DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten zum Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit (KOM (2005) 490 endgültig)

(2006/C 116/04)

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

1. Der Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit wurde dem Europäischen Datenschutzbeauftragten von der Kommission mit Schreiben vom 12. Oktober 2005 übermittelt. Der Europäische Datenschutzbeauftragte versteht dieses Schreiben als Ersuchen um Beratung der Organe und Einrichtungen der Gemeinschaft nach Artikel 28 Absatz 2 der Verordnung Nr. 45/2001/EG. Er ist der Auffassung, dass die vorliegende Stellungnahme in der Präambel des Rahmenbeschlusses erwähnt werden sollte.

2. Der Charakter dieser Stellungnahme muss im Zusammenhang mit den Ausführungen in Abschnitt II gesehen werden. Wie in Abschnitt II ausgeführt, ist es keineswegs selbstverständlich, dass der vorliegende Vorschlag — oder das im Vorschlag enthaltene Verfügbarkeitskonzept — letztendlich zur Annahme eines Rechtsakts führen wird. Zahlreiche Mitgliedstaaten plädieren nämlich für andere Konzepte.

3. Es liegt jedoch auf der Hand, dass das Thema der Verfügbarkeit von strafverfolgungsrelevanten Informationen über die innerstaatlichen Grenzen hinaus — oder, allgemeiner formuliert, der Austausch dieser Informationen — sowohl innerhalb als auch außerhalb des Rates sowie im Europäischen Parlament eine Priorität auf der Agenda der Mitgliedstaaten ist.

4. Auch ist offensichtlich, dass dieses Thema unter dem Gesichtspunkt des Schutzes personenbezogener Daten von großer Bedeutung ist, wie auch in dieser Stellungnahme dargelegt wird. Der Europäische Datenschutzbeauftragte weist darauf hin, dass die Vorlage des vorliegenden Vorschlags durch die Kommission in enger Verbindung steht 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, und zu dem er am 19. Dezember 2005 ebenfalls eine Stellungnahme abgegeben hat.

5. Der Europäische Datenschutzbeauftragte wird diese Gelegenheit nutzen, um in dieser Stellungnahme einige generelle und eher grundlegende Standpunkte zum Thema Austausch strafverfolgungsrelevanter Informationen und zu den Konzepten für die Regelung dieser Frage vorzulegen. Mit der Vorlage dieser Stellungnahme möchte er sicherstellen, dass der Aspekt des Datenschutzes bei künftigen Beratungen über dieses Thema gebührend berücksichtigt wird.

6. Der Europäische Datenschutzbeauftragte steht für weitere Konsultationen in einer späteren Phase zur Verfügung, wenn das Gesetzgebungsverfahren für diesen Vorschlag sowie für andere damit zusammenhängende Vorschläge weiter vorangekommen ist.

II. HINTERGRUND DES VORSCHLAGS

7. Der Verfügbarkeitsgrundsatz wurde als ein neuer wichtiger Rechtsgrundsatz mit dem Haager Programm eingeführt. Nach diesem Grundsatz können für die Kriminalitätsbekämpfung benötigte Informationen die Binnengrenzen der EU ungehindert passieren. Mit dem vorliegenden Vorschlag soll dieser Grundsatz in einen verbindlichen Rechtsakt umgesetzt werden.

8. Der Austausch polizeilicher Informationen zwischen verschiedenen Ländern ist für Gesetzgeber innerhalb und außerhalb des EU-Rahmens ein beliebtes Thema. Folgende Initiativen sind dem Europäischen Datenschutzbeauftragten in letzter Zeit aufgefallen.

9. Erstens hat Schweden am 4. Juni 2004 einen Rahmenbeschlusses über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union vorgelegt. Der Rat hat auf seiner Tagung vom 1. Dezember 2005 Einigung über eine allgemeine Ausrichtung zu diesem Vorschlag erzielt.

10. Zweitens haben sieben Mitgliedstaaten am 27. Mai 2005 in Prüm (Deutschland) einen Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration unterzeichnet. Mit diesem Vertrag werden unter anderem Maßnahmen zur Verbesserung des Austausches von DNS- und Fingerabdrucksinformationen eingeführt. Jeder Mitgliedstaat der Europäischen Union kann diesem Übereinkommen beitreten. Die Vertragsparteien haben die Absicht, die Bestimmungen des Vertrags in den Rechtsrahmen der Europäischen Union zu überführen.

11. Drittens wird die Verfügbarkeit von strafverfolgungsrelevanten Informationen über die Binnengrenzen der Europäischen Union hinweg auch durch andere Rechtsakte weiter erleichtert werden, beispielsweise durch die Vorschläge zum Schengener Informationssystem der zweiten Generation (SIS II), den Vorschlag über den Zugang zum Visa-Informationssystem (VIS) und den Vorschlag für einen Rahmenbeschluss über die Durchführung und den Inhalt des Austausches von Informationen aus den Strafregistern zwischen den Mitgliedstaaten. In diesem Zusammenhang sei auch auf die am 25. November 2005 von der Kommission veröffentlichte Mitteilung über die Verbesserung der Effizienz der europäischen Datenbanken im Bereich Justiz und Inneres und die Steigerung ihrer Interoperabilität sowie der Synergien zwischen ihnen hingewiesen.

12. In Anbetracht all dieser Initiativen liegt es auf der Hand, dass der vorliegende Vorschlag für einen Rahmenbeschluss zur Verfügbarkeit von Informationen nicht isoliert geprüft werden sollte, sondern dass auch andere Konzepte für den Austausch strafverfolgungsrelevanter Informationen berücksichtigt werden sollten. Dies ist umso wichtiger, als derzeit im Rat die Tendenz besteht, anderen Konzepten für den Informationsaustausch und für den Begriff der Verfügbarkeit als dem in diesem Kommissionsvorschlag enthaltenen allgemeinen Konzept Vorrang einzuräumen. Es ist durchaus möglich, dass der Vorschlag in der vorliegenden Fassung im Rat nicht einmal erörtert wird.

13. Ferner hängt dieser Vorschlag eng mit dem Vorschlag für einen Rahmenbeschluss über den Schutz personenbezogener Daten zusammen. Diese Stellungnahme muss im Zusammenhang mit der ausführlicheren Stellungnahme zum letztgenannten Rahmenbeschluss gesehen werden.

14. In seiner Stellungnahme zum Vorschlag für einen Rahmenbeschluss über den Schutz personenbezogener Daten hat der Europäische Datenschutzbeauftragte betont, wie wichtig ein angemessener Datenschutz als notwendige Folge eines Rechtsakts zur Verfügbarkeit von Informationen ist. Nach Auffassung des Europäischen Datenschutzbeauftragten sollte ein solcher Rechtsakt erst angenommen werden, wenn die wesentlichen datenschutzrechtlichen Garantien vorgesehen sind.

15. Der Europäische Datenschutzbeauftragte vertritt dieselbe Auffassung in Bezug auf die Annahme anderer Rechtsakte, mit denen der Fluss strafverfolgungsrelevanter Informationen über die EU-Binnengrenzen hinweg erleichtert werden soll. Daher begrüßt er es, dass sowohl der Rat als auch das Europäische Parlament dem oben genannten Vorschlag für einen Rahmenbeschluss über den Schutz personenbezogener Daten Vorrang eingeräumt haben.

III. DER VERFÜGBARKEITSGRUNDSATZ ALS SOLCHER

16. Der Verfügbarkeitsgrundsatz als solcher ist ein einfacher Grundsatz. Die Informationen, über die bestimmte Behörden in einem Mitgliedstaat verfügen, müssen auch gleichwertigen Behörden in anderen Mitgliedstaaten zur Verfügung gestellt werden. Die Informationen müssen so rasch und unkompliziert wie möglich zwischen den Behörden der Mitgliedstaaten ausgetauscht werden, und zwar vorzugsweise, indem ein unmittelbarer Online-Zugang zu den Daten gewährt wird.

17. Die Schwierigkeiten entstehen durch die Umgebung, in der der Verfügbarkeitsgrundsatz umgesetzt werden soll:

— Eine heterogene Organisation von Polizei und Justiz in den Mitgliedstaaten mit einer unterschiedlichen Kompetenzverteilung.

— Es werden unterschiedliche Arten von (sensiblen) Informationen erfasst (wie DNS oder Fingerabdrücke).

— Sogar innerhalb eines einzigen Mitgliedstaates bestehen für die zuständigen Behörden unterschiedliche Möglichkeiten des Zugriffs auf einschlägige Informationen.

— Aufgrund sprachlicher Unterschiede sowie Unterschiede zwischen den technologischen Systemen (Interoperabilität) und den Rechtssystemen ist es schwierig zu gewährleisten, dass Informationen aus einem anderen Mitgliedstaat richtig interpretiert werden.

— Der Grundsatz muss sich in das bestehende und umfassende Gefüge von Rechtsvorschriften für den länderübergreifenden Austausch von strafverfolgungsrelevanten Informationen einpassen.

18. Ungeachtet dieser komplexen Umgebung wird allgemein anerkannt, dass der Grundsatz für sich alleine genommen nicht funktionieren kann. Es bedarf zusätzlicher Maßnahmen um sicherzustellen, dass die Informationen tatsächlich gefunden und abgerufen werden können. Diese Maßnahmen müssen es den Strafverfolgungsbehörden auf jeden Fall erleichtern, herauszufinden, ob Strafverfolgungsbehörden in anderen Mitgliedstaaten über einschlägige Informationen verfügen und wo diese einschlägigen Informationen gefunden werden können. Solche ergänzenden Maßnahmen könnten darin bestehen, Schnittstellen einzurichten, die einen unmittelbaren Zugang zu allen oder zu spezifischen Daten ermöglichen, über die andere Mitgliedstaaten verfügen. Mit dem Vorschlag für einen Rahmenbeschluss über die Verfügbarkeit werden daher „Indexdaten“ eingeführt. Dabei handelt es sich um spezifische Daten, die grenzüberschreitend unmittelbar abgerufen werden können.

19. Ganz allgemein sollte der Verfügbarkeitsgrundsatz den Informationsfluss zwischen den Mitgliedstaaten erleichtern. Die Binnengrenzen werden abgeschafft, und die Mitgliedstaaten müssen gestatten, dass Informationen, die im Besitz ihrer Polizeibehörden sind, in zunehmenden Maße auch anderen Behörden zur Verfügung stehen. Die Mitgliedstaaten verlieren die Zuständigkeit für die Kontrolle über den Informationsfluss, was auch dazu führen wird, dass sie sich nicht länger auf ihre innerstaatlichen Rechtsvorschriften als ausreichendes Instrument für einen angemessenen Schutz der Informationen verlassen können.

20. Aus diesem Grund muss dem Vorschlag unter dem Gesichtspunkt des Schutzes personenbezogener Daten besondere Aufmerksamkeit gewidmet werden. Erstens müssen Informationen, die in der Regel vertraulich und gut gesichert sind, Behörden in anderen Mitgliedstaaten zur Verfügung gestellt werden. Zweitens ist es für das reibungslose Funktionieren der Regelung erforderlich, dass Indexdaten erzeugt und den Behörden in anderen Mitgliedstaaten zur Verfügung gestellt werden. Die Umsetzung dieses Grundsatzes wird folglich mehr Daten als die derzeit verfügbaren Daten.

IV. WICHTIGSTE ELEMENTE

Anwendungsbereich des Verfügbarkeitsgrundsatzes

21. Zunächst einmal ist es von wesentlicher Bedeutung festzulegen, für welche Art von Informationen der Verfügbarkeitsgrundsatz gelten wird. Der Anwendungsbereich dieses Grundsatzes ist allgemein in Artikel 2 des Vorschlags in Verbindung mit Artikel 1 Absatz 1 und Artikel 3 Buchstabe a festgelegt. Der Grundsatz findet auf die nachstehenden Informationen Anwendung:

    — vorhandene Informationen;

    — Informationen nach Anhang II, in dem sechs Informationsarten aufgeführt sind;

    — die den zuständigen Behörden zur Verfügung stehenden Informationen.

    Dies sind die drei wesentlichen Komponenten des Anwendungsbereichs des Verfügbarkeitsgrundsatzes nach dem Kommissionsvorschlag. Der Anwendungsbereich wird in Artikel 2 näher ausgeführt. In Artikel 2 Absatz 1 wird die Anwendung des Verfügbarkeitsgrundsatzes auf die Phase vor der Einleitung einer Strafverfolgungsmaßnahme beschränkt, während in Artikel 2 Absätze 2, 3 und 4 einige weitere spezifische Einschränkungen enthalten sind.

22. Zum besseren Verständnis der Auswirkungen des Vorschlags müssen die drei vorgenannten wesentlichen Komponenten eingehender analysiert werden. Die ersten beiden Komponenten des Anwendungsbereichs sind an sich ziemlich klar. Die Definition des Begriffs „vorhandene Informationen" wird in Artikel 2 Absatz 2 näher ausgeführt. Darin ist vorgesehen, dass der Rahmenbeschluss nicht die Verpflichtung beinhaltet, Informationen ausschließlich zum Zweck ihrer Weitergabe zu sammeln und zu speichern. Beim Verzeichnis in Anhang II ist die Gefahr von unterschiedlichen Auslegungen nicht gegeben. Es ist die dritte wesentliche Komponente, die an sich und in Verbindung mit den ersten beiden Komponenten einer weiteren Klarstellung bedarf.

23. In dem Vorschlag ist nicht angegeben, ob „vorhandene Informationen" lediglich Informationen sind, die bereits im Besitz der zuständigen Behörden sind, bzw. ob damit auch Informationen gemeint sind, die diese Behörden potenziell erhalten können. Nach Auffassung des Europäischen Datenschutzbeauftragten könnte der Vorschlag dahingehend ausgelegt werden, dass beide Arten von Informationen erfasst sind.

24. Zwar scheint sich aus Artikel 2 Absatz 2 insoweit ein engerer Anwendungsbereich zu ergeben, als vorgesehen ist, dass der Rahmenbeschluss „nicht dazu verpflichtet, Informationen zu dem ausschließlichen Zweck der Weitergabe […] zu sammeln und zu speichern" ; Artikel 3 Buchstabe a ermöglicht jedoch eine extensivere Auslegung, da darin vorgesehen ist, dass mit „Informationen" „vorhandene Informationen im Sinne von Anhang II" gemeint sind.

25. In Anhang II werden mindestens zwei Kategorien von Daten aufgeführt, die in der Regel nicht im Besitz der Polizei, sondern im Besitz von anderen Stellen sind. Die erste Kategorie betrifft Informationen zur Kfz-Registrierung. In vielen Mitgliedstaaten werden Datenbanken, die diese Informationen enthalten, nicht von den Strafverfolgungsbehörden verwaltet, auch wenn diese Behörden diese Datenbanken regelmäßig abfragen. Sollte diese Art von Informationen als „vorhandene Informationen" betrachtet werden, die gemäß Artikel 1 gleichwertigen zuständigen Behörden anderer Mitgliedstaaten zur Verfügung gestellt werden? Die zweite zu erwähnende Kategorie von in Anhang II aufgeführten Daten sind die Telefonnummern und andere Verbindungsdaten: Sollten diese Daten als „vorhanden" betrachtet werden, auch wenn sie nicht im Besitz von zuständigen Behörden, sondern im Besitz von privaten Einrichtungen sind?

26. Ferner wird der Standpunkt, wonach „verfügungsberechtigte Behörden" und sogar „verfügungsberechtigte Stellen" Informationen besitzen können, die für „zuständige Behörden" „vorhanden" sind, durch andere Bestimmungen des Vorschlags, insbesondere Artikel 3 Buchstabe d und Artikel 4 Absatz 1 Buchstabe c bestätigt. Aus dem Wortlaut des Vorschlags ergibt sich auch, dass eine „zuständige Behörde" eines Mitgliedstaats eine Behörde im Sinne des Artikels 29 erster Gedankenstrich des EU-Vertrags ist, während jede nationale Behörde als „verfügungsberechtigte Behörde" gelten kann.

27. Nach Auffassung des Europäischen Datenschutzbeauftragten wirft die Anwendung des Verfügbarkeitsgrundsatzes auf Informationen, die im Besitz von „verfügungsberechtigten Behörden" oder „verfügungsberechtigten Stellen" sind, folgende Fragen auf:

    — Bietet Artikel 30 Absatz 1 Buchstabe b eine ausreichende Rechtsgrundlage, da Informationen von verfügungsberechtigten Behörden oder verfügungsberechtigten Stellen bereitgestellt gestellt werden müssen und aus Datenbanken stammen, die nicht von der dritten Säule erfasst sind?

    — Wird der Rahmenbeschluss über den Schutz personenbezogener Daten Anwendung finden, wovon beispielsweise in Artikel 8 des Vorschlags ausgegangen wird?

    — Wenn nicht, erfolgt die Verarbeitung gemäß den in der Richtlinie 95/46/EG enthaltenen Verpflichtungen?

28. Zur Umsetzung eines so umfassenden Grundsatzes wie des „Verfügbarkeitsgrundsatzes“ muss eindeutig und genau definiert werden, welche Daten als vorhandene Daten betrachtet werden. Daher empfiehlt der Europäische Datenschutzbeauftragte Folgendes:

— Der Anwendungsbereich sollte klargestellt werden.

— Eine erste Option besteht darin, den Anwendungsbereich des Verfügbarkeitsgrundsatzes auf Informationen zu beschränken, die im Besitz der zuständigen Behörden sind.

— Eine zweite Option besteht darin, im Falle eines breiteren Anwendungsbereichs ausreichende Garantien für den Schutz personenbezogener Daten vorzusehen. Die in Nummer 27 aufgeworfenen Fragen müssen berücksichtigt werden.

Andere Fragen im Zusammenhang mit dem Anwendungsbereich

29. Gemäß Artikel 2 Absatz 1 des Vorschlags gilt der Rahmenbeschluss für die Verarbeitung von Informationen vor Einleitung einer Strafverfolgungsmaßnahme. Dieser Anwendungsbereich ist beschränkter als jener des Vorschlags für einen Rahmenbeschluss über den Schutz personenbezogener Daten, der ohne Einschränkung auf die justizielle Zusammenarbeit in Strafsachen Anwendung findet.

30. Nach Auffassung des Europäischen Datenschutzbeauftragten wird der Anwendungsbereich des Vorschlags mit dieser Einschränkung an sich jedoch nicht auf die polizeiliche Zusammenarbeit beschränkt. Er könnte auch die justizielle Zusammenarbeit in Strafsachen umfassen, da in einigen Mitgliedstaaten die Justizbehörden auch für strafrechtliche Ermittlungen vor Einleitung der Strafverfolgung zuständig sind. Die Tatsache jedoch, dass der Vorschlag ausschließlich auf Artikel 30 Absatz 1 Buchstabe b EUV gestützt ist, scheint darauf hinzudeuten, dass nur die polizeiliche Zusammenarbeit erfasst ist. Eine Klarstellung in Bezug auf diesen Aspekt wäre zu begrüßen.

31. Der vorliegende Vorschlag gilt für die Übermittlung von Informationen an Europol, während die Verarbeitung personenbezogener Daten durch Europol vom Anwendungsbereich des Rahmenbeschlusses über den Schutz personenbezogener Daten ausgenommen ist. Der Europäische Datenschutzbeauftragte empfiehlt, den Informationsaustausch mit Europol auf die eigentlichen Europol-Zwecke, die in Artikel 2 des Europol-Übereinkommens und dem dazugehörigen Anhang aufgeführt sind, zu beschränken. Ferner sollten die detaillierten Regeln für den Datenaustausch mit Europol beachtet werden, die bereits in mehreren Rechtakten des Rates niedergelegt wurden.

Keine neuen Datenbanken mit personenbezogenen Daten

32. Ausgangspunkt des Vorschlag ist, dass er nicht zur Errichtung von neuen Datenbanken mit personenbezogenen Daten führen wird. Diesbezüglich ist Artikel 2 Absatz 2 eindeutig: Es wird keine Verpflichtung begründet, Informationen ausschließlich zum Zeck ihrer Weitergabe zu sammeln und zu speichern. Unter dem Gesichtspunkt des Datenschutzes ist dies ein wichtiger und positiver Aspekt des Vorschlags. Der Europäische Datenschutzbeauftragte erinnert an seine Stellungnahme zum Vorschlag für eine Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden ([1]), in der er hervorgehoben hat, dass rechtliche Verpflichtungen, die zu umfangreichen Datenbanken führen, für den Betroffenen besondere Risiken bergen, unter anderem wegen der Gefahr der unrechtmäßigen Nutzung der Daten.

33. Es muss jedoch Folgendes berücksichtigt werden:

— Es ist wichtig, dafür zu sorgen, dass durch den Vorschlag nicht eine mit keinerlei Auflagen verbundene Verknüpfung von Datenbanken gefördert wird, die ein Netz von Datenbanken entstehen lassen würde, das sich kaum noch überwachen ließe.

— Es gibt eine Ausnahme von dem oben genannten Ausgangspunkt: Mit Artikel 10 des Vorschlags wird sichergestellt, dass Indexdaten online abgefasst werden können. Indexdaten können personenbezogene Daten enthalten oder zumindest auf deren Existenz hinweisen.

Mittelbarer und unmittelbarer Zugang zu Informationen

34. In dem Vorschlag ist der mittelbare und unmittelbare Zugang zu Informationen vorgesehen. In Artikel 9 ist der unmittelbare Online-Zugang auf in elektronischen Datenbanken gespeicherte Informationen vorgesehen, auf die die entsprechenden nationalen Behörden unmittelbar online zugreifen können. In Artikel 10 ist eine mittelbare Zugriffsmöglichkeit vorgesehen. Indexdaten, die auf online nicht zugängliche Informationen verweisen, können von gleichwertigen zuständigen Behörden anderer Mitgliedstaaten sowie von Europol online abgefragt werden. Ist die Suche in den Indexdaten erfolgreich, so kann die betreffende Behörde eine Informationsanfrage an die verfügungsberechtigte Behörde richten, um sich die durch die Indexdaten ermittelten Informationen zu beschaffen.

35. Der unmittelbare Zugang führt nicht zur Einrichtung neuer Datenbanken, erfordert jedoch eine Interoperabilität der Datenbanken der gleichwertigen zuständigen Systeme in den Mitgliedstaaten. Ferner wird dies zwangsläufig insofern zu einer neuen Nutzung bereits bestehender Datenbanken führen, als für alle zuständigen Behörden der Mitgliedstaaten eine Nutzungsmöglichkeit vorgesehen wird, die bislang nur nationalen zuständigen Behörden vorbehalten war. Der unmittelbare Zugang wird automatisch dazu führen, dass eine größere Anzahl von Personen Zugang zu einem Datenbestand haben wird, was daher auch ein zunehmendes Missbrauchsrisiko mit sich bringt.

([1]) Stellungnahme vom 26. September 2005 zum 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).

36. Im Falle des unmittelbaren Zugangs durch eine zuständige Behörde eines anderen Mitgliedstaats haben die verfügungsberechtigten Behörden des Mitgliedstaats, aus dem die Daten stammen, keine Kontrolle über den Zugriff auf die Daten und über deren weitere Nutzung. Diese Folge des im Vorschlag vorgesehenen unmittelbaren Zugangs muss aus folgenden Gründen genau geregelt werden:

— Die Befugnisse der verfügungsberechtigten Behörden, die Bereitstellung von Informationen zu verweigern (Artikel 14) scheinen dadurch unterlaufen zu werden.

— Wer ist für die Richtigkeit und die Aktualisierung der Daten verantwortlich, nachdem diese abgerufen wurden? Wie kann eine verfügungsberechtigte Behörde des Mitgliedstaates, aus dem die Daten stammen, sicherstellen, dass diese aktualisiert werden?

— Zum einen ist die verfügungsberechtigte Behörde nicht mehr in der Lage, alle ihre datenschutzrechtlichen Verpflichtungen einzuhalten, und zum anderen kann auch die nationale Datenschutzbehörde des Mitgliedstaats, aus dem die Daten stammen, die Anwendung der Verpflichtungen nicht länger überwachen, da sie nicht für die Strafverfolgungsbehörden anderer Mitgliedstaaten zuständig ist.

— Diese Probleme sind noch akuter im Falle des Zugangs zu Datenbanken von verfügungsberechtigten Behörden und verfügungsberechtigten Stellen, die keine Strafverfolgungsbehörden sind (siehe die Nummern 25-28 dieser Stellungnahme).

Diese Folge des unmittelbaren Zugangs erklärt weitgehend, weshalb die Annahme des vorliegenden Vorschlags von der Annahme eines Rahmenbeschlusses über den Schutz personenbezogener Daten abhängen sollte. Ein Problem besteht nach wie vor: Es ist kaum ersichtlich, wie eine verfügungsberechtigte Behörde die Bereitstellung von Informationen nach Artikel 14 verweigern kann.

37. Was den mittelbaren Zugang anhand von Indexdaten anbelangt, die im Wege eines Treffer/kein Treffer-Systems Informationen liefern, so ist dies kein neues Phänomen. Auf dieser Grundlage funktionieren große europäische Informationssysteme wie das Schengener Informationssystem. Die Einrichtung eines Systems mit Indexdaten bietet den Vorteil, dass die Mitgliedstaaten, aus denen die Daten stammen, den Austausch von Informationen aus ihren Polizeidateien kontrollieren können. Führt die Abfrage von Indexdaten zu einem Trefferfall, so kann die ersuchende Behörde eine Informationsanfrage zu der betreffenden Person stellen. Diese Informationsanfrage kann von der ersuchten Behörde genau überprüft werden.

38. Eine genaue Analyse ist jedoch erforderlich, da die Einrichtung eines Systems mit Indexdaten in Bereichen, in denen diese Systeme — abgesehen von den großen europäischen Informationssystemen — bisher nicht existierten, neue Risiken für das Datensubjekt mit sich bringen können. Der Europäische Datenschutzbeauftragte betont, dass Indexdaten zwar nicht viele Informationen zum Datensubjekt enthalten, die Abfrage von Indexdaten jedoch zu einem hoch sensiblen Ergebnis führen kann. Sie kann Aufschluss darüber erteilen, dass Daten zu einer Person im Zusammenhang mit Straftaten in einer Polizeidatei gespeichert sind.

39. Daher ist es von größter Bedeutung, dass der europäische Gesetzgeber angemessene Regeln vorsieht, zumindest für die Erzeugung von Indexdaten, die Verwaltung der Dateien mit Indexdaten und für die angemessene Organisation des Zugriffs auf diese Daten. Der Europäische Datenschutzbeauftragte hält den Vorschlag in diesen Punkten für nicht befriedigend. In der derzeitigen Phase möchte er drei Bemerkungen formulieren:

— Die Definition der Indexdaten ist unklar. Es ist nicht deutlich, ob Indexdaten als Metadaten, Primärschlüssel oder sogar beides zu verstehen sind. Der Begriff der Indexdaten muss präzisiert werden, da er eine unmittelbare Auswirkung auf das Datenschutzniveau und auf die notwendigen Garantien hat.

— In dem Vorschlag sollte klargestellt werden, welche Rolle die nationalen Kontaktstellen in Bezug auf Indexdaten haben. Eine Einschaltung von nationalen Kontaktstellen könnte sich insbesondere in Fällen als notwendig erweisen, in denen die Interpretation der Indexdaten besondere Fachkenntnisse erfordert, wie beispielsweise bei der etwaigen Zuordnung von Fingerabdrücken.

— Nach dem Vorschlag sollen die Vorschriften für die Zusammenstellung der Indexdaten im Rahmen von Durchführungsbestimmungen angenommen werden, die nach dem in Artikel 19 vorgesehenen Regelungsverfahren zu erlassen sind. Der Erlass von Durchführungsbestimmungen wird wohl unumgänglich sein, doch sollten die grundlegenden Vorschriften für die Zusammenstellung von Indexdaten im Rahmenbeschluss selbst enthalten sein.

Vorherige Genehmigung durch die Justizbehörden

40. Der Informationsaustausch darf die Mitgliedstaaten nicht davon abhalten, vorzuschreiben, dass bei den Justizbehörden eine vorherige Genehmigung zur Übermittlung der Informationen an die ersuchende Behörde eingeholt werden muss, wenn diese Informationen im ersuchten Land der Kontrolle der Justizbehörden unterliegen. Dies ist wichtig, da eine Untersuchung in Bezug auf die Befugnisse der Polizei für den Austausch von personenbezogenen Daten ([1]) ergeben hat, dass die Polizei nicht in allen Mitgliedstaaten einen autonomen Zugriff auf diese Daten hat. Nach Auffassung des Europäischen Datenschutzbeauftragten sollte der Verfügbarkeitsgrundsatz die nach innerstaatlichem Recht bestehende Verpflichtung, in Bezug auf die Informationen eine vorherige Genehmigung einzuholen, nicht beeinträchtigen. Zumindest sollten aber spezifische, in allen Mitgliedstaaten anwendbare Regeln für die Kategorien von Daten festgelegt werden, deren Übermittlung eine vorherige Genehmigung erfordert.

([1]) Antworten auf den Fragebogen zum Rahmenbeschluss über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der EU, insbesondere in Bezug auf schwerwiegende Straftaten einschließlich terroristischer Handlungen (Dokument des Rates 5815/1/05).

41. Diese Verpflichtung sollte in Verbindung mit Artikel 11 Absatz 2 des Vorschlags für einen Rahmenbeschluss über den Schutz personenbezogener Daten ausgelegt werden, in dem ebenfalls vorgesehen ist, dass der übermittelnde Mitgliedstaat in Bezug auf die weitere Nutzung der Daten in dem Mitgliedstaat, an den die Daten übermittelt wurden, ein Mitspracherecht hat. Der Europäische Datenschutzbeauftragte betont, wie wichtig dieser Grundsatz ist, mit dem sichergestellt werden muss, dass die Verfügbarkeit nicht dazu führen wird, dass die restriktiven innerstaatlichen Rechtsvorschriften über die weitere Nutzung personenbezogener Daten umgangen werden.

Schlussbemerkung

42. Diese Elemente erfordern einen hohen Datenschutzstandard. Besondere Aufmerksamkeit sollte der Gewährleistung der Grundsätze der Einschränkung des Verwendungszwecks und der Weiterverarbeitung sowie der Richtigkeit und der Zuverlässigkeit der abgerufenen Informationen gewidmet werden (siehe die Stellungnahme des Europäischen Datenschutzbeauftragten zum Rahmenbeschluss über den Schutz personenbezogener Daten, Abschnitte IV.2 und IV.6).

V. ANDERE KONZEPTE

Vorschlag Schwedens

43. Der schwedische Vorschlag ist nicht auf bestimmte Arten von Informationen beschränkt, sondern umfasst alle Informationen *und Erkenntnisse,* sogar solche, die im Besitz von anderen als den zuständigen Strafverfolgungsbehörden sind. In dem Vorschlag wird die Zusammenarbeit gefördert, indem Fristen für die Beantwortung von Informationsanfragen vorgegeben werden und die Diskriminierung zwischen dem Informationsaustausch innerhalb eines Mitgliedstaates und dem grenzüberschreitenden Informationsaustausch abgeschafft wird. Es sind keine zusätzlichen Maßnahmen vorgesehen, um sicherzustellen, dass die Informationen tatsächlich abgerufen werden können. Aus diesem Grunde ist nachvollziehbar, dass der schwedische Vorschlag als solcher nach Auffassung der Kommission kein angemessenes Instrument für die Verfügbarkeit von Informationen darstellt ([1]).

44. Aus datenschutzrechtlicher Sicht hat das Konzept im schwedischen Vorschlag die folgenden allgemeinen Auswirkungen:

— Es wird begrüßt, dass der Vorschlag strikt auf die Verarbeitung bestehender Daten beschränkt ist und nicht zur Errichtung neuer Datenbanken und nicht einmal zur Erzeugung von Indexdaten führt.

— Jedoch ist die Tatsache, dass keine Indexdaten vorgesehen sind, nicht unbedingt ein positives Element. Auf angemessene Weise gesicherte Indexdaten können eine gezielte und daher weniger eingreifende Suche nach sensiblen Daten erleichtern. Sie können auch zu einer besseren Filterung der Informationsanfragen und einer besseren Überwachung beitragen.

— Der Vorschlag führt auf jeden Fall zu einer Zunahme des grenzüberschreitenden Austausches personenbezogener Daten, was mit Risiken für den Schutz personenbezogener Daten verbunden ist, unter anderem weil die Zuständigkeit der Mitgliedstaaten, den Datenaustausch umfassend zu kontrollieren, beeinträchtigt wird. Der Vorschlag sollte nicht unabhängig von der Annahme des Rahmenbeschlusses über den Schutz personenbezogener Daten angenommen werden.

([1]) Siehe Arbeitsdokument der Kommission — Anlage zum Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Daten nach dem Verfügbarkeitsgrundsatz, SEK 2005 (1207) vom 12.10.2005.

Vertrag von Prüm

45. Im Vertrag von Prüm ist ein anderes Konzept in Bezug auf den Verfügbarkeitsgrundsatz vorgesehen. Im Gegensatz zu dem im vorliegenden Vorschlag für einen Rahmenbeschluss enthaltenen allgemeinen Konzept — wonach keine spezifischen Regeln für den Austausch spezifischer Arten von Informationen, sondern für alle Informationsarten geltende Regeln vorgesehen sind, soweit diese in Anhang II aufgeführt sind (siehe die Nummern 21–28 dieser Stellungnahme) — sieht der Vertrag von Prüm einen schrittweisen Ansatz vor.

46. Dieser Ansatz wird manchmal „Datenfeld-für-Datenfeld"-Ansatz genannt. Er gilt für bestimmte Arten von Informationen (DNS, Fingerabdruck- und Fahrzeugregisterdaten) und umfasst die Verpflichtung, die spezifische Art der Daten zu berücksichtigen. Nach dem Vertrag müssen zum Zwecke der Untersuchung von Straftaten nationale DNS-Analyse-Dateien errichtet und geführt werden. Eine ähnliche Verpflichtung ist für Fingerabdruckdaten vorgesehen. In Bezug auf die Fahrzeugregisterdaten muss den nationalen Kontaktstellen anderer Mitgliedstaaten ein unmittelbarer Zugang gewährt werden.

47. Das im Vertrag von Prüm gewählte Konzept gibt Anlass zu drei Arten von Bemerkungen.

48. Erstens ist es natürlich klar, dass der Europäische Datenschutzbeauftragte nicht ein Verfahren gutheißen kann, das außerhalb des institutionellen Rahmens der Europäischen Union und daher ohne die substanzielle Beteiligung der Kommission zu diesem Vertrag geführt hat. Ferner bedeutet dies, dass eine demokratische Kontrolle durch das Europäische Parlament nicht stattgefunden hat und dass auch die gerichtliche Kontrolle durch den Gerichtshof ausbleibt, weshalb es weniger Garantien dafür gibt, dass alle (öffentlichen) Interessen in ausgewogener Weise berücksichtigt werden. Dies gilt auch für den Aspekt des Datenschutzes. Mit anderen Worten haben die Organe der Europäischen Union keine Möglichkeit, vor der Einrichtung des Systems zu bewerten, welche Auswirkungen die gewählte Strategie auf den Schutz personenbezogener Daten haben wird.

49. Zweitens liegt es auf der Hand, dass einige Elemente des Vertrags von Prüm für das Datensubjekt eindeutig eine eingreifendere Wirkung haben als der Rahmenbeschluss über die Verfügbarkeit. Der Vertrag führt zwangsläufig zur Einrichtung neuer Datenbanken, was zu Risiken für den Schutz personenbezogener Daten führt. Die Notwendigkeit und Verhältnismäßigkeit der Einrichtung dieser neuen Datenbanken sollten nachgewiesen werden. Es sollten angemessene Garantien für den Schutz personenbezogener Daten vorgesehen werden.

„Ein Datenfeld-für-Datenfeld-Ansatz"

50. Drittens ist im Vertrag — wie bereits erwähnt — ein Datenfeld-für-Datenfeld-Ansatz vorgesehen. Der Europäische Datenschutzbeauftragte hat in dieser Stellungnahme bereits auf die Schwierigkeiten und Ungewissheiten hingewiesen, die mit der Umgebung zusammenhängen, in der der Verfügbarkeitsgrundsatz umgesetzt werden muss. Unter diesen Umständen wäre es nach Auffassung des Datenschutzbeauftragten besser, kein System für eine Reihe von Daten einzurichten, sondern mit einem vorsichtigeren Konzept zu beginnen, das eine Datenart umfasst, und zu prüfen, inwieweit der Verfügbarkeitsgrundsatz eine wirksame Hilfe bei der Strafverfolgung sein kann und welches die spezifischen Risiken für den Schutz personenbezogener Daten sein können. Anhand dieser Erfahrungen könnte das System gegebenenfalls auf andere Datentypen ausgeweitet und/oder geändert werden, um es wirksamer zu gestalten.

51. Mit diesem Datenfeld-für-Datenfeld-Ansatz könnte auch besser den Anforderungen des Verhältnismäßigkeitsgrundsatzes entsprochen werden. Nach Auffassung des Europäischen Datenschutzbeauftragten könnte der Bedarf an einem besseren grenzüberschreitenden Datenaustausch für die Zwecke der Strafverfolgung die Annahme eines Rechtsakts auf EU-Ebene rechtfertigen; im Interesse der Verhältnismäßigkeit sollte das Instrument jedoch angemessen sein, um das damit verfolgte Ziel zu erreichen, was sich nach einem Zeitraum praktischer Erfahrungen besser nachweisen lässt. Ferner sollte dem Datensubjekt mit dem Rechtsakt nicht unverhältnismäßig geschadet werden. Der Austausch sollte nicht mehr Datenarten umfassen, als unbedingt notwendig ist, wobei eine Möglichkeit des anonymen Datenaustausches vorgesehen werden sollte, und sollte unter strikter Einhaltung der Voraussetzungen für den Datenschutz erfolgen.

52. Ferner könnte ein vorsichtigeres Konzept, wie es vom Europäischen Datenschutzbeauftragten befürwortet wird, eventuell ergänzend zum„Datenfeld-für-Datenfeld-Ansatz" beinhalten, dass nur im Wege des mittelbaren Zugangs anhand von Indexdaten mit der Umsetzung des Verfügbarkeitsgrundsatzes begonnen wird. Der Datenschutzbeauftragte erwähnt diesen Punkt, damit er im weiteren Gesetzgebungsverfahren berücksichtigt wird.

VI. **WELCHE DATEN?**

53. In Anhang II sind die Informationsarten aufgeführt, auf die nach dem vorgeschlagenen Rahmenbeschluss zugegriffen werden darf. Die sechs dort aufgeführten Informationsarten sind personenbezogene Daten, da sie alle einer bestimmten oder bestimmbaren Person zugeordnet werden können.

54. Nach Artikel 3 Buchstabe g des Vorschlags bezeichnet der Ausdruck „Indexdaten" Daten, deren Zweck darin besteht, gezielt auf Informationen zu verweisen, die mit Hilfe einer Suchroutine abgefragt werden können um festzustellen, ob Informationen vorliegen oder nicht. In dem „Konzept zur Umsetzung des Grundsatzes der Verfügbarkeit" [1] werden die nachstehenden Daten als Indexdaten eingestuft:

— die Identifizierungsdaten der betreffenden Personen;

— eine Identifizierungsnummer für die betreffenden Objekte (Fahrzeuge, Dokumente);

— Fingerabdrücke/Digitalfotos.

Ein anderer Typ von Daten, die als Indexdaten eingestuft werden könnten, sind DNS-Profile. Diese Liste von Indexdaten zeigt, dass Indexdaten personenbezogene Daten beinhalten können und ein angemessener Schutz daher erforderlich ist.

55. Der Europäische Datenschutzbeauftragte möchte speziell auf die Frage der DNS-Profile eingehen. Die DNS-Analyse ist für die Aufklärung von Straftaten nachgewiesenermaßen sehr wichtig, und ein effizienter Austausch von DNS-Daten kann für die Kriminalitätsbekämpfung von wesentlicher Bedeutung sein. Entscheidend ist jedoch, dass das Konzept von DNS-Daten eindeutig definiert wird und dass den speziellen Merkmalen dieser Daten gebührend Rechnung getragen wird. Aus datenschutzrechtlicher Sicht gibt es nämlich einen großen Unterschied zwischen DNS-Proben und DNS-Profilen.

56. DNS-Proben (die oft von Strafverfolgungsbehörden erhoben und gespeichert werden) sollten als besonders sensibel betrachtet werden, da sie mit größerer Wahrscheinlichkeit das gesamte DNS-Bild enthalten. Sie können Informationen über genetische Merkmale und über den Gesundheitszustand einer Person liefern, was für völlig andere Zwecke — z.B. zur medizinischen Beratung von Einzelpersonen oder jungen Paaren — erforderlich sein kann.

57. DNS-Profile hingegen enthalten nur einen Teil der aus der DNS-Probe gewonnenen DNS-Informationen: Sie können zur Überprüfung der Identität einer Person genutzt werden, aber erteilen grundsätzlich keinen Aufschluss über die genetischen Merkmale einer Person. Allerdings kann der wissenschaftliche Fortschritt zu einer Zunahme der von DNS-Profilen gelieferten Informationen führen: Was zu einem bestimmten Zeitpunkt als „unschuldiges" DNS-Profil betrachtet wird, kann später viel mehr Informationen liefern als erwartet wurde und notwendig ist, insbesondere Informationen über die genetischen Merkmale einer Person. Die Informationen aus DNS-Profilen sollten daher als dynamische Informationen betrachtet werden.

58. Vor diesem Hintergrund hält der Europäische Datenschutzbeauftragte fest, dass sowohl der Vertrag von Prüm als auch der Kommissionsvorschlag den Austausch von DNS zwischen den Strafverfolgungsbehörden fördern, dies jedoch auf unterschiedliche Art und Weise tun.

[1] Dokument des Vorsitzes an den Rat vom 5. April 2005 (Dok. 7641/05).

59. Der Europäische Datenschutzbeauftragte begrüßt, dass im Kommissionsvorschlag keine Verpflichtung zur Erhebung von DNS-Daten enthalten und der Austausch von DNS-Daten eindeutig auf DNS-Profile beschränkt wird. In Anhang II werden DNS-Profile durch eine erste gemeinsame Liste von DNS-Markern definiert, die in kriminaltechnischen DNS-Analysen in den Mitgliedstaaten genutzt werden. Durch diese Liste, die auf den sieben DNS-Markern des Europäischen Standardsatzes basiert, wie er in Anhang I der Entschließung des Rates vom 25. Juni 2001 über den Austausch von DNS-Analyseergebnissen definiert ist [1], wird sichergestellt, dass aus DNS-Proben gewonnene DNS-Profile keine Informationen über spezifisches Erbgut enthalten.

60. Der Europäische Datenschutzbeauftragte betont, dass diese Entschließung des Rates einige sehr wichtige Garantien enthält, die speziell auf die dynamische Natur von DNS-Profilen abstellen. In Abschnitt III der Entschließung wird der Austausch von DNS-Analyseergebnissen nämlich auf „Chromosomenbereiche […] beschränkt, von denen nicht bekannt ist, dass sie Informationen über bestimmte Erbmerkmale enthalten"; außerdem wird den Mitgliedstaaten hier empfohlen, nicht länger DNS-Marker zu verwenden, die bei entsprechenden Entwicklungen in der Wissenschaft die Feststellung bestimmter Erbmerkmale ermöglichen könnten.

61. Im Vertrag von Prüm ist ein anderes Konzept vorgesehen, da dieser Vertrag die Vertragsparteien verpflichtet, zum Zwecke der Verfolgung von Straftaten nationale DNS-Analyse-Dateien zu errichten und zu führen. Dieser Vertrag bewirkt somit die Einrichtung neuer DNS-Datenbanken sowie eine Zunahme von DNS-Daten-Erhebungen. Ferner ist nicht klar, welche Art von Daten von den DNS-Analyse-Dateien erfasst werden sollen. Auch wird die dynamische Entwicklung von DNS-Profilen im Vertrag nicht berücksichtigt.

62. Der Europäische Datenschutzbeauftragte weist darauf hin, dass jeder Rechtsakt über den Austausch von DNS-Daten folgenden Anforderungen entsprechen sollte:

— Die Art von DNS-Informationen, die ausgetauscht werden dürfen, sollte präzise begrenzt und eindeutig definiert werden (auch unter Berücksichtigung des wesentlichen Unterschieds zwischen DNS-Proben und DNS-Profilen).

— Es sollten gemeinsame technische Standards vorgesehen werden, um zu vermeiden, dass praktische Unterschiede zwischen den kriminaltechnischen DNS-Datenbanken in den Mitgliedstaaten beim Austausch der Daten zu Schwierigkeiten und ungenauen Ergebnissen führen.

— Es sollten angemessene rechtsverbindliche Garantien vorgesehen werden, um zu verhindern, dass im Zuge des wissenschaftlichen Fortschritts aus den DNS-Profilen personenbezogene Daten gewonnen werden können, bei denen es sich zum einen um sensible Daten und zum anderen um Daten handelt, die für die Zwecke, für die sie erhoben wurden, nicht erforderlich sind.

63. In diesem Zusammenhang bestätigt und übernimmt der Europäische Datenschutzbeauftragte die von ihm in der Stellungnahme zum Rahmenbeschluss über den Schutz personenbezogener Daten bereits formulierten Bemerkungen (Nummer 80). In der genannten Stellungnahme hatte der Datenschutzbeauftragte in Bezug auf DNS-Daten darauf hingewiesen, dass spezifische Garantien vorzusehen sind, um sicherzustellen, dass die verfügbaren Informationen ausschließlich zur Identifizierung von Personen zum Zwecke der Verhütung, Aufdeckung oder Untersuchung von Straftaten genutzt werden, dass die sachliche Richtigkeit von DNS-Profilen gebührend berücksichtigt wird und von dem Betroffenen anhand leicht zugänglicher Mittel angefochten werden kann, und dass die Wahrung der Würde der Person in jeder Hinsicht gewährleistet ist [2].

64. Aus diesen Erwägungen ergibt sich ferner, dass die Rechtsvorschriften über die Errichtung von DNS-Dateien und den Austausch von Daten aus diesen Dateien erst nach Durchführung einer Folgenabschätzung angenommen werden sollten, in der die Vorteile und die Risiken angemessen bewertet werden konnten. Der Europäische Datenschutzbeauftragte empfiehlt, in diese Rechtsvorschriften die Verpflichtung aufzunehmen, dass sie nach ihrem Inkrafttreten regelmäßig bewertet werden müssen.

65. Schließlich können nach Anhang II noch andere Arten von Informationen ausgetauscht werden. Der Anhang umfasst Informationen von privaten Einrichtungen (Telefonnummern und sonstige Verbindungsdaten sowie Verkehrsdaten stammen in der Regel von Telefonbetreibern). In der Begründung wird bestätigt, dass die Mitgliedstaaten sicherstellen müssen, dass strafverfolgungsrelevante Informationen, die im Besitz von hierzu ermächtigten Behörden oder privaten Einrichtungen verwaltet sind, von gleichwertigen zuständigen Behörden anderer Mitgliedstaaten und von Europol mit genutzt werden können. Da der Vorschlag für personenbezogene Daten von privaten Einrichtungen gilt, sollte der geltende Rechtsrahmen nach Auffassung des Datenschutzbeauftragten zusätzliche Garantien enthalten, um die Richtigkeit der Daten zu gewährleisten und somit das Datensubjekt zu schützen.

VII. **DATENSCHUTZGRUNDSÄTZE**

66. Der vorgeschlagene Rahmenbeschluss enthält keine speziellen Regeln für den Schutz personenbezogener Daten, während in anderen Instrumenten wie dem Vertrag von Prüm oder dem schwedischen Vorschlag durchaus einige spezifische Bestimmungen über den Schutz personenbezogener Daten vorgesehen sind. Die Tatsache, dass im Vorschlag über die Verfügbarkeit keine speziellen Bestimmungen über den Schutz personenbezogener Daten enthalten sind, ist nur insoweit akzeptabel, als die generellen Regeln, die im Vorschlag für einen Rahmenbeschluss über den Datenschutz im Rahmen der dritten Säule enthalten sind, uneingeschränkt Anwendung finden und ausreichenden Schutz bieten. Im Übrigen sollten Datenschutzregeln, die in spezifischen Instrumenten wie dem schwedischen Vorschlag oder dem Vertrag von Prüm niedergelegt sind, das durch den generellen Rahmen gewährleistete Schutzniveau nicht absenken. Der Datenschutzbeauftragte empfiehlt, eine spezielle Kollisionsnorm über die Anwendbarkeit von verschiedenen Datenschutzregeln aufzunehmen.

[1] ABl. C 187, S.1.

[2] Siehe hierzu auch das Dokument des Europarats „Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data" (Fortschrittsbericht über die Anwendung der Grundsätze des Übereinkommens 108 auf die Erfassung und Verarbeitung biometrischer Daten), Europarat, 2005.

67. Unter Bezugnahme auf seine Stellungnahme zum Rahmenbeschluss über den Schutz personenbezogener Daten möchte der Europäische Datenschutzbeauftragte an dieser Stelle erneut betonen, wie wichtig es ist, über kohärente und umfassende Datenschutzregeln für die Zusammenarbeit bei der Strafverfolgung zu verfügen, die für alle Verarbeitungsvorgänge gelten. Ferner bekräftigt er die anderen in der genannten Stellungnahme formulierten Argumente. In dieser Nummer werden die nachstehenden Datenschutzaspekte hervorgehoben:

— Rechtmäßige Verarbeitung personenbezogener Daten: Der Datenschutzbeauftragte unterstützt das Konzept, wonach Informationen nur zur Verfügung gestellt werden dürfen, wenn sie rechtmäßig erhoben worden sind (wie in Artikel 2 Absatz 2 in Bezug auf die unter Einsatz von Zwangsmaßnahmen erlangten Informationen vorgesehen ist). Durch eine rechtmäßige Verarbeitung personenbezogener Daten wäre ferner gewährleistet, dass zur Verfügung gestellte und ausgetauschte Informationen auch in Gerichtsverfahren ordnungsgemäß genutzt werden können. Obwohl nach der Einleitung eines Strafverfahrens verarbeitete Informationen vom Anwendungsbereich des vorgeschlagenen Rechtsakts ausgenommen sind, dürften nämlich vorher durch die Strafverfolgungsbehörden ausgetauschte Informationen höchstwahrscheinlich letztendlich wohl doch in Gerichtsverfahren Verwendung finden.

— Von besonderer Bedeutung ist die Qualität personenbezogener Daten, da der Verfügbarkeitsgrundsatz bewirkt, dass Informationen von Strafverfolgungsbehörden genutzt werden, die außerhalb des Umfeldes tätig sind, in dem diese Daten erhoben wurden. Diese Behörden haben sogar unmittelbaren Zugang zu den Datenbanken anderer Mitgliedstaaten. Die Qualität der personenbezogenen Daten kann nur gewährleistet werden, wenn ihre Richtigkeit regelmäßig und sorgfältig überprüft wird, wenn zwischen den Informationen je nach Kategorie der Personen, auf die sie sich beziehen, unterschieden wird (Opfer, Verdächtige, Zeugen usw.) und wenn, erforderlichenfalls, der Grad der sachlichen Richtigkeit angegeben wird (siehe Stellungnahme des Europäischen Datenschutzbeauftragten zum Schutz personenbezogener Daten, IV.6).

  Diese Punkte machen erneut deutlich, aus welchen Gründen Datenschutzregeln und insbesondere Regeln über die Richtigkeit für alle Formen der Verarbeitung, auch für die innerstaatliche Datenverarbeitung, gelten sollten. Ohne solche Regeln könnten personenbezogene Daten, auf die unmittelbar zugegriffen werden kann, unrichtig oder überholt sein und damit sowohl die Rechte des Datensubjekts verletzen als auch die Wirksamkeit der Untersuchungen beeinträchtigen.

— Eingrenzung des Verwendungszwecks: Nach dem Verfügbarkeitsgrundsatz haben gleichwertige Behörden anderer Mitgliedstaaten Zugriff auf personenbezogene Daten. Die Kompetenzen der Strafverfolgungsbehörden können jedoch von Land zu Land sehr unterschiedlich sein. Es muss daher unbedingt sichergestellt werden, dass das grundlegende Prinzip der Eingrenzung des Verwendungszwecks ungeachtet des unterschiedlichen Umfangs der Kompetenzen der einzelnen zuständigen Behörden, die Daten austauschen, eingehalten wird. Informationen, die von einer bestimmten Behörde für einen bestimmten Zweck erhoben und verarbeitet werden, können allein aufgrund der Tatsache, dass die Empfängerbehörde andere, vielleicht weiter reichende Kompetenzen hat, nicht für einen anderen Zweck genutzt werden.

  Daher begrüßt der Europäische Datenschutzbeauftragte Artikel 7 des vorgeschlagenen Rahmenbeschlusses, der als Spezifizierung der allgemeinen Regeln ausgelegt werden sollte, die im vorgeschlagenen Rahmenbeschluss über den Schutz personenbezogener Daten enthalten sind. Ferner weist der Datenschutzbeauftragte darauf hin, dass die Bewertung der Gleichwertigkeit der einzelnen Behörden (die nach dem vorliegenden Vorschlag im Wege des Regelungsverfahrens erfolgt) sorgfältig und unter gebührender Berücksichtigung des Grundsatzes der Eingrenzung des Verwendungszwecks durchgeführt werden sollte.

— Auch bei den Fristen für die Speicherung ausgetauschter Informationen ist der Grundsatz der Einschränkung des Verwendungszwecks zu berücksichtigen: Für einen Zweck abgerufene oder ausgetauschte Informationen sollten gelöscht werden, wenn sie für diesen Zweck nicht länger erforderlich sind. Dadurch ließe sich vermeiden, dass Datenbanken unnötig vervielfältigt werden, wobei die zuständigen Behörden die verfügbaren (aktualisierten) Informationen jedoch erneut abrufen könnten, falls dies für einen anderen legitimen Zweck erforderlich ist.

— Protokollierung der nach dem Verfügbarkeitsgrundsatz übermittelten Informationen: Die Protokollierung sollte auf beiden Seiten erfolgen, nämlich im ersuchten und im ersuchenden Mitgliedstaat. Nicht nur der Austausch, sondern auch der Zugang zu den Daten sollte protokolliert werden (siehe Stellungnahme des Europäischen Datenschutzbeauftragten zum Schutz personenbezogener Daten, Nummer 133), auch um sicherzustellen, dass die nationalen zuständigen Behörden sich gegenseitig vertrauen und nicht ganz die Kontrolle über die verfügbaren Informationen verlieren. Die Notwendigkeit der Rückverfolgbarkeit von Informationen beinhaltet auch, dass es möglich sein muss, Informationen zu aktualisieren und/oder zu berichtigen.

— Rechte der Datensubjekte: Durch die Einrichtung von Systemen für den Austausch von Informationen zwischen den EU-Strafverfolgungsbehörden kommt es häufiger zu Situationen, in denen personenbezogene Daten (vorübergehend) gleichzeitig von den zuständigen Behörden in unterschiedlichen Mitgliedstaaten verarbeitet werden. Dies bedeutet zum einen, dass gemeinsame EU-Normen zu den Rechten der Datensubjekte erarbeitet werden sollten, und zum anderen, dass die Datensubjekte in dem nach den Datenschutzregeln der dritten Säule zulässigen Maße in der Lage sein sollten, ihre Rechte sowohl in Bezug auf Behörden, die Daten zur Verfügung stellen, als auch in Bezug auf Behörden, die diese Daten abfragen und verarbeiten, wahrzunehmen.

— Überwachung: Der Europäische Datenschutzbeauftragte weist darauf hin, dass im Einzelfall mehr als eine nationale Behörde dafür zuständig sein kann, die im Rahmen der vorliegenden Vorschläge erfolgende Verarbeitung personenbezogener Daten zu überwachen. In diesem Zusammenhang erfordert der unmittelbare Online-Zugang zu strafverfolgungsrelevanten Informationen eine verstärkte Überwachung und Koordinierung durch die einschlägigen nationalen Datenschutzbehörden.

VIII. **FAZIT**

Allgemeine Schlussfolgerungen in Bezug auf den Verfügbarkeitsgrundsatz

68. Der Europäische Datenschutzbeauftragte möchte in dieser Stellungnahme einige generelle und grundlegendere Standpunkte zum Thema Austausch von strafverfolgungsrelevanten Informationen und zu den Konzepten zur Regelung dieses Themas formulieren. Er steht für weitere Konsultationen in einer späteren Phase gern zur Verfügung, wenn das Gesetzgebungsverfahren für diesen Vorschlag sowie für andere damit zusammenhängende Vorschläge vorangekommen ist.

69. Nach Auffassung des Europäischen Datenschutzbeauftragten sollte der Verfügbarkeitsgrundsatz in ein rechtsverbindliches Instrument umgesetzt werden, dem ein vorsichtigeres graduelles Konzept zugrunde liegt, das nur auf einen Datentyp abstellt. Im Rahmen dieses Konzepts wäre zu prüfen, inwieweit der Verfügbarkeitsgrundsatz eine wirksame Hilfe bei der Strafverfolgung sein kann und welches die speziellen Risiken für den Schutz personenbezogener Daten sind. Dieser vorsichtigere Ansatz könnte auch beinhalten, dass mit der Umsetzung des Verfügbarkeitsgrundsatzes nur im Wege des mittelbaren Zugangs anhand von Indexdaten begonnen wird. Zur Steigerung der Effizienz könnte das System auf der Grundlage dieser Erfahrungen gegebenenfalls auf andere Datentypen ausgeweitet und/oder angepasst werden.

70. Rechtsakte zur Umsetzung des Verfügbarkeitsgrundsatzes sollten nicht angenommen werden, bevor nicht wesentliche datenschutzrechtliche Garantien, wie sie im Rahmenbeschluss über den Schutz personenbezogener Daten enthalten sind, vorgesehen sind.

Empfehlungen zur Änderung des vorliegenden Vorschlags

71. Der Europäische Datenschutzbeauftragte empfiehlt, den Anwendungsbereich des Verfügbarkeitsgrundsatzes wie folgt zu präzisieren:

— Es muss einee klare und genaue Definition der als „verfügbar“ betrachteten Daten aufgenommen werden.

— Eine erste Option besteht darin, den Anwendungsbereich des Verfügbarkeitsgrundsatzes auf Informationen zu beschränken, die im Besitz der von zuständigen Behörden sind.

— Eine zweite Option besteht darin, im Falle eines breiteren Anwendungsbereichs ausreichende Garantien für den Schutz personenbezogener Daten vorzusehen. Die in Nummer 27 aufgeworfenen Fragen müssen berücksichtigt werden.

72. Zum unmittelbaren Zugang durch eine zuständige Behörde eines anderen Mitgliedstaates formuliert der Europäische Datenschutzbeauftragte die nachstehenden Bemerkungen:

— Die Frage muss angemessen geregelt werden, denn im Falle des unmittelbaren Zugangs haben die zuständigen Behörden des Mitgliedstaates, aus dem die Daten stammen, keine Kontrolle über den Zugriff auf die Daten und auf deren weitere Nutzung.

— Der Vorschlag darf nicht dazu führen, dass es zu einer mit keinerlei Auflagen verbundenen Verknüpfung von Datenbanken kommt, weil es schwierig wäre, ein Netz von Datenbanken zu überwachen.

73. Der Rahmenbeschluss sollte die Errichtung eines Systems von Indexdaten präziser regeln. Dabei ist insbesondere Folgendes zu berücksichtigen:

— Der Vorschlag sollte angemessene Regeln enthalten, zumindest für die Erzeugung von Indexdaten, die Verwaltung der Dateien von Indexdaten und die angemessene Organisation des Zugangs zu diesen Indexdaten.

— Die Definition von Indexdaten muss präzisiert werden.

— Im Vorschlag sollte klargestellt werden, welches die Rolle der nationalen Kontaktstellen in Bezug auf Indexdaten ist.

— Die Grundregeln für die Erzeugung von Indexdaten sollten in den Rahmenbeschluss selbst aufgenommen und nicht im Wege des Regelungsverfahrens in den Durchführungsbestimmungen festgelegt werden.

74. Der Europäische Datenschutzbeauftragte weist darauf hin, dass der Vorschlag — soweit darin der Austausch von DNS-Daten vorgesehen ist — folgende Aspekte regeln sollte:

— Die Art von DNS-Informationen, die ausgetauscht werden dürfen, sollte deutlich begrenzt und definiert werden (auch unter Berücksichtigung des wesentlichen Unterschieds zwischen DNS-Proben und DNS-Profilen).

— Es sollten gemeinsame technische Standards vorgesehen werden, um zu vermeiden, dass praktische Unterschiede zwischen den kriminaltechnischen DNS-Datenbanken in den Mitgliedstaaten beim Austausch der Daten zu Schwierigkeiten und ungenauen Ergebnissen führen.

— Es sollten angemessene rechtsverbindliche Garantien vorgesehen werden, um zu verhindern, dass im Zuge des wissenschaftlichen Fortschritts aus DNS-Profilen personenbezogene Daten gewonnen werden können, bei denen es sich zum einen um sensible Daten und zum anderen um Daten handelt, die für die Zwecke, für die sie erhoben wurden, nicht erforderlich sind.

— Die Annahme sollte nicht ohne vorherige Folgenabschätzung erfolgen.

75. Der Europäische Datenschutzbeauftragte empfiehlt, den Informationsaustausch mit Europol auf die von Europol selbst verfolgten Zwecke, die in Artikel 2 des Europol-Übereinkommens und dem dazugehörigen Anhang aufgeführt sind, zu beschränken.

Geschehen zu Brüssel am 28. Februar 2006

Peter HUSTINX

Europäischer Datenschutzbeauftragter