einzelnen würde beeinträchtiget.

37. Der EDPS macht eigens auf den *Austausch von Daten mit Drittländern* aufmerksam. Die Mitgliedstaaten nutzen in Drittstaaten eingeholte und verarbeitete Daten, die ihnen zum Zwecke der Strafverfolgung übermittelt werden, und sie übermitteln von ihnen selbst erhobene und/oder verarbeitete personenbezogene Daten an zuständige Behörden in Drittländern und an internationale Einrichtungen.

38. Nach den Artikeln 30 und 31 EUV sind von Drittstaatsbehörden erhobene personenbezogene Daten nicht anders zu behandeln als ursprünglich von den zuständigen Behörden in den Mitgliedstaaten erhobene Daten. Aus Drittstaaten stammende Daten müssen denselben Standards wie in den Mitgliedstaaten erhobene Daten entsprechen. Die Datenqualität lässt sich jedoch nicht immer ohne Weiteres sichern (auf diesen Aspekt wird im nächsten Abschnitt dieser Stellungnahme eingegangen).

39. Die Übermittlung personenbezogener Daten von zuständigen Behörden der Mitgliedstaaten an Drittstaaten fällt genau genommen nicht in den Anwendungsbereich des Titels VI des EU-Vertrags. Falls jedoch Daten an Drittstaaten übermittelt werden könnten, ohne dass der Schutz der betroffenen Person gewährleistet wäre, würde dies dem in diesem Vorschlag für das EU-Gebiet vorgesehenen Schutz aus den in Abschnitt III.4 dieser Stellungnahme genannten Gründen sehr abträglich sein. Kurzum:

— Die durch diesen Vorschlag gesicherten Rechte der Betroffenen würden unmittelbar beeinträchtigt, wenn die Übermittlung an Drittstaaten keinen Datenschutzvorschriften unterworfen würden.

— Es bestünde die Gefahr, dass die zuständigen Behörden der Mitgliedstaaten die strengen Datenschutznormen umgehen.

40. Zusammenfassend lässt sich sagen, dass zum Schutz personenbezogener Daten, die von den zuständigen Behörden der Mitgliedstaaten mit Behörden von Drittstaaten und internationalen Organisationen ausgetauscht werden, gemeinsame Regeln anwendbar sein müssen, damit die gemeinsamen Regeln zum Schutz personenbezogener Daten zwischen den zuständigen Behörden der Mitgliedstaaten wirksam sein können; sie sind somit zur Verbesserung der Zusammenarbeit zwischen den Mitgliedstaaten nötig. Artikel 30 und 31 EUV bieten hier die erforderliche Rechtsgrundlage.

### III.3 **Spezifische Bemerkungen zum Anwendungsbereich des Vorschlags**

*Von Justizbehörden verarbeitete personenbezogene Daten*

41. Ausgetauscht und verarbeitet werden personenbezogene Daten von Polizeibehörden und auch von Justizbehörden. Der auf die Artikel 30 und 31 EUV gestützte Vorschlag gilt für die Zusammenarbeit zwischen Polizeibehörden und für die Zusammenarbeit zwischen Justizbehörden. Zum gegenwärtigen Zeitpunkt hat der Vorschlag einen weiter gefassten Anwendungsbereich als der Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen, der sich auf die polizeiliche Zusammenarbeit beschränkt und nur für den Informationsaustausch vor Beginn einer Strafverfolgungsmaßnahme gilt.

42. Der EDPS begrüßt die Tatsache, dass sich der Vorschlag auch auf von Justizbehörden verarbeitete personenbezogene Daten erstreckt. Es gibt triftige Gründe dafür, polizeiliche Daten und Daten von Justizbehörden, die zum Zwecke der Strafverfolgung verarbeitet werden, in ein und demselben Vorschlag zu behandeln. Zunächst einmal ist die strafrechtliche Ermittlungs- und Strafverfolgungskette in den Mitgliedstaaten unterschiedlich organisiert. Die Justizbehörden werden in den einzelnen Mitgliedstaaten in verschiedenen Phasen eingeschaltet. Zum anderen können alle personenbezogenen Daten in dieser Kette letztendlich in eine Gerichtsakte einfließen. Es wäre unlogisch, wenn für den Datenschutz in den vorgeschalteten Stufen unterschiedliche Regelungen gelten würden.

43. Für die Aufsicht der Datenverarbeitung ist indes ein anderer Ansatz erforderlich. In Artikel 30 des Vorschlags sind die Aufgaben der Aufsichtsbehörden aufgelistet. Nach Artikel 30 Absatz 9 schränken die Befugnisse der Aufsichtsbehörden die Unabhängigkeit der Justiz nicht ein. Der EDPS empfiehlt, in dem Vorschlag klarzustellen, dass die Aufsichtsbehörden die Datenverarbeitung durch Justizbehörden nicht kontrollieren, soweit diese im Rahmen ihrer justiziellen Befugnisse handeln ([1]).

*Verarbeitung durch Europol und Eurojust (und das Zollinformationssystem)*

44. Nach Artikel 3 Absatz 2 des Vorschlags gilt der Rahmenbeschluss nicht für die Verarbeitung personenbezogener Daten durch Europol, Eurojust und das Zollinformationssystem ([2]).

([1]) Die Bestimmung könnte jener in Artikel 46 der Verordnung 45/2001/EG entsprechen.

([2]) Das Zollinformationssystem ist ein kleines, aber ziemlich komplexes System bestehend aus nationalen und supranationalen Elementen, das dem Schengener Informationssystem vergleichbar ist. Da der Vorschlag für das Zollinformationssystem eher von begrenzter Bedeutung ist, wird es auch in Anbetracht der Komplexität des Systems selbst in dieser Stellungnahme außer Acht gelassen. Der EDPS wird sich in einem anderen Kontext mit dem Zollinformationssystem befassen.

45. Diese Bestimmung ist streng genommen überflüssig, jedenfalls soweit sie sich auf Europol und Eurojust bezieht. Ein Rahmenbeschluss nach Artikel 34 Buchstabe b EUV kann nur zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten angenommen werden und nicht an Europol und Eurojust gerichtet sein.

46. Inhaltlich veranlasst der Wortlaut des Artikels 3 Absatz 2 zu folgenden Bemerkungen:

— Der Vorschlag sieht einen allgemeinen Rahmen vor, der grundsätzlich für alle Sachverhalte im Rahmen der dritten Säule gelten sollte. Ein kohärenter Rechtsrahmen für den Datenschutz trägt schon an sich dazu bei, dass die Wirksamkeit des Datenschutzes erhöht wird.

— Europol und Eurojust verfügen derzeit über präzise definierte Datenschutzsysteme, die auch ein Aufsichtssystem umfassen. Daher ist es nicht dringend erforderlich, die anwendbaren Regeln an den Wortlaut dieses Vorschlags anzupassen.

— Langfristig sollten die für Europol und Eurojust geltenden Datenschutzbestimmungen allerdings uneingeschränkt mit dem Rahmenbeschluss in Einklang gebracht werden.

— Dies ist umso wichtiger, als der Vorschlag für einen Rahmenbeschluss — mit Ausnahme seines Kapitels III — für die Erhebung und Verarbeitung personenbezogener Daten gilt, die von den Mitgliedstaaten an Europol und Eurojust übermittelt werden.

### III.4 **Aufbau des Vorschlags**

47. Der EDPS hat den Vorschlag analysiert und zieht den Schluss, dass er allgemein einen auf mehreren Ebenen umfassenden Schutz bietet. Die in Kapitel II (und für spezifische Aspekte in den Kapiteln IV-VII) des Vorschlags festgelegten gemeinsamen Standards umfassen einen Schutz auf zwei Ebenen:

— Umsetzung der allgemeinen Datenschutzgrundsätze nach der Richtlinie 95/46/EG und anderer Rechtsinstrumente der Europäischen Gemeinschaften sowie des Übereinkommens des Europarates Nr. 108 im Rahmen der dritten Säule;

— zusätzliche, für alle Verarbeitungen personenbezogener Daten im Rahmen der dritten Säule geltende Datenschutzvorschriften. Beispiele hierfür sind in Artikel 4 Absätze 3 und 4 des Vorschlags zu finden.

48. In Kapitel III wird eine dritte Schutzebene für bestimmte Verarbeitungsformen hinzugefügt. Die Überschriften der beiden Abschnitte des Kapitels III und der Wortlaut einiger Bestimmungen des Vorschlags scheinen zu implizieren, dass dieses Kapitel nur für Daten gilt, die von zuständigen Behörden anderer Mitgliedstaaten übermittelt oder zur Verfügung gestellt werden. Dies würde darauf hinauslaufen, dass einige für den Schutz personenbezogener Daten wichtige Bestimmungen nicht für personenbezogene Daten gelten, wenn diese nicht zwischen Mitgliedstaaten ausgetauscht werden. Der Wortlaut ist somit zweideutig, da die Bestimmungen selbst über unmittelbar mit dem Austausch von Daten zusammenhängende Tätigkeiten hinauszugehen scheinen. Diese Einschränkung des Anwendungsbereichs wird jedenfalls weder in der Begründung noch in der Folgenabschätzung ausdrücklich erläutert oder begründet.

49. Der EDPS unterstreicht den zusätzlichen Nutzen einer solchen auf mehreren Ebenen umfassenden Struktur, die den Betroffenen unter Berücksichtigung der spezifischen Erfordernisse der Strafverfolgung an sich optimalen Schutz bieten kann. Dies trägt der Notwendigkeit eines angemessenen Datenschutzes Rechnung, wie auf der Frühjahrskonferenz im April 2005 in Krakau zum Ausdruck gebracht, und steht grundsätzlich in Übereinstimmung mit Artikel 8 der EU-Grundrechtscharta und der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten, insbesondere Artikel 8.

50. Eine Analyse des Wortlauts des Vorschlags veranlasst indes zu den nachstehenden Bemerkungen.

51. Erstens: Es sollte dafür gesorgt werden, dass die zusätzlichen Datenschutzbestimmungen in Kapitel II (die unter Nummer 47 erwähnte zweite Ebene) nicht von den allgemeinen Datenschutzgrundsätzen abweichen. Nach Auffassung des EDPS sollten die ergänzenden Vorschriften in Kapitel II den betroffenen Personen zusätzlichen Schutz im Zusammenhang mit dem spezifischen Kontext der dritten Säule (polizeiliche und justizielle Erkenntnisse) bieten. Mit anderen Worten: diese ergänzenden Vorschriften dürfen kein niedrigeres Schutzniveau nach sich ziehen.

52. Außerdem sollte Kapitel III über besondere Formen der Verarbeitung (in dessen Rahmen die dritte Schutzebene vorgesehen ist) nicht von Kapitel II abweichen. Nach Auffassung des EDPS müssen die Bestimmungen des Kapitels III den betroffenen Personen in Fällen, in denen zuständige Behörden von mehr als einem Mitgliedstaat beteiligt sind, zusätzlichen Schutz bieten, wobei diese Bestimmungen jedoch kein niedrigeres Schutzniveau nach sich ziehen dürfen.

53. Zweitens: Bestimmungen allgemeiner Art sollten nicht in Kapitel III stehen. Der EDPS empfiehlt, diese in Kapitel II aufzunehmen. In Kapitel III dürfen lediglich die Bestimmungen aufgenommen werden, die sich unmittelbar auf den Schutz personenbezogener Daten beim Datenaustausch zwischen Mitgliedstaaten beziehen. Dies ist umso wichtiger, als Kapitel III wichtige Bestimmungen hinsichtlich eines hohen Schutzniveaus für die Betroffenen im Kontext der Strafverfolgung enthält (siehe Abschnitt IV.1 dieser Stellungnahme).

## IV. **ANALYSE DER EINZELNEN BESTANDTEILE DES VORSCHLAGS**

### IV.1 **Ausgangspunkte der Analyse**

54. Der EDPS wird bei seiner Analyse der verschiedenen wesentlichen Bestandteile des Vorschlags dessen besonderer Struktur und dessen besonderem Inhalt Rechnung tragen. Er wird sich dabei nicht zu jedem Artikel einzeln äußern.

55. Zunächst einmal gehen die meisten Bestimmungen des Vorschlags auf bestehende Rechtsakte der EU über den Schutz personenbezogener Daten zurück. Sie stehen mit dem Rechtsrahmen der EU im Bereich des Datenschutzes in Einklang und sind ausreichend, angemessene Datenschutzgarantien in der dritten Säule bereitzustellen.

56. Der EDPS stellt allerdings fest, dass einige der Bestimmungen zurzeit im Kapitel III des Vorschlags enthalten — die spezifische Aspekte der Verarbeitung betreffen und die generell (siehe Nummer 48 dieser Stellungnahme) nur für den Datenaustausch mit anderen Mitgliedstaaten gelten — allgemeine und wesentliche Grundsätze des EU-Datenschutzrechts beinhalten. Diese Bestimmungen sollten daher aus Kapitel III in Kapitel II übernommen werden und für jede Verarbeitung von Daten durch Strafverfolgungsbehörden gelten. Dies trifft für die Bestimmungen betreffend die Überprüfung der Datenqualität (Artikel 9 Absätze 1 und 6) und die Bestimmungen zur Regelung der Weiterverarbeitung personenbezogener Daten (Artikel 11 Absatz 1) zu.

57. In einigen der übrigen Artikel des Kapitels III des Vorschlags wird nicht unterschieden zwischen zusätzlichen Voraussetzungen, die speziell den Datenaustausch mit anderen Mitgliedstaaten betreffen — wie die Zustimmung der zuständigen Behörde des übermittelnden Mitgliedstaates — und Garantien, die dagegen auch für innerhalb eines Mitgliedstaates verarbeitete Daten relevant und notwendig sind. Diesbezüglich empfiehlt der EDPS, dass die zuletzt genannten Garantien generell gelten sollten, also auch für die personenbezogenen Daten, die nicht von einem anderen Mitgliedstaat übermittelt oder zur Verfügung gestellt werden. Diese Empfehlung betrifft

— die Übermittlung von Daten an nicht-öffentliche Stellen und andere Behörden als Strafverfolgungsbehörden (Artikel 13 Buchstaben a und b, Artikel 14 Buchstaben a und b) und

— die Übertragung an Drittländer oder internationale Gremien (Artikel 15, ausgenommen Buchstabe c).

58. In diesem Teil der Stellungnahme wird die Aufmerksamkeit des Gesetzgebers zudem auf einige zusätzliche Garantien gelenkt, die im aktuellen Vorschlag nicht enthalten sind. Nach Auffassung des EDPS sollten diese zusätzlichen Garantien im Hinblick auf automatisierte Einzelentscheidungen, von Drittstaaten erhaltene personenbezogene Daten, den Zugang zu Datenbanken nicht-öffentlicher Stellen sowie die Verarbeitung biometrischer Daten und von DNA-Profilen vorgesehen werden.

59. Darüber hinaus enthält die nachstehende Analyse Empfehlungen zur Verbesserung des aktuellen Wortlauts, damit die Wirksamkeit der Bestimmungen, die Kohärenz des Textes und die Übereinstimmung mit dem derzeit für den Datenschutz geltenden Rechtsrahmen gewährleistet wird.

### IV.2 **Zweckbindung und Weiterverarbeitung**

60. Nach Artikel 4 Absatz 1 Buchstabe b müssen Daten für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. In der Regel werden Daten im Zusammenhang mit einer bestimmten Straftat (oder unter bestimmten Umständen für Ermittlungen in Bezug auf eine kriminelle Vereinigung oder ein kriminelles Netzwerk usw.) gesammelt. Sie können für diesen ursprünglichen Zweck verwendet werden und könnten anschließend für einen anderen Zweck verarbeitet werden, sofern dieser mit dem ursprünglichen Zweck vereinbar ist (Daten, die zu einer wegen Drogenhandels verurteilten Person gesammelt wurden, könnten beispielsweise für Ermittlungen in Bezug auf ein Drogenhändlernetz genutzt werden). Dieser Ansatz spiegelt den auch in Artikel 8 der Menschrechtscharta der Europäischen Union verankerten Grundsatz der Zweckbindung angemessen wider und steht somit in Einklang mit den geltenden Datenschutzvorschriften.

*Weiterverarbeitung für Zwecke im Rahmen des Anwendungsbereichs des Rahmenbeschlusses*

61. Der EDPS stellt fest, dass eine Situation, die im Rahmen der Polizeiarbeit auftreten kann, in dem Vorschlag nicht völlig zufrieden stellend behandelt wird: die Notwendigkeit, Daten für einen Zweck weiterzuverwenden, der mit dem Zweck, für den sie gesammelt wurden, unvereinbar ist. Es könnte sein, dass von der Polizei gesammelte Daten zur Aufklärung einer ganz anderen Straftat benötigt werden. Zur Veranschaulichung dessen lässt sich der Fall anführen, dass Daten zur Ahndung von Zuwiderhandlungen im Straßenverkehr gesammelt und dann zur Auffindung und Verfolgung einer Person, die einen Kfz-Diebstahl begangen hat, genutzt werden. Bei dem zweiten Verwendungszweck, so legitim er auch sein mag, kann nicht davon ausgegangen werden, dass er mit dem Zweck, zu dem die Daten gesammelt wurden, vollkommen in Einklang steht. Falls es den Strafverfolgungsbehörden nicht gestattet wäre, die Daten für diesen zweiten Zweck zu nutzen, könnten sie dazu neigen, Daten zu allgemeinen oder nicht näher präzisierten Zwecken zu erheben, wodurch der Grundsatz der Zweckbindung für die Erhebung belanglos würde. Außerdem würde auch die Anwendung anderer Grundsätze wie jener der Verhältnismäßigkeit, der Richtigkeit und der Zuverlässigkeit behindert (siehe Artikel 4 Absatz 1 Buchstaben c und d).

62. Nach dem EU-Datenschutzrecht müssen personenbezogene Daten für festgelegte eindeutige Zwecke erhoben werden und dürfen sie nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Der EDPS vertritt jedoch die Ansicht, dass hinsichtlich der Weiterverwendung eine gewisse Flexibilität möglich sein muss. Die Einschränkung in Bezug auf die Erhebung wird wahrscheinlich dann umfassend eingehalten, wenn die für die innere Sicherheit zuständigen Behörden wissen, dass sie — sofern angemessene Garantien vorgesehen werden — auf eine Ausnahmeregelung zu der Einschränkung hinsichtlich der Weiterverarbeitung zählen können.

63. Es ist zu präzisieren, dass diese Notwendigkeit der Weiterverarbeitung in Artikel 11 des Vorschlags anerkannt wird, allerdings in recht unzureichender Weise. Artikel 11 gilt nur für Daten, die von der zuständigen Behörde eines anderen Mitgliedstaates übermittelt oder zur Verfügung gestellt wurden und sieht keine ausreichenden Garantien vor.

64. Der EDPS empfiehlt, Artikel 11 Absatz 1 auf alle Daten anzuwenden, ungeachtet dessen, ob sie von einem anderen Mitgliedstaat übermittelt wurden. Außerdem sollten die Bestimmungen des Artikels 11 Absatz 1 Buchstabe b um strengere Garantien ergänzt werden: Die Weiterverwendung von Daten für einen Zweck, der als mit dem ursprünglichen Zweck unvereinbar gilt, sollte nur zulässig sein, wenn dies in einem konkreten Fall zur Verhütung, Ermittlung, Untersuchung und Verfolgung von Straftaten oder zum Schutz der Interessen oder Grundrechte einer Person unerlässlich ist. Faktisch schlägt der EDPS vor, diese Bestimmung in einen neuen Artikel 4a (und in jedem Fall in Kapitel II des Vorschlags) einfließen zu lassen.

65. Artikel 11 Absatz 2 und Artikel 11 Absatz 3 bleiben unverändert anwendbar; sie sehen zusätzliche Garantien für von anderen Mitgliedstaaten übermittelte Daten vor. Der EDPS weist darauf hin, dass Artikel 11 Absatz 3 für den Datenaustausch über das SIS II gelten wird: Der EDPS hat in seiner Stellungnahme zum SIS II bereits darauf hingewiesen, dass dafür zu sorgen ist, dass SIS-Daten nicht für andere Zwecke als die Zwecke des Systems selbst genutzt werden können.

*Weiterverarbeitung für Zwecke außerhalb des Anwendungsbereichs der polizeilichen und justiziellen Zusammenarbeit*

66. In einigen Fällen müssen die Daten zur Sicherung anderer wichtiger Interessen verarbeitet werden. Sie könnten in diesen Fällen sogar von anderen als den nach diesem Rahmenbeschluss zuständigen Behörden verarbeitet werden. Diese Zuständigkeiten der Mitgliedstaaten könnten sich auf eine in die Persönlichkeitsrechte eingreifende Verarbeitung erstrecken (beispielsweise die Sicherheitsüberprüfung einer nicht verdächtigen Person) und sollten daher an sehr strikte Auflagen gebunden sein, etwa die Verpflichtung, dass die Mitgliedstaaten besondere Rechtsvorschriften erlassen müssen, wenn sie diese Ausnahmeregelung in Anspruch nehmen wollen. Im Rahmen der ersten Säule wurde dies in Artikel 13 der Richtlinie 95/46/EG geregelt, der besagt, dass in bestimmten Fällen Einschränkungen in Bezug auf bestimmte Vorschriften der Richtlinie zulässig sind. Mitgliedstaaten, die derartige Einschränkungen anwenden, müssen dies im Einklang mit Artikel 8 EMRK tun.

67. Derselben Argumentation folgend sollte in Kapitel II dieses Rahmenbeschlusses festgelegt werden, dass die Mitgliedstaaten Rechtvorschriften erlassen können, wonach eine Weiterverarbeitung zulässig ist, wenn dies notwendig ist zur Gewährleistung:

— der Abwehr von Bedrohungen der öffentlichen Sicherheit, der Landesverteidigung oder der Sicherheit des Staates;

— des Schutzes wichtiger wirtschaftlicher oder finanzieller Interessen eines Mitgliedstaates oder der Europäischen Union;

— des Schutzes der betroffenen Person.

### IV.3 **Kriterien für eine rechtmäßige Datenverarbeitung**

68. Nach Artikel 5 des Vorschlags dürfen personenbezogene Daten von den zuständigen Behörden nur verarbeitet werden, wenn es eine entsprechende Rechtsvorschrift gibt, in der festgelegt ist, dass diese Verarbeitung zur Erfüllung der rechtmäßigen Aufgaben der betreffenden Behörden sowie zur Verhütung, Ermittlung, Untersuchung und Verfolgung von Straftaten notwendig ist. Der EDPS befürwortet die strengen Anforderungen des Artikels 5.

69. Der Text des Artikels 5 unterschätzt jedoch, dass unter bestimmten Umständen eine Rechtmäßigkeit der Datenverarbeitung auch aus anderen rechtlichen Gründen gegeben sein muss. Bei diesem Artikel handelt es sich um eine wichtige Bestimmung, die es beispielsweise der Polizei nicht unmöglich machen darf, ihrer sich aus dem einzelstaatlichen Recht ergebenden gesetzlichen Verpflichtung zur Weitergabe von Informationen an die Einwanderungs- oder Steuerbehörden nachzukommen. Der EDPS schlägt daher vor, dass in Artikel 5 andere stichhaltige rechtliche Gründe für die Verarbeitung personenbezogener Daten berücksichtigt werden sollten, etwa dass ein für die Verarbeitung Verantwortlicher eine ihm obliegende gesetzliche Verpflichtung erfüllen muss, die ausdrückliche Zustimmung des Betroffenen, vorausgesetzt die Verarbeitung erfolgt im Interesse des Betroffenen, oder die Notwendigkeit, die grundlegenden Interessen des Betroffenen zu schützen.

70. Der EDPS weist darauf hin, dass die Einhaltung der Kriterien betreffend die Rechtmäßigkeit der Datenverarbeitung für die polizeiliche und justizielle Zusammenarbeit besonders wichtig ist, da eine rechtlich unzulässige Erhebung personenbezogener Daten durch Polizeikräfte dazu führen kann, dass diese Daten vor Gericht nicht als Beweismaterial verwendet werden können.

### IV.4 **Notwendigkeit und Verhältnismäßigkeit**

71. Mit den Artikeln 4 und 5 des Vorschlags soll auch — in allgemein zufrieden stellender Weise — gewährleistet werden, dass die Einschränkungen beim Schutz personenbezogener Daten notwendig und verhältnismäßig sind, wie dies gemäß dem Recht der Europäischen Union und nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu Artikel 8 EMRK vorgeschrieben ist:

— In Artikel 4 Absatz 1 Buchstabe c ist die allgemeine Regel festgelegt, dass die Daten den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen.

— In Artikel 5 wird präzisiert, dass die Verarbeitung zur Erfüllung der rechtmäßigen Aufgaben der betreffenden Behörden sowie zur Verhütung, Untersuchung, Ermittlung oder Verfolgung von Straftaten *notwendig* ist.

— In Artikel 4 Absatz 4 ist vorgesehen, dass eine Verarbeitung personenbezogener Daten nur notwendig ist, falls bestimmte besondere Bedingungen erfüllt sind.

72. Der EDPS stellt fest, dass die für Artikel 4 Absatz 4 vorgeschlagene Formulierung den in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte betreffend Artikel 8 EMRK festgelegten Kriterien nicht gerecht wird, wonach ein Eingriff in die Persönlichkeitsrechte nur statthaft ist, wenn dies in einer demokratischen Gesellschaft notwendig ist. Gemäß dem Vorschlag wird eine Verarbeitung personenbezogener Daten nicht nur dann als notwendig erachtet, wenn sie den Strafverfolgungs- und Justizbehörden die Erfüllung ihrer Aufgaben *ermöglichen* würde, sondern auch dann, wenn *berechtigter Grund zu der Annahme* besteht, dass die betreffenden personenbezogenen Daten die Verhütung, Ermittlung, Untersuchung und Verfolgung einer Straftat lediglich *erleichtern oder beschleunigen* würden.

73. Diese Kriterien stehen nicht mit den Anforderungen des Artikels 8 EMRK in Einklang, da nahezu jede Verarbeitung personenbezogener Daten als Erleichterung der Tätigkeiten von Polizei- und Justizbehörden betrachtet werden könnte, auch wenn die betreffenden Daten nicht wirklich zu deren Erledigung benötigt werden.

74. Mit Artikel 4 Absatz 4 in seinem jetzigen Wortlaut würde der Weg geebnet für eine unannehmbar umfassende Erhebung personenbezogener Daten, die sich lediglich auf die Annahme stützt, dass personenbezogene Daten die Verhütung, Untersuchung, Ermittlung und Verfolgung einer Straftat *erleichtern können*. Die Verarbeitung personenbezogener Daten darf aber im Gegenteil nur dann als notwendig erachtet werden, wenn die zuständigen Behörden eindeutig nachweisen können, dass sie notwendig ist, und sofern keine weniger stark in die Persönlichkeitsrechte eingreifenden Maßnahmen zur Verfügung stehen.

75. Der EDPS empfiehlt daher, Artikel 4 Absatz 4 erster Gedankenstrich so umzuformulieren, dass die Rechtsprechung zu Artikel 8 EMRK beachtet wird. Aus systematischen Gründen schlägt der EDPS ferner vor, Artikel 4 Absatz 4 an das Ende des Artikels 5 zu stellen.

### IV.5 **Verarbeitung besonderer Datenkategorien**

76. In Artikel 6 ist ein grundsätzliches Verarbeitungsverbot für besonders schützenswerte Daten festgelegt, d. h. personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben. Dieses Verbot findet keine Anwendung, wenn die Verarbeitung gesetzlich vorgeschrieben und für die Erfüllung der rechtmäßigen Aufgabe der betreffenden Behörde im Hinblick auf die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten unbedingt erforderlich ist. Besonders sensitive Daten können auch dann verarbeitet werden, wenn die betroffene Person ausdrücklich ihre Einwilligung dazu erteilt hat. In beiden Fällen müssen geeignete spezifische Garantien vorgesehen werden.

77. Der Wortlaut des Artikels 6 veranlasst zu zwei Bemerkungen. Zum einen stützt sich Artikel 6 in zu starkem Maße auf die Zustimmung des Betroffenen. Der EDPS unterstreicht, dass die Verarbeitung besonders schützenswerter Daten auf der Grundlage der ausdrücklichen Zustimmung des Betroffenen nur insoweit zulässig sein sollte, als die Verarbeitung im Interesse des Betroffenen erfolgt und die Verweigerung der Zustimmung keine nachteiligen Auswirkungen für den Betroffenen nach sich zieht. Der EDPS empfiehlt, Artikel 6 entsprechend zu ändern, und zwar auch, um ihn mit dem geltenden EU-Datenschutzrecht in Einklang zu bringen.

78. Zum anderen könnten nach Auffassung des EDPS hinsichtlich der Verarbeitung auch andere rechtliche Gründe Berücksichtigung finden, etwa die Notwendigkeit, die grundlegenden Interessen des Betroffenen oder einer anderen Person (wenn die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben) zu schützen.

79. Im Bereich der polizeilichen und justiziellen Zusammenarbeit kommt der Verarbeitung anderer Kategorien von möglicherweise besonders sensitiven personenbezogenen Daten, wie biometrische Daten und DNA-Profile, zunehmende Bedeutung zu. Diese Daten werden von Artikel 6 des Vorschlags nicht ausdrücklich erfasst. Der EDPS ersucht den EU-Gesetzgeber um besondere Aufmerksamkeit bei der Umsetzung der in diesem Vorschlag vorgesehenen allgemeinen Datenschutzgrundsätze in weitere Rechtsvorschriften, die die Verarbeitung dieser besonderen Datenkategorien nach sich ziehen. Als Beispiel wäre hier der Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit (siehe Nummern 12-15) zu nennen, der die Verarbeitung und den Austausch von biometrischen Daten und DNA-Profilen ausdrücklich zulässt (siehe Anhang II des Vorschlags), jedoch nicht die besondere Schutzwürdigkeit und die Besonderheiten dieser Daten aus datenschutzrechtlicher Sicht behandelt.

80. Der EDPS empfiehlt, spezifische Garantien vorzusehen, mit denen insbesondere gewährleistet werden soll, dass:

— biometrische Daten und DNA-Profile nur auf der Grundlage präzise definierter und kompatibler technischer Normen genutzt werden dürfen;

— deren sachliche Richtigkeit gebührend berücksichtigt wird und diese von dem Betroffenen anhand leicht zugänglicher Mittel angefochten werden kann, und

— die Wahrung der Würde der Person in jeder Hinsicht gewährleistet ist.

Die Entscheidung darüber, ob diese zusätzlichen Garantien in diesem Rahmenbeschluss oder in den spezifischen Rechtsakten zur Regelung der Erhebung und des Austauschs dieser besonderen Datenkategorien vorgesehen werden, bleibt dem Gesetzgeber überlassen.

### IV.6 **Richtigkeit und Zuverlässigkeit**

81. In Artikel 4 Absatz 1 Buchstabe d sind die allgemeinen Regeln betreffend die Datenqualität festgelegt. Danach hat der für die Verarbeitung Verantwortliche dafür zu sorgen, dass die Daten sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind. Er hat alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden. Dies entspricht den allgemeinen Grundsätzen der EU-Datenschutzvorschriften.

82. Nach Artikel 4 Absatz 1 Buchstabe d Satz 3 können die Mitgliedstaaten vorsehen, dass Daten mit unterschiedlicher sachlicher Richtigkeit und Zuverlässigkeit verarbeitet werden dürfen. Der EDPS fasst diese Bestimmung als Ausnahmeregelung zu dem allgemeinen Grundsatz der Richtigkeit auf und empfiehlt, den Ausnahmecharakter dieser Bestimmung dadurch zu präzisieren, dass „jedoch" oder „nichtsdestoweniger" in Artikel 4 Absatz 1 Buchstabe d Satz 3 am Satzanfang hinzugefügt wird. In diesen Fällen, in denen die Richtigkeit der Daten nicht umfassend gewährleistet werden kann, ist der für die Verarbeitung Verantwortliche gehalten, die Daten nach sachlicher Richtigkeit und Zuverlässigkeit zu unterscheiden und sich dabei insbesondere auf den grundlegenden Unterschied zwischen faktischen Daten und sich auf Meinungen oder persönlichen Ansichten gründenden Daten zu beziehen. Der EDPS unterstreicht, dass diese Verpflichtung sowohl hinsichtlich der betroffenen Personen als auch hinsichtlich der Strafverfolgungsbehörden sehr wichtig ist, insbesondere wenn die Daten weitab von ihrer Quelle verarbeitet werden (siehe Nummer 7 dieser Stellungnahme).

*Überprüfung der Datenqualität*

83. Ergänzt wird der in Artikel 4 Absatz 1 Buchstabe d festgelegte allgemeine Grundsatz durch die spezifischeren Garantien in Artikel 9 betreffend die Überprüfung der Datenqualität. Artikel 9 besagt insbesondere Folgendes:

1. Die Qualität personenbezogener Daten wird spätestens vor ihrer Übermittlung oder Bereitstellung überprüft. Darüber hinaus wird die Qualität von Daten, die im Wege eines automatischen direkten Zugriffs verfügbar gemacht werden, regelmäßig überprüft (Artikel 9 Absätze 1 und 2).

2. Bei allen Datenübermittlungen ist nach Möglichkeit auf ergangene Gerichtsentscheidungen und erfolgte Verfahrenseinstellungen hinzuweisen; in Bezug auf Daten, die sich auf Stellungnahmen gründen, ist vor der Übermittlung eine Überprüfung an der Quelle durchzuführen und die sachliche Richtigkeit und Zuverlässigkeit der Daten anzugeben (Artikel 9 Absatz 1).

3. Personenbezogene Daten werden auf Antrag der betroffenen Person gekennzeichnet, falls ihre sachliche Richtigkeit von der betroffenen Person in Abrede gestellt wird und nicht ermittelt werden kann (Artikel 9 Absatz 6).

84. Artikel 4 Absatz 1 und Artikel 9 gewährleisten somit bei gemeinsamer Anwendung eine angemessene Überprüfung der Qualität der personenbezogenen Daten sowohl durch den Betroffenen als auch durch diejenigen Behörden, die den Quellen der verarbeiteten Daten am nächsten und daher am ehesten zu ihrer Überprüfung in der Lage sind.

85. Der EDPS begrüßt diese Bestimmungen, da sie — obwohl sie sich auf die Erfordernisse der Strafverfolgungsbehörden konzentrieren — gewährleisten, dass die einzelnen Daten gebührend berücksichtigt und entsprechend ihrer Richtigkeit und Zuverlässigkeit verwendet werden, wodurch verhindert wird, dass sich für einen Betroffenen in unverhältnismäßigem Maße negative Folgen ergeben, weil einige der ihn betreffenden Daten möglicherweise nicht richtig sind.

86. Für die Betroffenen ist die Überprüfung der Datenqualität ein wesentliches Element des Schutzes, insbesondere was die von den Polizei- und Justizbehörden verarbeiteten personenbezogenen Daten anbelangt. Daher bedauert der EDPS, dass Artikel 9 betreffend die Überprüfung der Datenqualität nur für Daten gilt, die anderen Mitgliedstaaten übermittelt oder zur Verfügung gestellt werden. Dies ist bedauerlich, da es darauf hinausläuft, dass die Qualität personenbezogener Daten, die ja auch für Strafverfolgungszwecke von grundlegender Bedeutung ist, nur dann in vollem Umfang gewährleistet wäre, wenn diese Daten anderen Mitgliedstaaten übermittelt oder zur Verfügung gestellt werden, nicht jedoch, wenn sie innerhalb eines Mitgliedstaates verarbeitet werden [1]. Vielmehr ist — sowohl im Interesse der Betroffenen als auch der zuständigen Behörden — unbedingt dafür zu sorgen, dass in die sachgemäße Überprüfung der Qualität sämtliche personenbezogenen Daten einbezogen werden, einschließlich jener, die nicht von anderen Mitgliedstaaten übermittelt oder zur Verfügung gestellt werden.

87. Der EDPS empfiehlt daher, auf jeden Fall die Einschränkungen des Anwendungsbereichs des Artikels 9 Absätze 1 und 6 dadurch aufzuheben, dass diese Bestimmungen in Kapitel II des Vorschlags übernommen werden.

*Unterscheidung zwischen verschiedenen Kategorien von Daten*

88. Nach Artikel 4 Absatz 3 hat der für die Verarbeitung Verantwortliche für eine klare Unterscheidung zwischen den personenbezogenen Daten verschiedener Kategorien von Personen (Verdächtige, Verurteilte, Zeugen, Opfer, Informanten, Kontaktpersonen, Sonstige) zu sorgen. Der EDPS begrüßt diesen Ansatz. Sicherlich müssen Strafverfolgungs- und Justizbehörden gegebenenfalls Daten zu sehr unterschiedlichen Kategorien von Personen verarbeiten, jedoch ist dabei von grundlegender Bedeutung, dass diese Daten entsprechend dem jeweiligen Grad der Beteiligung an der Straftat unterschieden werden. Die Bedingungen für die Erhebung von Daten, die Fristen, die Bedingungen, unter denen Betroffenen der Zugang oder Auskunft verweigert werden kann, und die Modalitäten für den Zugang zu Daten durch die zuständigen Behörden sollten vor allem jedoch die Besonderheiten der verschiedenen Kategorien verarbeiteter Daten und die verschiedenen Zwecke, zu denen diese Daten von den Strafverfolgungs- und Justizbehörden erhoben werden, widerspiegeln.

89. Der EDPS bittet in diesem Zusammenhang darum dass den Daten betreffend Nichtverdächtige besondere Aufmerksamkeit gewidmet wird. Es bedarf besonderer Bedingungen und Garantien, um Verhältnismäßigkeit zu gewährleisten und zu verhindern, dass Personen, die nicht aktiv an einer Tat beteiligt waren, Nachteile erwachsen. Der Vorschlag sollte für diese Personenkategorie zusätzliche Bestimmungen zur Einschränkung des Verarbeitungszwecks, zur Festlegung präziser Fristen und zur Begrenzung des Zugangs zu den Daten enthalten. Der EDPS empfiehlt, den Vorschlag entsprechend zu ändern.

[1] Dies stünde auch nicht mit der Empfehlung Nr. R (87) 15 des Ministerkomitees des Europarates an die Mitgliedstaaten über die Nutzung personenbezogener Daten im Polizeibereich in Einklang. Insbesondere ist in Grundsatz 7.2 vorgesehen, dass im Benehmen mit der Kontrollbehörde oder gemäß dem innerstaatlichen Recht „regelmäßige Kontrollen" der Qualität personenbezogener Daten vorgesehen werden sollten.

90. Der Vorschlag enthält in seiner aktuellen Fassung eine spezifische Garantie für Nichtverdächtige in Artikel 7 Absatz 1. Hierbei handelt es sich nach Auffassung des EDPS um eine wichtige Garantie, vor allem, da die Mitgliedstaaten keine Ausnahmeregelungen vorsehen dürfen. Bedauerlicherweise beziehen sich die in Artikel 7 Absatz 1 festgelegten spezifischen Garantien ausschließlich auf die Fristen; zudem gilt diese Bestimmung nur für die in Artikel 4 Absatz 3 letzter Gedankenstrich des Vorschlags aufgeführte Personenkategorie. Die vorgesehenen Garantien sind daher unzureichend und es ist nicht die gesamte Gruppe der Nichtverdächtigen erfasst ([1]).

91. Auch Daten über verurteilte Personen verdienen besondere Aufmerksamkeit. Hinsichtlich dieser Daten sollte den jüngsten und künftigen Initiativen zum Austausch von Strafregisterauszügen gebührend Rechnung getragen und für Kohärenz gesorgt werden ([2]).

92. In Anbetracht der vorstehenden Ausführungen empfiehlt der EDPS, Artikel 4 um einen neuen Absatz zu ergänzen, der folgende Elemente enthält:

— ergänzende Bestimmungen zur Einschränkung des Verarbeitungszwecks, zur Festlegung präziser Fristen und zur Beschränkung des Zugangs zu den Daten, soweit Nichtverdächtige betroffen sind;

— die Verpflichtung für die Mitgliedstaaten, die Rechtsfolgen der vorzunehmenden Unterscheidung zwischen personenbezogenen Daten verschiedener Personenkategorien festzulegen; diese sollen die Besonderheiten der verschiedenen Kategorien verarbeiteter Daten und die unterschiedlichen Zwecke, zu denen diese Daten von den Strafverfolgungs- und Justizbehörden erhoben werden, widerspiegeln;

— die Rechtsfolgen sollten sich auf die Bedingungen für die Erhebung personenbezogener Daten, die Fristen, die Weiterleitung und Verwendung der Daten und die Bedingungen der Zugangs- oder Auskunftsverweigerung gegenüber dem Betroffenen beziehen.

### IV.7 **Fristen für die Speicherung personenbezogener Daten**

93. Die allgemeinen Grundsätze zur Regelung der Fristen für die Speicherung personenbezogener Daten sind in Artikel 4 Absatz 1 Buchstabe e und Artikel 7 Absatz 1 des Vorschlags enthalten. Ein allgemeiner Grundsatz lautet, dass personenbezogene Daten nicht länger gespeichert werden dürfen, als es für die Erfüllung des Zwecks, zu dem sie gesammelt wurden, nötig ist. Dies entspricht den Datenschutzvorschriften der EU ([3]).

94. Die allgemeine Bestimmung in Artikel 7 Absatz 1 gilt jedoch nur, „sofern nicht durch innerstaatliche Rechtsvorschriften anderes bestimmt ist". Der EDPS ist der Auffassung, dass diese Ausnahme sehr allgemein ist und über die nach Artikel 4 Absatz 1 Buchstabe e zulässigen Ausnahmen hinausgeht. Der EDPS schlägt vor, dass die allgemeine Ausnahme nach Artikel 7 Absatz 1 gestrichen wird oder zumindest die öffentlichen Interessen, die die Anwendung dieser Ausnahme durch die Mitgliedstaaten rechtfertigen, ausdrücklich eingegrenzt werden ([4]).

95. In Artikel 7 Absatz 2 heißt es, dass verfahrensrechtliche und technische Maßnahmen vorgesehen werden, um sicherzustellen, dass die Fristen für die Speicherung personenbezogener Daten eingehalten werden, und dass die Fristen regelmäßig überprüft werden. Der EDPS begrüßt diese Bestimmung, empfiehlt jedoch, ausdrücklich zu erwähnen, dass mit den geeigneten verfahrensrechtlichen und technischen Maßnahmen nach einem bestimmten Zeitraum für eine automatische und regelmäßige Löschung personenbezogener Daten gesorgt wird.

### IV.8 **Austausch personenbezogener Daten mit Drittländern**

96. Eine wirksame polizeiliche und justizielle Zusammenarbeit innerhalb der Grenzen der EU hängt verstärkt von einer Zusammenarbeit mit Drittländern und internationalen Einrichtungen ab. Zahlreiche Maßnahmen, mit denen die Zusammenarbeit der Strafverfolgungs- und Justizbehörden mit Drittländern oder internationalen Einrichtungen verbessert werden soll, werden gegenwärtig auf nationaler Ebene und auf EU-Ebene erörtert oder in Aussicht genommen ([5]). Die Gestaltung dieser internationalen Zusammenarbeit wird voraussichtlich in hohem Maße den Austausch personenbezogener Daten beinhalten.

97. Es ist daher unerlässlich, dass die Grundsätze einer Verarbeitung nach Treu und Glauben und auf rechtmäßige Weise — sowie im Allgemeinen die Grundsätze eines fairen Verfahrens — auch für die Erhebung und den Austausch personenbezogener Daten über die Grenzen der Union hinweg gelten und dass personenbezogene Daten nur dann an Drittländer oder internationale Einrichtungen übermittelt werden, wenn von den betreffenden dritten Parteien ein angemessener Schutz oder angemessene Garantien gewährleistet werden.

---

([1]) Siehe insbesondere Nummer 94 dieser Stellungnahme.

([2]) Der Beschluss 2005/876/JI des Rates über den Austausch von Informationen aus dem Strafregister ist am 9. Dezember in Kraft getreten. Er ergänzt und erleichtert die derzeitigen, auf bestehende Übereinkommen gestützten Verfahren zur Übermittlung von Informationen über Verurteilungen; dazu zählen das Europäische Übereinkommen über die Rechtshilfe in Strafsachen von 1959 und das Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union von 2000. Dieser Text wird zu einem späteren Zeitpunkt durch einen präziseren Rahmenbeschluss des Rates ersetzt. Die Kommission beabsichtigt, einen neuen Rahmenbeschluss in diesem Bereich vorzuschlagen.

([3]) Neben der allgemeinen Bestimmung über Fristen für die Speicherung personenbezogener Daten in Artikel 7 enthält der Vorschlag weitere spezifische Bestimmungen zu personenbezogenen Daten, die mit anderen Mitgliedstaaten ausgetauscht werden. So legt Artikel 9 Absatz 7 insbesondere fest, dass personenbezogene Daten gelöscht werden,

1. falls die Daten nicht hätten übermittelt, zur Verfügung gestellt oder entgegengenommen werden dürfen,
2. falls eine nach dem innerstaatlichen Recht des anderen Mitgliedstaats vorgesehene diesbezügliche Frist abgelaufen ist und die Behörde, die die betreffenden Daten übermittelt oder zur Verfügung gestellt hat, die empfangende Behörde bei der Übermittlung oder Bereitstellung über diese Frist in Kenntnis gesetzt hat, und die personenbezogenen Daten nicht mehr für Gerichtsverfahren benötigt werden,
3. falls die Daten nicht mehr für den Zweck, zu dem sie übermittelt oder zur Verfügung gestellt wurden, benötigt werden.

([4]) In Betracht käme eine Beschränkung auf die Terrorismusbekämpfung und/oder die spezifischen öffentlichen Interessen, die in Artikel 4 Absatz 1 Buchstabe e genannt werden: historische, statistische oder wissenschaftliche Zwecke.

([5]) Siehe beispielsweise die jüngste Mitteilung der Kommission mit dem Titel „Eine Strategie für die Außendimension des Raums der Freiheit, der Sicherheit und des Rechts" (KOM(2005) 491 endg.).

*Übertragung personenbezogener Daten an Drittländer*

98. Der EDPS begrüßt in diesem Zusammenhang Artikel 15 des Vorschlags, in dem ein Schutz im Falle einer Übertragung an zuständige Behörden von Drittländern oder internationale Einrichtungen vorgesehen ist. Diese Bestimmung, die in Kapitel III des Vorschlags enthalten ist, gilt jedoch nur für Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übersandt oder zur Verfügung gestellt wurden. Infolge dieser Einschränkung bleibt im System des Datenschutzes auf der Ebene der Europäischen Union eine Lücke in Bezug auf Daten bestehen, die nicht von der zuständigen Behörde eines anderen Mitgliedstaats übersandt wurden. Der EDPS ist der Auffassung, dass diese Lücke aus den folgenden Gründen nicht akzeptiert werden kann.

99. Zum einen sollte das durch EU-Recht gebotene Schutzniveau bei einer Übertragung an Drittländer nicht von der Quelle der Daten abhängen, also von der Frage, ob die Quelle eine Polizeibehörde in dem Mitgliedstaat ist, der die Daten an ein Drittland weiterleitet, oder eine Polizeibehörde in einem anderen Mitgliedstaat.

100. Zum anderen sei darauf hingewiesen, dass die Regeln für die Übertragung personenbezogener Daten an Drittländer einen wesentlichen Grundsatz des Datenschutzrechts widerspiegeln. Dieser Grundsatz stellt nicht nur eine der grundlegenden Bestimmungen der Richtlinie 95/46/EG dar, sondern ist auch im Zusatzprotokoll zum Übereinkommen Nr. 108 verankert ([1]). Einheitliche Bestimmungen für den Schutz personenbezogener Daten, auf die in Artikel 1 des Vorschlags Bezug genommen wird, könnten nicht gewährleistet werden, wenn einheitliche Regeln für die Übertragung personenbezogener Daten an Drittländer nicht alle Verarbeitungsoperationen erfassen. Die Rechte betroffener Personen, wie sie mit dem vorliegenden Vorschlag gewährleistet werden, würden daher unmittelbar beeinträchtigt, wenn personenbezogene Daten an Drittländer, die kein angemessenes Schutzniveau bieten, übermittelt werden könnten.

101. Drittens könnte eine Einschränkung des Anwendungsbereichs dieser Regelungen auf „ausgetauschte Daten" dazu führen, dass es bei Daten, die lediglich innerhalb eines Landes verarbeitet werden, keine Garantien gäbe: Paradoxerweise könnten personenbezogene Daten in diesem Falle unabhängig von einem angemessenen Schutz der Daten leichter an Drittländer übermittelt werden als an andere Mitgliedstaaten. Dies würde Möglichkeiten der „Informationswäsche" eröffnen. Zuständige Behörden von Mitgliedstaaten könnten die strengen Datenschutzbestimmungen umgehen, indem sie Daten an Drittländer oder internationale Einrichtungen übermitteln, wo eine zuständige Behörde eines anderen Mitgliedstaats Zugang zu ihnen hätte oder von wo aus sie sogar an eine solche Behörde weitergeleitet werden könnten.

102. Der EDPS empfiehlt daher, den vorliegenden Vorschlag dahin gehend zu ändern, dass Artikel 15 für den Austausch *aller* personenbezogener Daten mit Drittländern gilt. Diese Empfehlung bezieht sich nicht auf Artikel 15 Absatz 1 Buchstabe c, der dem Wesen nach nur bei personenbezogenen Daten, die mit anderen Mitgliedstaaten ausgetauscht werden, relevant sein kann.

*Übertragung im Ausnahmefall an Länder, in denen ein angemessener Datenschutz nicht gewährleistet ist*

103. Artikel 15 enthält eine Reihe von Bedingungen für die Übertragung von Daten an zuständige Behörden in Drittländern oder an internationale Einrichtungen; diese Bedingungen sind mit denen in Artikel 25 der Richtlinie 95/46/EG vergleichbar. Nach Artikel 15 Absatz 6 können jedoch Daten an Drittländer oder internationale Einrichtungen übermittelt werden, in denen ein angemessener Datenschutz nicht gewährleistet ist, wenn dies zum Schutz der grundlegenden Interessen eines Mitgliedstaats oder zur Abwehr einer drohenden ernsthaften Gefahr für die öffentliche Sicherheit oder für eine oder mehrere Personen unbedingt notwendig ist.

104. Die Anwendbarkeit der in Absatz 6 vorgesehenen Ausnahme sollte geklärt werden. Der EDPS empfiehlt daher Folgendes:

— Es sollte deutlich gemacht werden, dass diese Ausnahme lediglich eine Abweichung von der Bedingung des „angemessenen Schutzes" erlaubt, sich jedoch nicht auf die übrigen Bedingungen auswirkt, die in Artikel 15 Absatz 1 aufgeführt sind.

— Es sollte hinzugefügt werden, dass die Übertragung von Daten im Rahmen dieser Ausnahme von angemessenen Bedingungen abhängig gemacht (beispielsweise der expliziten Bedingung, dass die Daten nur vorübergehend und zu bestimmten Zwecken verarbeitet werden) und der zuständigen Kontrollstelle mitgeteilt werden sollten.

*Verarbeitung personenbezogener Daten, die von einem Drittland übermittelt werden*

105. Im Zusammenhang mit dem zunehmenden Austausch personenbezogener Daten mit Polizei- und Justizbehörden von Drittländern sollte ferner besonders auf personenbezogene Daten geachtet werden, die aus denjenigen Drittländern „importiert" werden, in denen eine angemessene Achtung der Menschenrechte — und insbesondere ein angemessener Schutz personenbezogener Daten — nicht gewährleistet sind.

([1]) Das Zusatzprotokoll zum Europäischen Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr wurde am 8.11.2001 unterzeichnet und ist am 1.7.2004 in Kraft getreten. Dieses verbindliche internationale Rechtsinstrument ist bislang von elf Staaten unterzeichnet worden (neun dieser Staaten sind Mitgliedstaaten der EU). Artikel 2 Absatz 1 des Protokolls enthält folgenden allgemeinen Grundsatz: „Jede Vertragspartei sieht vor, dass personenbezogene Daten an einen Empfänger, der der Hoheitsgewalt eines Staates oder einer Organisation untersteht, der beziehungsweise die nicht Vertragspartei des Übereinkommens ist, nur dann weitergegeben werden dürfen, wenn dieser Staat oder diese Organisation ein angemessenes Schutzniveau für die beabsichtigte Datenweitergabe gewährleistet."

106. Aus allgemeinerer Sicht vertritt der EDPS die Auffassung, dass der Gesetzgeber dafür sorgen sollte, dass personenbezogene Daten, die von Drittländern übermittelt werden, zumindest internationalen Standards für die Achtung der Menschenrechte entsprechen. Beispielsweise sollten Daten, die durch Folter oder Menschenrechtsverletzungen erlangt wurden, und schwarze Listen, die lediglich auf politischen Überzeugungen oder sexuellen Vorlieben basieren, nicht verarbeitet und von Strafverfolgungs- oder Justizbehörden berücksichtigt werden, es sei denn, dies erfolgt im Interesse des Betroffenen. Der EDPS empfiehlt, dass dies zumindest in einem Erwägungsgrund des Vorschlags, eventuell durch Bezugnahme auf einschlägige internationale Instrumente, deutlich gemacht wird ([1]).

107. Was speziell den Schutz personenbezogener Daten angeht, so weist der EDPS darauf hin, dass in dem Fall, personenbezogene Daten von Ländern übermittelt werden, in denen es keine angemessenen Standards und Garantien für den Schutz personenbezogener Daten gibt, gebührend geprüft werden muss, ob etwaige Unzulänglichkeiten bei der Datenqualität bestehen, damit vermieden wird, dass sich Strafverfolgungsbehörden der EU irrtümlich auf solche Informationen verlassen und für die Betroffenen Nachteile entstehen.

108. Der EDPS empfiehlt daher, in Artikel 9 des Vorschlags eine Bestimmung aufzunehmen, wonach die Qualität personenbezogener Daten, die von Drittländern übermittelt werden, sofort bei Erhalt der Daten besonders zu prüfen ist und dass der Grad der Richtigkeit und Zuverlässigkeit der Daten anzugeben ist.

### IV.9 **Austausch personenbezogener Daten mit nicht-öffentlichen Stellen und Behörden, die keine Strafverfolgungsbehörden sind**

109. Die Artikel 13 und 14 des Vorschlags enthalten eine Reihe von Anforderungen, die zu erfüllen sind, wenn personenbezogene Daten an nicht-öffentliche Stellen und Behörden, die keine Strafverfolgungsbehörden sind, übermittelt werden. Wie bereits erwähnt, ergänzen diese Artikel die allgemeinen Bestimmungen in Kapitel II, die auf jeden Fall eingehalten werden müssen.

110. Der EDPS ist der Auffassung, dass eine Übermittlung an nicht-öffentliche Stellen und andere Behörden in besonderen Fällen für die Verhütung und Bekämpfung von Straftaten zwar erforderlich sein kann, dass aber besondere und strenge Bedingungen gelten sollten. Dies entspricht dem Standpunkt, den die europäischen Datenschutzbeauftragten im Krakauer Positionspapier geäußert haben ([2]).

111. Der EDPS ist vor diesem Hintergrund der Auffassung, dass die zusätzlichen Bedingungen in den Artikeln 13 und 14 als zufrieden stellend betrachtet werden könnten, wenn sie zusammen mit den allgemeinen Bestimmungen in Kapitel II angewandt werden und die Regelungen für eine Weiterverarbeitung umfassend zum Tragen kommen (siehe oben, Abschnitt IV.2). Im gegenwärtigen Vorschlag wird jedoch die Anwendung der Artikel 13 und 14 auf personenbezogene Daten beschränkt, die von den zuständigen Behörden eines anderen Mitgliedstaats übersandt oder zur Verfügung gestellt wurden.

112. Die generelle Anwendung der letztgenannten Bedingungen ist sogar noch wichtiger, wenn man den zunehmenden Datenaustausch zwischen Strafverfolgungsbehörden und anderen Behörden oder nicht-öffentlichen Stellen auch innerhalb eines Mitgliedstaats bedenkt. Als Beispiel lässt sich die öffentlich-private Partnerschaft im Strafverfolgungsbereich anführen ([3]).

113. Der EDPS empfiehlt daher, den vorliegenden Vorschlag dahin gehend zu ändern, dass die Artikel 13 und 14 für den Austausch *aller* personenbezogener Daten gelten, und zwar auch für Daten, die nicht von einem anderen Mitgliedstaat übersandt oder zur Verfügung gestellt wurden. Diese Empfehlung bezieht sich nicht auf Artikel 13 Buchstabe c und Artikel 14 Buchstabe c.

*Zugang zu personenbezogenen Daten, die von nicht-öffentlichen Stellen verwaltet werden, und Weiterverwendung solcher Daten*

114. Der Austausch personenbezogener Daten mit nicht-öffentlichen Stellen erfolgt in beide Richtungen: Personenbezogene Daten werden auch von nicht-öffentlichen Stellen an Strafverfolgungs- und Justizbehörden übermittelt oder ihnen zur Verfügung gestellt.

115. In diesem Falle werden personenbezogene Daten, die für Geschäftszwecke erhoben wurden (Geschäftsvorgänge, Marketing, Erbringung von Dienstleistungen usw.) und von nicht-öffentlichen Verarbeitungsverantwortlichen verwaltet werden, von öffentlichen Stellen für den ganz anderen Zweck der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten eingesehen und weiterverwendet. Die Richtigkeit und Zuverlässigkeit von Daten, die zu Geschäftszwecken verarbeitet wurden, ist zudem sorgfältig zu prüfen, wenn diese Daten für Strafverfolgungszwecke verwendet werden ([4]).

([1]) VN-Übereinkommen gegen Folter und andere grausame, unmenschliche oder erniedrigende Behandlung oder Strafe, das von allen Mitgliedstaaten der EU unterzeichnet wurde und am 26. Juni 1987 in Kraft getreten ist. Insbesondere in Artikel 15 ist Folgendes festgelegt: „Jeder Vertragsstaat trägt dafür Sorge, dass Aussagen, die nachweislich durch Folter herbeigeführt worden sind, nicht als Beweis in einem Verfahren verwendet werden, es sei denn gegen eine der Folter angeklagte Person als Beweis dafür, dass die Aussage gemacht wurde."

([2]) Positionspapier über Strafverfolgung und Informationsaustausch in der EU, angenommen auf der Frühjahrskonferenz der europäischen Datenschutzbehörden vom 25./26. April 2005 in Krakau.

([3]) Siehe das Legislativ- und Arbeitsprogramm der Kommission für 2006, KOM(2005) 531 endg.

([4]) Beispielsweise ist eine Telefonrechnung für Geschäftszwecke zuverlässig, solange sie korrekt angibt, welche Telefongespräche geführt wurden; Strafverfolgungsbehörden können sich jedoch nicht uneingeschränkt auf die gleiche Telefonrechnung als schlüssigen Beweis dafür stützen, wer ein bestimmtes Telefongespräch geführt hat.

116. Ein jüngeres und sehr wichtiges Beispiel für den Zugang zu nicht-öffentlichen Datenbanken für Strafverfolgungszwecke ist der gebilligte Text der Richtlinie über die Vorratsspeicherung von Kommunikationsdaten (siehe oben, Nummern 16 bis 18), nach der Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreiber eines öffentlichen Kommunikationsnetzes bestimmte Kommunikationsdaten bis zu zwei Jahre lang aufbewahren müssen, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung stehen. Dem gebilligten Text zufolge gehen Fragen betreffend den Zugang zu diesen Daten über das Gemeinschaftsrecht hinaus und können nicht von der Richtlinie selbst geregelt werden. Diese wichtigen Fragen können stattdessen durch einzelstaatliche Rechtsvorschriften oder Maßnahmen nach Titel VI EUV geregelt werden ([1]).

117. In seiner Stellungnahme zum Vorschlag für diese Richtlinie ist der EDPS für eine weiter gefasste Auslegung des EG-Vertrags eingetreten, da eine Einschränkung des Zugangs erforderlich ist, um einen angemessenen Schutz des Betroffenen, dessen Kommunikationsdaten auf Vorrat gespeichert werden müssen, zu gewährleisten. Der europäische Gesetzgeber hat leider keine Zugangsregelungen in die genannte Richtlinie aufgenommen.

118. In der vorliegenden Stellungnahme bringt der EDPS erneut zum Ausdruck, dass er nachdrücklich dafür eintritt, dass das EU-Recht einheitliche Standards für den Zugang und die Weiterverwendung durch Strafverfolgungsbehörden enthalten sollte. Solange dies nicht im Rahmen der ersten Säule geregelt ist, könnte ein Rechtsinstrument der dritten Säule für den erforderlichen Schutz sorgen. Dieser Standpunkt des EDPS wird durch den allgemeinen Anstieg des Datenaustausches zwischen den Mitgliedstaaten und den unlängst vorgelegten Vorschlag zum Grundsatz der Verfügbarkeit noch bestätigt. Unterschiedliche einzelstaatliche Vorschriften über den Zugang und die Weiterverwendung wären mit der geplanten EU-weiten „Freizügigkeit" von Strafverfolgungsinformationen, zu denen auch Daten aus nicht-öffentlichen Datenbanken gehören, nicht vereinbar.

119. Der EDPS ist daher der Auffassung, dass für den Zugang der Strafverfolgungsbehörden zu personenbezogenen Daten, die von nicht-öffentlichen Stellen verwaltet werden, einheitliche Standards gelten sollten, damit sichergestellt wird, dass der Zugang nur auf der Grundlage klar umrissener Bedingungen und Einschränkungen zulässig ist. Insbesondere sollte der Zugang der zuständigen Behörden nur auf Einzelfallbasis unter ganz bestimmten Umständen für bestimmte Zwecke zulässig sein und in den Mitgliedstaaten der gerichtlichen Kontrolle unterliegen.

([1]) In den Erwägungsgründen der Richtlinie heißt es wie folgt: „Fragen des Zugangs zu Daten, die gemäß dieser Richtlinie auf Vorrat gespeichert werden, seitens einzelstaatlicher Stellen im Zusammenhang mit Tätigkeiten gemäß Artikel 3 Absatz 2 erster Gedankenstrich der Richtlinie 95/46/EG, fallen nicht in den Anwendungsbereich des Gemeinschaftsrechts. Hierzu können jedoch einzelstaatliche Rechtsvorschriften oder Maßnahmen nach Titel VI des Vertrags über die Europäische Union erlassen werden, wobei zu beachten ist, dass solche Rechtsvorschriften oder Maßnahmen die Grundrechte, die sich aus den gemeinsamen verfassungsrechtlichen Traditionen der Mitgliedstaaten ergeben und die in der Europäischen Menschenrechtskonvention garantiert sind, uneingeschränkt wahren müssen. Nach Artikel 8 der Europäischen Menschenrechtskonvention in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte …"

### IV.10 **Rechte der betroffenen Person**

120. Kapitel IV befasst sich mit den Rechten der betroffenen Person in einer Weise, die im Allgemeinen mit den gegenwärtigen Datenschutzvorschriften und mit Artikel 8 der EU-Grundrechtecharta im Einklang steht.

121. Der EDPS begrüßt diese Bestimmungen, da sie betroffenen Personen ein harmonisiertes Spektrum von Rechten bieten und zugleich den Besonderheiten der Verarbeitung durch Strafverfolgungs- und Justizbehörden Rechnung tragen. Dies ist eine erhebliche Verbesserung, da die gegenwärtige Lage von einer großen Vielfalt an Regelungen und Praktiken insbesondere betreffend das Auskunftsrecht gekennzeichnet ist. Einige Mitgliedstaaten lassen nicht zu, dass die betroffene Person Auskunft über ihre Daten erhält, haben jedoch ein System der „indirekten Auskunft" (die über die nationale Datenschutzbehörde im Namen der betroffenen Person erfolgt).

122. Mit dem Vorschlag werden die möglichen Ausnahmen vom direkten Auskunftsrecht harmonisiert. Dies ist umso wichtiger, damit der Bürger, dessen Daten von zuständigen Behörden verschiedener Mitgliedstaaten der EU in zunehmendem Maße verarbeitet und ausgetauscht werden, als betroffene Person unabhängig davon, in welchem Mitgliedstaat die Daten erhoben oder verarbeitet werden, ein harmonisiertes Spektrum von Rechten geltend machen kann ([2]).

123. Der EDPS erkennt die Möglichkeit an, die Rechte der betroffenen Person in den Fällen einzuschränken, in denen dies für die Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten erforderlich ist. Da diese Einschränkungen als Ausnahmen von grundlegenden Rechten der betroffenen Person betrachtet werden müssen, sollte auf alle Fälle eine strenge Prüfung der Verhältnismäßigkeit erfolgen. Dies bedeutet, dass Ausnahmen begrenzt und klar umrissen sein sollten und dass Einschränkungen möglichst nur partiell und zeitlich begrenzt erfolgen sollten.

124. Vor diesem Hintergrund möchte der EDPS den Gesetzgeber insbesondere auf Absatz 2 Buchstabe a der Artikel 19, 20 und 21 aufmerksam machen, der eine sehr weit gefasste und unspezifische Ausnahme von den Rechten der betroffenen Person enthält; dort heißt es nämlich, dass die Rechte eingeschränkt werden können, wenn dies notwendig ist, „um dem für die Verarbeitung Verantwortlichen die ordnungsgemäße Erfüllung seiner Aufgaben zu ermöglichen". Darüber hinaus überschneidet sich diese Ausnahme mit den Bestimmungen von Buchstabe b, der Einschränkungen der Rechte der betroffenen Person

([2]) Kapitel IV befasst sich insbesondere mit dem Informationsrecht (Artikel 19 und 20) und dem Auskunftsrecht, dem Recht auf Berichtigung, Löschung oder Sperrung (Artikel 21). Generell bieten diese Artikel dem Betroffenen sämtliche Rechte, die üblicherweise in den EU-Datenschutzvorschriften vorgesehen sind, und legen zugleich eine Reihe von Ausnahmen fest, mit denen den Besonderheiten der dritten Säule Rechnung getragen werden soll. Insbesondere werden Einschränkungen der Rechte des Betroffenen durch nahezu identische Bestimmungen beim Informationsrecht (Artikel 19 Absatz 2 und Artikel 20 Absatz 2) und beim Auskunftsrecht (Artikel 21 Absatz 2) zugelassen.

zulässt, wenn dies notwendig ist, „um nicht laufende Ermittlungen, Untersuchungen oder Verfahren oder die zuständigen Behörden bei der ordnungsgemäßen Erfüllung ihrer Aufgaben zu behindern". Zwar kann die letztgenannte Ausnahme als gerechtfertigt angesehen werden, aber die erstgenannte legt offensichtlich eine unverhältnismäßige Einschränkung der Rechte der betroffenen Person fest. Der EDPS empfiehlt daher, Absatz 2 Buchstabe a der Artikel 19, 20 und 21 zu streichen.

125. Darüber hinaus empfiehlt der EDPS, die Artikel 19, 20 und 21 wie folgt zu verbessern:

— Es sollte angegeben werden, dass die Einschränkungen der Rechte der betroffenen Person nicht obligatorisch sind, nicht für unbefristete Zeit gelten und „nur" in den spezifischen Fällen zulässig sind, die in den Artikeln aufgeführt sind.

— Es sollte berücksichtigt werden, dass die Informationen von dem für die Verarbeitung Verantwortlichen von sich aus und nicht erst nach einer Anforderung seitens der betroffenen Person zur Verfügung gestellt werden sollten;

— In Artikel 19 Absatz 1 Buchstabe c sollte hinzugefügt werden, dass auch Informationen über die „Fristen für die Speicherung der Daten" erteilt werden sollten.

— Es sollte sichergestellt werden (durch eine Änderung von Artikel 20 Absatz 1 im Einklang mit anderen Datenschutzinstrumenten der EU), dass die betroffene Person in dem Fall, dass die Daten nicht bei der betroffenen Person oder bei der betroffenen. Person ohne deren Kenntnis erhoben wurden, Informationen „spätestens dann erhält, wenn die Daten erstmals weitergegeben werden".

— Es sollte gewährleistet werden, dass der Mechanismus, nach dem gegen die vollständige oder teilweise Einschränkung der Rechte der betroffenen Person Einspruch eingelegt werden kann, bei Einschränkungen des Rechts auf Information Anwendung findet; der letzte Satz von Artikel 19 Absatz 4 sollte entsprechend geändert werden.

*Automatisierte Einzelentscheidungen*

126. Der EDPS bedauert, dass in dem Vorschlag auf die wichtige Frage der automatisierten Einzelentscheidungen überhaupt nicht eingegangen wird. Die praktische Erfahrung zeigt nämlich, dass die Strafverfolgungsbehörden zunehmend auf die automatisierte Verarbeitung von Daten zurückgreifen, um einzelne Aspekte einer Person, insbesondere ihre Zuverlässigkeit und ihr Verhalten, zu bewerten.

127. Dem EDPS ist zwar bewusst, dass diese Systeme in bestimmten Fällen notwendig sein können, um die Effizienz der Strafverfolgung zu erhöhen, weist aber darauf hin, dass Entscheidungen, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten ergehen, sehr strengen Bedingungen und Garantien unterliegen sollten, wenn sie für eine Person rechtliche Folgen nach sich ziehen oder die Person erheblich beeinträchtigen. Dies ist im Rahmen der dritten Säule umso wichtiger, als die zuständigen Behörden hier zu Zwangsmaßnahmen berechtigt sind und ihre Entscheidungen oder Maßnahmen daher eine Person beeinträchtigen oder einen größeren Eingriff darstellen könnten, als dies normalerweise der Fall wäre, wenn solche Entscheidungen/Maßnahmen durch nichtöffentliche Stellen erfolgen.

128. Insbesondere sollten im Einklang mit allgemeinen Datenschutzgrundsätzen derartige Entscheidungen oder Maßnahmen nur dann erlaubt sein, wenn das Gesetz oder die zuständige Kontrollstelle sie ausdrücklich zulässt, und sie sollten geeigneten Maßnahmen unterliegen, mit denen die legitimen Interessen der betroffenen Person gewahrt werden. Darüber hinaus sollten der betroffenen Person ohne Weiteres Mittel zur Verfügung stehen, die es ihr erlauben, ihren Standpunkt darzulegen und die Begründung für die Entscheidung zu erfahren, sofern dies nicht mit dem Zweck unvereinbar ist, zu dem die Daten verarbeitet werden.

129. Der EDPS empfiehlt daher, im Einklang mit den gegenwärtigen EU-Datenschutzvorschriften zum Datenschutz eine spezifische Bestimmung über automatisierte Einzelentscheidungen aufzunehmen.

### IV.11 **Sicherheit der Verarbeitung**

130. Was die Sicherheit der Verarbeitung anbelangt, so enthält Artikel 24 die Verpflichtung, dass der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführt, die mit anderen EU-Rechtsinstrumenten zum Datenschutz im Einklang stehen. Absatz 2 enthält darüber hinaus eine detaillierte und umfassende Liste von Maßnahmen, die im Hinblick auf die automatisierte Datenverarbeitung zu ergreifen sind.

131. Der EDPS begrüßt diese Bestimmung, schlägt jedoch vor, in die Liste der Maßnahmen in Absatz 2 die folgende zusätzliche Maßnahme aufzunehmen, damit eine wirksame Kontrolle durch die Kontrollstellen erleichtert wird: „*k) dafür zu sorgen, dass die Effizienz dieser Sicherheitsmaßnahmen systematisch überwacht und darüber Bericht erstattet wird (systematische Eigenkontrolle der Sicherheitsmaßnahmen)*" ([1]).

*Protokollierung von Daten*

132. Nach Artikel 10 wird jede automatische Übermittlung und jeder automatische Erhalt personenbezogener Daten protokolliert und jede nicht automatische Übermittlung und jeder nicht automatische Erhalt personenbezogener Daten dokumentiert, um die anschließende Überprüfung der Rechtmäßigkeit der Übermittlung und Verarbeitung zu ermöglichen. Die Informationen werden der zuständigen Kontrollstelle auf Anforderung übermittelt.

([1]) Siehe im gleichen Sinne die Stellungnahme des EDPS zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für den kurzfristigen Aufenthalt (KOM(2004) 835 endg.), veröffentlicht auf der Website www.edps.eu.int.

133. Der EDPS begrüßt diese Bestimmung. Er weist jedoch darauf hin, dass für eine umfassende Überwachung und Überprüfung der ordnungsgemäßen Nutzung personenbezogener Daten auch der „Zugang" zu den Daten protokolliert oder dokumentiert werden muss. Diese Informationen sind unerlässlich, da eine effiziente Überwachung der ordnungsgemäßen Verarbeitung personenbezogener Daten nicht nur auf die Rechtmäßigkeit der Übermittlung personenbezogener Daten zwischen Behörden, sondern auch auf die Rechtmäßigkeit des Zugangs dieser Behörden zu den Daten gerichtet sein muss [1]. Der EDPS empfiehlt daher, Artikel 10 so zu ändern, dass auch die Protokollierung oder Dokumentierung des Zugangs zu den Daten vorgeschrieben wird.

### IV.12. **Rechtsbehelfe, Haftung und Sanktionen**

134. Kapitel VI des Vorschlags befasst sich mit Rechtsbehelfen (Artikel 27), Haftung (Artikel 28) und Sanktionen (Artikel 29). Die Bestimmungen stehen im Allgemeinen mit den gegenwärtigen EU-Datenschutzvorschriften im Einklang.

135. Was Sanktionen betrifft, so begrüßt der EDPS insbesondere die Angabe, dass die bei Verstößen gegen die Vorschriften zur Umsetzung dieses Rahmenbeschlusses zu verhängenden Sanktionen wirksam, angemessen und abschreckend sein müssen. Darüber hinaus werden strafrechtliche Sanktionen für vorsätzliche Straftaten, die schwere Verstöße — insbesondere hinsichtlich der Geheimhaltung und der Sicherheit der Verarbeitung — darstellen, eine größere abschreckende Wirkung hinsichtlich schwerwiegenderer Verstöße gegen das Datenschutzrecht haben.

### IV.13. **Kontroll-, Überwachungs- und Beratungsaufgaben**

136. Die Bestimmungen des Vorschlags über die Kontrolle und die Aufsicht der Datenverarbeitung sowie über die Konsultation zu Fragen im Zusammenhang mit der Datenverarbeitung ähneln weitgehend den Bestimmungen der Richtlinie 95/46/EG. Der EDPS begrüßt, dass sich die Kommission in ihrem Vorschlag für bereits erprobte und gut funktionierende Mechanismen entschieden hat, und hebt insbesondere die Einführung eines (obligatorischen) Systems der Vorabkontrolle hervor. Ein solches System ist nicht nur in der Richtlinie 95/46/EG vorgesehen, sondern ist darüber hinaus auch in der Verordnung 45/2001/EG enthalten und hat sich als wirksames Instrument erwiesen, das dem EDPS bei der Überwachung der Datenverarbeitung durch Organe und Einrichtungen der Europäischen Gemeinschaften zur Verfügung steht.

137. Ein anderes Instrument für die Kontrolle und Überwachung der Datenverarbeitung, das sich als effizient erwiesen hat, ist die Ernennung von Datenschutzbeauftragten durch den für die Verarbeitung Verantwortlichen. Dieses Instrument gibt es in mehreren Mitgliedstaaten. Es ist in der Verordnung 45/2001/EG als obligatorisches Instrument vorgeschrieben und spielt auf der Ebene der Europäischen Gemeinschaften eine wichtige Rolle. Datenschutzbeauftragte sind Verwalter innerhalb einer Organisation, die in unabhängiger Art und Weise die interne Anwendung von Datenschutzbestimmungen garantieren.

138. Der EDPS empfiehlt, in den Vorschlag Bestimmungen über Datenschutzbeauftragte aufzunehmen. Diese Bestimmungen könnten gemäß zu den Artikeln 24 bis 26 der Verordnung 45/2001/EG gestaltet werden.

139. Der Vorschlag für einen Rahmenbeschluss ist an die Mitgliedstaaten gerichtet. Es ist daher logisch, dass Artikel 30 des Vorschlags eine Aufsicht durch unabhängige Kontrollstellen vorsieht. Dieser Artikel ist an Artikel 28 der Richtlinie 95/46/EG angelehnt. Diese nationalen Stellen sollten untereinander und mit den nach Titel VI des Vertrags über die Europäische Union eingesetzten gemeinsamen Kontrollinstanzen und mit dem EDPS zusammenarbeiten. Darüber hinaus sieht Artikel 31 des Vorschlags die Einsetzung einer Gruppe vor, die eine ähnliche Rolle wie die Art. 29 Datenschutzgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten in Fragen der ersten Säule zu spielen hat. Alle einschlägigen Akteure im Bereich des Datenschutzes werden in Artikel 31 des Vorschlags genannt.

140. Es versteht sich von selbst, dass in einem Vorschlag, mit dem die polizeiliche und justizielle Zusammenarbeit zwischen den Mitgliedstaaten verbessert werden soll, die Zusammenarbeit zwischen allen einschlägigen Akteuren im Bereich des Datenschutzes eine wichtige Rolle spielt. Der EDPS begrüßt daher, dass in dem Vorschlag die Zusammenarbeit zwischen den Kontrollstellen hervorgehoben wird.

141. Der EDPS betont darüber hinaus, wie wichtig ein stimmiges Vorgehen in Fragen des Datenschutzes ist, das durch die Förderung der Kommunikation zwischen der bestehenden Art. 29 Datenschutzgruppe und der Gruppe, die mit dem vorliegenden Vorschlag für einen Rahmenbeschluss eingesetzt wird, verbessert werden könnte. Der EDPS empfiehlt eine Änderung von Artikel 31 Absatz 2 des Vorschlags, damit auch der Vorsitzende der Art. 29 Datenschutzgruppe berechtigt ist, an Sitzungen der neuen Gruppe teilzunehmen oder in den Sitzungen vertreten zu sein.

142. Der Wortlaut von Artikel 31 des Vorschlags enthält einen bemerkenswerten Unterschied gegenüber Artikel 29 der Richtlinie 95/46/EG. Der EDPS ist Vollmitglied der Art. 29 Datenschutzgruppe. Diese Mitgliedschaft beinhaltet das Stimmrecht. Auch im vorliegenden Vorschlag wird der EDPS als Mitglied der Gruppe benannt (Artikel 31), jedoch ist für ihn kein Stimmrecht vorgesehen. Es ist nicht ersichtlich, aus welchen Gründen der vorliegende Vorschlag von Artikel 29 der Richtlinie 95/46/EG abweicht. Der EDPS ist der Auffassung, dass der vorgeschlagene Text hinsichtlich der Rolle des EDPS unklar ist, was die Wirksamkeit seiner Beteiligung an der Arbeit der Gruppe beeinträchtigen könnte. Der EDPS empfiehlt daher, die Übereinstimmung mit dem Wortlaut der Richtlinie zu wahren.

[1] Dies steht im Einklang mit Artikel 18 des Vorschlags, dem zufolge die Behörde, die die personenbezogenen Daten übersandt oder zur Verfügung gestellt hat, auf deren Antrag über die weitere Verarbeitung oder deren Ergebnisse unterrichtet werden muss, und mit Artikel 24 über Sicherheitsmaßnahmen, und zwar auch im Lichte der vorgeschlagenen systematischen Eigenkontrolle der Maßnahmen.

### IV.14. **Sonstige Bestimmungen**

143. Kapitel VIII des Vorschlags enthält einige Schlussbestimmungen zur Änderung des Schengener Durchführungsübereinkommens und zur Beziehung zu anderen Instrumenten für die Verarbeitung und den Schutz personenbezogener Daten.

*Schengener Durchführungsübereinkommen*

144. Nach Artikel 33 des Vorschlags werden die Artikel 126 bis 130 des Schengener Durchführungsübereinkommens in Bezug auf Angelegenheiten, die in den Anwendungsbereich des EU-Vertrags fallen, durch den Rahmenbeschluss ersetzt. Die Artikel 126 bis 130 des Schengener Durchführungsübereinkommens enthalten die allgemeinen Datenschutzbestimmungen für die Verarbeitung von Daten, die gemäß dem Übereinkommen (aber außerhalb des Schengener Informationssystems) übermittelt werden.

145. Der EDPS begrüßt, dass die Bestimmungen des Schengener Durchführungsabkommen ersetzt werden, da dadurch die Einheitlichkeit der Datenschutzregelung in der dritten Säule verbessert wird und dies in einigen Aspekten, beispielsweise durch die Ausweitung der Befugnisse der Kontrollinstanzen, eine bedeutende Verbesserung des Schutzes personenbezogener Daten darstellt. In manchen Punkten ist das Ergebnis jedoch eine unbeabsichtigte — und bedauerliche — Senkung des Datenschutzniveaus. Einige Bestimmungen des Schengener Durchführungsübereinkommens sind nämlich strenger als die Bestimmungen des Rahmenbeschlusses.

146. Der EDPS weist insbesondere auf Artikel 126 Absatz 3 Buchstabe b des Schengener Durchführungsübereinkommens hin, wonach Daten ausschließlich durch die Behörden und Gerichte genutzt werden dürfen, die für eine Aufgabe im Rahmen der Zwecke des Übereinkommens zuständig sind. Mit dieser Bestimmung wird offensichtlich eine Übermittlung an nicht-öffentliche Stellen ausgeschlossen, während eine solche Übermittlung im Rahmen des vorgeschlagenen Rahmenbeschlusses zulässig wäre. Ein weiterer Punkt ist, dass die Datenschutzbestimmungen im Schengener Durchführungsübereinkommen auch auf *alle* Daten Anwendung finden, die aus einer *nichtautomatisierten Datei* übermittelt oder in eine solche Datei aufgenommen werden (Artikel 127), während nichtautomatisierte Dateien vom Anwendungsbereich des vorgeschlagenen Rahmenbeschlusses ausgenommen sind.

*Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union*

147. Nach Artikel 34 wird Artikel 23 des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union durch den Rahmenbeschluss ersetzt. Der EDPS weist darauf hin, dass dadurch im Allgemeinen ein besserer Schutz personenbezogener Daten, die im Rahmen des Übereinkommens ausgetauscht werden, gewährleistet würde, dass dies jedoch auch einige Probleme hinsichtlich der Kompatibilität der beiden Instrumente aufwerfen könnte.

148. Das Übereinkommen befasst sich nämlich auch mit Rechtshilfe bei der Überwachung des Telekommunikationsverkehrs. Der ersuchte Mitgliedstaat kann in diesem Fall seine Zustimmung — zur Überwachung oder Übermittlung der Aufzeichnung des Telekommunikationsverkehrs — von der Erfüllung jeglicher Bedingungen abhängig machen, die in einem vergleichbaren innerstaatlichen Fall zu erfüllen wären. Nach Artikel 23 Absatz 4 des Übereinkommens haben in den Fällen, in denen die Verwendung personenbezogener Daten an diese zusätzlichen Bedingungen geknüpft ist, diese Bedingungen Vorrang vor den Datenschutzbestimmungen in Artikel 23. Dementsprechend bestimmt Artikel 23 Absatz 5, dass die zusätzlichen Bestimmungen zum Schutz von Informationen, die von gemeinsamen Ermittlungsgruppen erhoben werden, Vorrang haben. Der EDPS weist darauf hin, dass unklar wäre, ob die genannten zusätzlichen Bestimmungen noch Anwendung finden würden, wenn Artikel 23 durch den Rahmenbeschluss ersetzt wird. Er empfiehlt daher, diese Frage zu klären und dabei die Folgen einer vollständigen Ersetzung von Artikel 23 des Übereinkommens durch diesen Rahmenbeschluss gründlich zu prüfen.

*Übereinkommen Nr. 108 des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten*

149. Nach Artikel 34 Absatz 2 sind Bezugnahmen auf das Übereinkommen Nr. 108 als Bezugnahmen auf den Rahmenbeschluss zu verstehen. Die Auslegung und die konkrete Anwendbarkeit dieser Bestimmung sind bei weitem nicht klar. Der EDPS geht jedenfalls davon aus, dass diese Bestimmung nur innerhalb des sachlichen Anwendungsbereichs des Rahmenbeschlusses gilt.

*Sonstige Fragen*

150. Was den systematischen Aufbau des Textes betrifft, so weist der EDPS darauf hin, dass einige Artikel im Text des Vorschlags an einer besser geeigneten Stelle stehen könnten.

Der EDPS schlägt daher Folgendes vor:

1. Artikel 16 („Ausschuss“) sollte von Kapitel III („Formen der Datenverarbeitung“) in ein neues Kapitel übertragen werden.

2. Artikel 25 („Verzeichnis“) und Artikel 26 („Vorabkontrolle“) sollten von Kapitel V („Geheimhaltung und Sicherheit der Verarbeitung“) in ein neues Kapitel übertragen werden.

## V. **SCHLUSSBEMERKUNGEN**

*Ein erheblicher Fortschritt*

a) Die Annahme des Vorschlags wäre ein erheblicher Fortschritt für den Schutz personenbezogener Daten in einem wichtigen Bereich, in dem vor allem ein kohärenter und effizienter Mechanismus für den Schutz personenbezogener Daten auf Ebene der Europäischen Union erforderlich ist.

b) Ein wirksamer Schutz personenbezogener Daten ist nicht nur für die betroffenen Personen wichtig, sondern trägt auch zum Erfolg der polizeilichen und justiziellen Zusammenarbeit an sich bei. In vielen Aspekten greifen beide öffentliche Interessen eng ineinander.

*Einheitliche Standards*

c) Der EDPS ist der Auffassung, dass ein neues Regelwerk für den Datenschutz nicht nur die Grundsätze des Datenschutzes wahren sollte (es ist wichtig, dass die Einheitlichkeit des Datenschutzes innerhalb der Europäischen Union gewährleistet ist), sondern auch zusätzliche Regelungen bietet, die den Besonderheiten des Strafverfolgungsbereichs Rechnung tragen.

d) Mit dem vorliegenden Vorschlag werden diese Voraussetzungen erfüllt: Er gewährleistet, dass die bestehenden Grundsätze des Datenschutzes nach der Richtlinie 95/46/EG auch innerhalb der dritten Säule angewandt werden, da die meisten Bestimmungen des Vorschlags andere EU-Rechtsinstrumente zum Schutz personenbezogener Daten widerspiegeln und mit diesen Rechtsinstrumenten im Einklang stehen. Darüber hinaus bietet er einheitliche Standards für diese Grundsätze im Hinblick auf ihre Anwendung in diesem Bereich, die im Großen und Ganzen ausreichen, um angemessene Garantien für den Datenschutz in der dritten Säule zu gewährleisten.

*Anwendung auf die gesamte Datenverarbeitung*

e) Für die Erreichung der Ziele des Rahmenbeschlusses ist es unerlässlich, dass er alle polizeilichen und justiziellen Daten erfasst, auch wenn sie nicht von zuständigen Behörden anderer Mitgliedstaaten übermittelt oder zur Verfügung gestellt werden.

f) Artikel 30 Absatz 1 Buchstabe b und Artikel 31 Absatz 1 Buchstabe c VEU bieten eine Rechtsgrundlage für Datenschutzbestimmungen, die nicht auf den Schutz personenbezogener Daten beschränkt sind, die zwischen den zuständigen Behörden der Mitgliedstaaten ausgetauscht werden, sondern auch für innerstaatliche Situationen gelten.

g) Der Vorschlag gilt weder für die Datenverarbeitung im Rahmen der zweiten Säule des EU-Vertrags (Gemeinsame Außen- und Sicherheitspolitik) noch für die Datenverarbeitung durch Nachrichtendienste und den Zugang dieser Dienste zu Daten, wenn die Daten von zuständigen Behörden oder anderen Parteien verarbeitet werden (dies folgt aus Artikel 33 EUV). In diesen Bereichen sollen die einzelstaatlichen Rechtsvorschriften für einen angemessenen Schutz der betroffenen Personen sorgen. Diese Lücke im Schutz auf EU-Ebene macht einen umso wirksameren Schutz in den Bereichen erforderlich, die von dem Vorschlag erfasst werden.

h) Der EDPS begrüßt, dass der Vorschlag für personenbezogene Daten gilt, die von Justizbehörden verarbeitet werden.

*Verhältnis zu anderen Rechtsinstrumenten*

i) Wenn andere spezifische Rechtsinstrumente nach Titel VI des EU-Vertrags genauere Bedingungen oder Einschränkungen für die Datenverarbeitung oder den Zugang zu Daten vorsehen, sollte das spezifische Rechtsinstrument als „lex specialis“ Anwendung finden.

j) Der vorliegende Vorschlag für einen Rahmenbeschluss des Rates zum Datenschutz hat seinen eigenen Nutzen und ist selbst dann erforderlich, wenn ein Rechtsakt über die Verfügbarkeit (wie von der Kommission am 12. Oktober 2005 vorgeschlagen) nicht angenommen wird.

k) Der Umstand, dass das Europäische Parlament die Richtlinie über die Vorratsspeicherung von Kommunikationsdaten gebilligt hat, macht es sogar noch dringender, dass ein Rechtsrahmen für den Datenschutz in der dritten Säule festgelegt wird.

*Struktur des Vorschlags*

l) Die zusätzlichen Bestimmungen in Kapitel II (zusätzlich zu den allgemeinen Grundsätzen der Richtlinie 95/46/EG) sollten im spezifischen Rahmen der dritten Säule einen zusätzlichen Schutz für die betroffenen Personen bieten, dürfen jedoch nicht zu einem niedrigeren Schutzniveau führen.

m) Kapitel III über die Formen der Datenverarbeitung (das die dritte Ebene des Schutzes beinhaltet) darf Kapitel II nicht einschränken: Die Bestimmungen von Kapitel III sollten den betroffenen Personen in Fällen, in denen zuständige Behörden von mehr als einem Mitgliedstaat beteiligt sind, einen zusätzlichen Schutz bieten, aber diese Bestimmungen dürfen nicht zu einem niedrigeren Schutzniveau führen.

n) Die Bestimmungen zur Überprüfung der Qualität der Daten (Artikel 9 Absätze 1 und 6) und zur Weiterverarbeitung von personenbezogenen Daten (Artikel 11 Absatz 1) sollten nach Kapitel II übertragen werden und für die gesamte Datenverarbeitung durch Strafverfolgungsbehörden gelten, und zwar auch wenn die personenbezogenen Daten nicht von einem anderen Mitgliedstaat übermittelt oder zur Verfügung gestellt wurden. Insbesondere ist es sowohl im Interesse der betroffenen Personen als auch der zuständigen Behörden wichtig, dafür zu sorgen, dass sich die ordnungsgemäße Überprüfung der Qualität auf alle personenbezogenen Daten erstreckt.

*Zweckbindung*

o) Der Vorschlag geht nicht vollkommen zufrieden stellend auf eine Situation ein, die in der Polizeiarbeit eintreten kann, nämlich das Erfordernis, die Daten zu einem Zweck weiter zu verwenden, der als unvereinbar mit dem Zweck gilt, zu dem sie erhoben wurden.

p) Nach den Datenschutzvorschriften der EU müssen personenbezogene Daten zu spezifischen und ausdrücklich festgelegten Zwecken erhoben werden und dürfen nicht in einer Weise weiterverarbeitet werden, die mit diesen Zwecken unvereinbar ist. Eine gewisse Flexibilität ist für die Weiterverwendung vorzusehen. Es ist wahrscheinlicher, dass die Einschränkung bei der Erhebung korrekt eingehalten wird, wenn die für die innere Sicherheit zuständigen Behörden wissen, dass sie bei entsprechenden Garantien auf eine Ausnahme von der Einschränkung der Weiterverwendung zählen können.

q) In Kapitel II des Rahmenbeschlusses sollte festgelegt werden, dass es den Mitgliedstaaten gestattet ist, Rechtsetzungsmaßnahmen anzunehmen, mit denen eine Weiterverarbeitung erlaubt wird, wenn diese Maßnahme erforderlich ist, um Folgendes zu gewährleisten:

— die Abwehr von Gefahren für die öffentliche Sicherheit, die Landesverteidigung oder die innerstaatliche Sicherheit;

— den Schutz eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats;

— den Schutz der betroffenen Person.

Diese Befugnisse der Mitgliedstaaten könnten eine in die Persönlichkeitsrechte eingreifende Verarbeitung beinhalten und sollten daher an sehr strenge Bedingungen geknüpft sein.

*Notwendigkeit und Verhältnismäßigkeit*

r) Die Grundsätze der Notwendigkeit und der Verhältnismäßigkeit des Vorschlags sollten uneingeschränkt die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte widerspiegeln, indem sichergestellt wird, dass die Verarbeitung personenbezogener Daten nur dann für notwendig erachtet wird, wenn die zuständigen Behörden eine eindeutige Notwendigkeit belegen können und sofern Maßnahmen, die mit einem geringeren Eingriff in die Persönlichkeitsrechte verbunden sind, nicht zur Verfügung stehen.

*Austausch personenbezogener Daten mit Drittländern*

s) Wenn Daten an Drittländer übermittelt werden könnten, ohne dass der Schutz der betroffenen Person gewährleistet ist, würde dies den mit diesem Vorschlag angestrebten Schutz innerhalb der Europäischen Union erheblich beeinträchtigen. Der EDPS empfiehlt, den Vorschlag dahin gehend zu ändern, dass Artikel 15 für den Austausch *aller* personenbezogener Daten mit Drittländern gilt. Diese Empfehlung bezieht sich nicht auf Artikel 15 Absatz 1 Buchstabe c.

t) Wenn personenbezogene Daten von Drittländern übermittelt werden, sollte ihre Qualität vor dem Hintergrund der Achtung der Menschenrechte und der Datenschutznormen sorgfältig geprüft werden, bevor sie verwendet werden.

*Austausch personenbezogener Daten mit nicht-öffentlichen Stellen und Behörden, die keine Strafverfolgungsbehörden sind*

u) Die Übermittlung an nicht-öffentliche Stellen und andere Behörden kann in bestimmten Fällen für die Verhütung und Bekämpfung von Kriminalität erforderlich sein, aber es sollten spezifische und strenge Voraussetzungen gelten. Der EDPS empfiehlt, den vorliegenden Vorschlag dahin gehend zu ändern, dass die Artikel 13 und 14 für den Austausch *aller* personenbezogener Daten gelten, und zwar auch für Daten, die nicht von einem anderen Mitgliedstaat übersandt oder zur Verfügung gestellt wurden. Diese Empfehlung bezieht sich nicht auf Artikel 13 Buchstabe c und Artikel 14 Buchstabe c.

v) Für den Zugang der Strafverfolgungsbehörden zu personenbezogenen Daten von nicht-öffentlichen Stellen sollten einheitliche Standards gelten, um zu gewährleisten, dass der Zugang nur auf der Grundlage genau umrissener Bedingungen und Einschränkungen zulässig ist.

*Spezielle Datenkategorien*

w) Es sollten spezifische Garantien vorgesehen werden, um insbesondere zu gewährleisten, dass

— biometrische Daten und DNA-Profile nur auf der Grundlage sorgfältig festgelegter und interoperabler technischer Standards verwendet werden,

— ihre Richtigkeit sorgfältig berücksichtigt wird und von der betroffenen Person durch ohne Weiteres verfügbare Mittel angefochten werden kann und

— die Achtung der Würde der Person voll und ganz gewährleistet ist.

*Unterscheidung zwischen bestimmten Datenkategorien*

x) Personenbezogene Daten zu unterschiedlichen Personengruppen (Verdächtige, verurteilte Personen, Opfer, Zeugen usw.) sollten nach unterschiedlichen und angemessenen Bedingungen und Garantien verarbeitet werden. Der EDPS schlägt daher vor, in Artikel 4 einen neuen Absatz aufzunehmen, der folgende Punkte enthält:

— die Verpflichtung der Mitgliedstaaten, die Rechtsfolgen der Unterschiede, die zwischen personenbezogenen Daten unterschiedlicher Personengruppen zu machen sind, festzulegen;

— zusätzliche Bestimmungen, um den Zweck der Verarbeitung zu begrenzen, genaue Fristen festzulegen und den Zugang zu Daten einzuschränken, soweit Personen betroffen sind, die keine Verdächtige sind.

*Automatisierte Einzelentscheidungen*

y) Entscheidungen, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten ergehen, sollten sehr strengen Bedingungen unterliegen, wenn sie für eine Person Folgen nach sich ziehen oder die Person erheblich beeinträchtigen. Der EDPS empfiehlt daher, besondere Bestimmungen über automatisierte Einzelentscheidungen aufzunehmen, die an die Bestimmungen der Richtlinie 95/46/EG angelehnt sind.

*Weitere Empfehlungen*

z) Der EDPS empfiehlt,

— Artikel 4 Absatz 4 ersten Gedankenstrich so umzuformulieren, dass der Rechtsprechung zu Artikel 8 EMRK Rechnung getragen wird, da die vorgeschlagene Formulierung von Artikel 4 Absatz 4 nicht den Kriterien entspricht, die durch die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zu Artikel 8 EMRK festgesetzt wurden;

— die weit gesteckte Ausnahme in Artikel 7 Absatz 1 zu streichen oder zumindest die öffentlichen Interessen, die ihre Anwendung durch die Mitgliedstaaten rechtfertigen, ausdrücklich einzuschränken;

— Artikel 10 so zu ändern, dass auch der Zugang zu Daten protokolliert oder dokumentiert werden muss;

— in den Artikeln 19, 20 und 21 jeweils Absatz 2 Buchstabe a zu streichen;

— in den Vorschlag zusätzlich Bestimmungen zu Datenschutzbeauftragten aufzunehmen. Diese Bestimmungen könnten entsprechend den Artikeln 24 bis 26 der Verordnung 45/2001/EG gestaltet werden;

— Artikel 31 Absatz 2 des Vorschlags so zu ändern, dass auch der Vorsitzende der Art. 29 Datenschutzgruppe an Sitzungen der neuen Gruppe teilnehmen oder in ihnen vertreten sein kann.

Geschehen zu Brüssel am 19. Dezember 2005

Peter HUSTINX

*Europäischer Datenschutzbeauftragter*