Ministerium für Justiz,
Arbeit und Europa
des Landes Schleswig-Holstein

Ministerium für Justiz, Arbeit und Europa
des Landes Schleswig-Holstein | Postfach 71 45 | 24171 Kiel

An den
Vorsitzenden des
Innen- und Rechtsausschusses des
Schleswig-Holsteinischen Landtages
Herrn Werner Kalinka, MdL
Landeshaus
24105 Kiel

Ihr Zeichen:
Ihre Nachricht vom:
Mein Zeichen: II 321 / 9324-31
Meine Nachricht vom:
Dr. Kai Hamdorf
Telefon: 0431 988-3860
Telefax: 0431 988-3881

Schleswig-Holsteinischer Landtag
Umdruck 16/3195

28. Mai 2008

Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken; Sachstandsbericht

Sehr geehrter Herr Vorsitzender,

gerne komme ich der in der Sitzung vom 21. Mai 2008 geäußerten Bitte des Innen- und Rechtsausschusses nach einer schriftlichen Information über den aktuellen Stand im Zusammenhang mit dem Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen zu Strafverfolgungszwecken nach.

Über die überwiegend kritischen Empfehlungen der Bundesratsausschüsse und die Haltung des Kabinetts zu der Strichdrucksache 826/1/07 hatte ich bereits berichtet. Den anschließend ergangenen Beschluss des Bundesrates vom 15. Februar 2008, BR-Drs. 826/07 (Beschluss) füge ich diesem Schreiben bei.

Der Rahmenbeschlussvorschlag wird derzeit im Rat der Europäischen Union in der „Multidisziplinäre[n] Arbeitsgruppe Organisierte Kriminalität" verhandelt. Die Arbeitsgruppe hat – soweit mir bekannt – den Vorschlag bislang viermal behandelt, und zwar in ihren Sitzungen am 4. Februar, am 25. und 26. März, am 14. und 15. April sowie am 24., 25. und 28. April 2008.

Inzwischen liegt auch eine Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Rahmenbeschluss vor. Die am 1. Mai 2008 im Amtsblatt der Europäischen Union veröffentlichte Stellungnahme füge ich diesem Schreiben bei.

Mit freundlichen Grüßen

Uwe Döring
Minister

I

(Entschließungen, Empfehlungen und Stellungnahmen)

STELLUNGNAHMEN

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten (EDSB) zu dem Entwurf eines Vorschlags für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken

(2008/C 110/01)

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 [1],

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr [2], insbesondere auf Artikel 41,

gestützt auf das am 13. November 2007 eingegangene Ersuchen der Europäischen Kommission um Stellungnahme nach Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001.

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN

I. EINLEITUNG

Konsultation des EDSB

1. Der Entwurf eines Vorschlags für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken (nachstehend „der Vorschlag" genannt) wurde dem EDSB von der Kommission zwecks Konsultation gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 übermittelt.

2. Der Vorschlag betrifft die Verarbeitung von PNR-Daten innerhalb der EU und steht in engem Zusammenhang mit anderen Regelungen für die Erhebung und Nutzung von Fluggastdaten, insbesondere dem Abkommen zwischen der EU und den USA vom Juli 2007. Diese Regelungen sind von großem Interesse für den EDSB, der bereits Gelegenheit hatte, einige erste Bemerkungen zu dem Fragebogen der Kommission zu dem vorgesehenen PNR-System der EU, der im Dezember 2006 an die Beteiligten [3] gesandt wurde, zu übermitteln. Der EDSB begrüßt die Anhörung seitens der Kommission. Nach Auffassung des EDSB sollte in der Präambel des Ratsbeschlusses auf die vorliegende Stellungnahme verwiesen werden.

Hintergrund des Vorschlags

3. Der Vorschlag bezweckt die Harmonisierung der Vorschriften der Mitgliedstaaten über die Pflichten der Fluggesellschaften, die Flüge aus mindestens einem oder in mindestens einen Mitgliedstaat durchführen, soweit sie die Übermittlung von PNR-Daten an die zuständigen Behörden zum Zwecke der Verhütung und Bekämpfung von terroristischen Straftaten und organisierter Kriminalität betreffen.

4. Die Europäische Union hat mit den USA sowie mit Kanada Vereinbarungen über die Übermittlung von PNR-Daten für vergleichbare Zwecke getroffen. Das erste Abkommen mit den USA vom Mai 2004 wurde im Juli 2007 durch ein

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 8 vom 12.1.2001, S. 1.
[3] Unter anderem Mitgliedstaaten, Datenschutzbehörden und Vereinigungen von Fluggesellschaften. Die Kommission hatte den Fragebogen im Hinblick auf die Ausarbeitung der Folgenabschätzung zu ihrem Vorschlag erstellt.

neues Abkommen ([1]) ersetzt. Ein ähnliches Abkommen wurde im Juli 2005 mit Kanada geschlossen ([2]). Ferner sollen demnächst Verhandlungen zwischen der EU und Australien über ein Abkommen über den Austausch von PNR-Daten aufgenommen werden; auch Südkorea fordert die Übermittlung von PNR-Daten für Flüge in sein Hoheitsgebiet, doch sind derzeit keine Verhandlungen auf europäischer Ebene mit diesem Land vorgesehen.

5. Innerhalb der EU bildet der Vorschlag eine Ergänzung zu der Richtlinie 2004/82/EG des Rates ([3]) über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen, so genannte erweiterte Fluggastdaten, zu übermitteln, um die illegale Einwanderung zu bekämpfen und die Grenzkontrollen zu verbessern. Diese Richtlinie hätte spätestens am 5. September 2006 in das nationale Recht der Mitgliedstaaten umgesetzt werden müssen. Die Umsetzung ist jedoch noch nicht in allen Mitgliedstaaten erfolgt.

6. Im Gegensatz zu den erweiterten Fluggastdaten (API-Daten), die zur Identifizierung von Personen beitragen sollen, würden die in dem Vorschlag genannten PNR-Daten dazu beitragen, Risikoanalysen in Bezug auf Personen vorzunehmen, neue Erkenntnisse zu sammeln und Verbindungen zwischen bekannten und unbekannten Personen herzustellen.

7. Der Vorschlag hat folgende Hauptbestandteile:

   — er ermöglicht die Weitergabe von PNR-Daten durch Fluggesellschaften an die zuständigen Behörden der Mitgliedstaaten zum Zwecke der Verhütung und Bekämpfung terroristischer Straftaten und organisierter Kriminalität,

   — er sieht vor, dass grundsätzlich in jedem Mitgliedstaat eine PNR-Zentralstelle benannt wird, die die Aufgabe hat, bei Fluggesellschaften (oder benannten Datenmittlern) die PNR-Daten zu erheben und Risikoanalysen in Bezug auf Fluggäste durchzuführen,

   — die entsprechend ausgewerteten Informationen werden den zuständigen Behörden in jedem Mitgliedstaat übermittelt. Diese Informationen werden mit anderen Mitgliedstaaten auf Einzelfallbasis für den vorstehend genannten Zweck ausgetauscht,

   — die Weitergabe von Daten an Staaten außerhalb der Europäischen Union ist an zusätzliche Bedingungen geknüpft,

   — die Daten werden insgesamt 13 Jahre auf Vorrat gespeichert, davon acht Jahre in einer ruhenden Datenbank,

   — die Verarbeitung soll gemäß dem (im Entwurfsstadium befindlichen) Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (nachstehend „Datenschutz-Rahmenbeschluss“) ([4]), erfolgen,

   — ein Ausschuss mit Vertretern der Mitgliedstaaten soll die Kommission in Protokoll- und Verschlüsselungsangelegenheiten sowie hinsichtlich der Kriterien und Verfahren für Risikoanalysen unterstützen,

   — der Beschluss soll innerhalb von drei Jahren nach seinem Inkrafttreten überprüft werden.

Schwerpunkt der Stellungnahme

8. Der Vorschlag, zu dem der EDSB konsultiert wird, ist ein weiterer Schritt auf dem Weg zu einer routinemäßigen Erhebung der Daten von Personen, die im Grunde keiner Straftat verdächtigt werden. Wie bereits erwähnt, vollzieht sich diese Entwicklung sowohl weltweit als auch auf europäischer Ebene.

9. Der EDSB stellt fest, dass auch die Datenschutzgruppe und die Gruppe „Polizei und Justiz“ eine gemeinsame Stellungnahme zu dem Vorschlag vorgelegt haben ([5]). Der EDSB unterstützt jene Stellungnahme. In der vorliegenden Stellungnahme werden einige zusätzliche Punkte in den Vordergrund gerückt und näher ausgeführt.

10. Obschon in der Stellungnahme des EDSB alle relevanten Aspekte des Vorschlags untersucht werden, liegt ihr Schwerpunkt auf den folgenden vier Hauptfragen:

    — Die erste Hauptfrage betrifft die Rechtmäßigkeit der beabsichtigten Maßnahmen. Die Frage des Zwecks, der Notwendigkeit und der Verhältnismäßigkeit des Vorschlags wird anhand der Kriterien des Artikels 8 der Charta der Grundrechte der Europäischen Union beurteilt.

    — In der Stellungnahme wird ferner die Frage untersucht, welches Recht auf die vorgeschlagene Verarbeitung anwendbar ist. Besondere Aufmerksamkeit verdient der Zusammenhang zwischen dem Geltungsbereich des Datenschutz-Rahmenbeschlusses und der Anwendung der Datenschutzvorschriften der ersten Säule. Die Auswirkungen der geltenden Datenschutzregelung hinsichtlich der Wahrnehmung der Rechte der betroffenen Person werden ebenfalls geprüft.

([1]) Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records — PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS) (PNR-Abkommen von 2007) (ABl. L 204 vom 4.8.2007, S. 18).

([2]) Abkommen zwischen der Europäischen Gemeinschaft und der Regierung Kanadas über die Verarbeitung von erweiterten Fluggastdaten und Fluggastdatensätzen (ABl. L 82 vom 21.3.2006, S. 15).

([3]) Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln (ABl. L 261 vom 6.8.2004, S. 24).

([4]) Die letzte Fassung des betreffenden Entwurfs ist beim Rat unter der Nummer 16397/07 registriert.

([5]) Gemeinsame Stellungnahme zu dem von der Kommission am 6. November 2007 vorgelegten Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken, die von der Datenschutzgruppe am 5. Dezember 2007 und von der Gruppe „Polizei und Justiz“ am 18. Dezember 2007 angenommen wurde (WP 145, WPPJ 01/07).

— In der Stellungnahme wird anschließend gezielt auf die Eigenschaft der Datenempfänger auf nationaler Ebene eingegangen. Insbesondere die Eigenschaft der PNR-Zentralstellen, der Datenmittler und der zuständigen Behörden, die benannt werden, um Risikoanalysen durchzuführen und Fluggastdaten auszuwerten, wirft spezifische Bedenken auf, da der Vorschlag diesbezüglich keine genauen Festlegungen enthält.

— Die vierte Hauptfrage betrifft die Bedingungen für die Weitergabe von Daten an Drittstaaten. Es ist nicht klar, welche Bedingungen für diese Weitergaben gelten werden, wenn verschiedene Regelungen bestehen: die Weitergabe-Bedingungen gemäß dem Vorschlag, zusammen mit denen des Datenschutz-Rahmenbeschlusses, und die der bestehenden internationalen Abkommen (mit den USA und mit Kanada).

11. Weitere wichtige Punkte werden im letzten Teil angesprochen, darunter positive Schritte beim Datenschutz, jedoch auch solche Aspekte des Vorschlags, die zusätzliche Bedenken hervorrufen.

II. RECHTMÄSSIGKEIT DER VORGESCHLAGENEN MASSNAHMEN

12. Zur Untersuchung der Rechtmäßigkeit der vorgeschlagenen Maßnahmen gemäß den grundlegenden Datenschutzprinzipien, insbesondere gemäß Artikel 8 der EU-Grundrechtecharta und gemäß den Artikeln 5 bis 8 des Übereinkommens Nr. 108 des Europarates ([1]), ist es erforderlich, den Zweck der beabsichtigten Verarbeitung personenbezogener Daten eindeutig zu ermitteln sowie die Notwendigkeit und Verhältnismäßigkeit dieser Verarbeitung zu beurteilen. Es sollte gewährleistet sein, dass zum Erreichen des beabsichtigten Zwecks kein anderes Mittel zur Verfügung steht, das einen geringeren Eingriff bewirkt.

Ermittlung des Zwecks

13. Der Text des Vorschlags und die dazugehörige Folgenabschätzung lassen erkennen, dass das Ziel nicht lediglich darin besteht, bekannte Terroristen oder bekannte Straftäter, die an der organisierten Kriminalität beteiligt sind, durch Abgleich ihrer Namen mit den von den Strafverfolgungsbehörden geführten Daten ausfindig zu machen. Der Zweck besteht darin, Erkenntnisse über den Terrorismus und die organisierte Kriminalität zusammenzutragen, und ganz konkret „Risikoanalysen in Bezug auf Personen vorzunehmen, neue Erkenntnisse zu sammeln und Verbindungen zwischen bekannten und unbekannten Personen herzustellen“ ([2]). Der in Artikel 3 Absatz 5 des Vorschlags genannte Zweck besteht dementsprechend vorrangig in der „Identifizierung von Personen *und deren Komplizen*, die an einer terroristischen oder der organisierten Kriminalität zugerechneten Straftat beteiligt sind *oder sein könnten*“.

14. Dieser Grund wird als Erläuterung dafür angeführt, dass API-Daten für das Erreichen des genannten Zwecks nicht ausreichen. Während die API-Daten — wie bereits erwähnt — zur Identifizierung von Personen beitragen sollen, wird mit den PNR-Daten keine Identifizierung bezweckt; vielmehr würden die PNR-Daten dazu beitragen, Risikoanalysen in Bezug auf Personen vorzunehmen, neue Erkenntnisse zu sammeln und Verbindungen zwischen bekannten und unbekannten Personen herzustellen.

15. Der Zweck der vorgesehenen Maßnahmen erstreckt sich nicht nur auf die Ergreifung von *bekannten* Personen, sondern auch auf das Ausfindigmachen von Personen, die den Kriterien des Vorschlags entsprechen *könnten*.

Die Identifizierung dieser Personen soll insbesondere anhand von Risikoanalysen und durch Feststellung von Verhaltensmustern erfolgen. In Erwägungsgrund 9 des Vorschlags ist explizit dargelegt, dass die Daten „lange genug aufbewahrt werden müssen, damit sie für die Entwicklung von Risikoindikatoren und die Feststellung von Reise- und Verhaltensmustern verwendet werden können“.

16. Die Zweckbeschreibung umfasst somit zwei Ebenen: Die erste Ebene besteht in dem Gesamtziel der Bekämpfung von Terrorismus und organisierter Kriminalität, während die zweite Ebene die Mittel und Maßnahmen zur Verwirklichung dieses Ziels umfasst. Während der Zweck der Bekämpfung von Terrorismus und organisierter Kriminalität ausreichend deutlich und rechtmäßig zu sein scheint, besteht hinsichtlich der zum Erreichen dieses Zwecks vorgesehenen Mittel Raum für Diskussionen.

Erstellung von Verhaltensmustern und Risikoanalysen

17. Aus dem Vorschlag wird nicht deutlich, wie Verhaltensmuster erstellt und Risikoanalysen durchgeführt werden sollen. Die Folgenabschätzung enthält folgende Angaben zur Art der Verwendung von PNR-Daten: Abgleich der Fluggastdaten „mit einer Reihe von Merkmalen und Verhaltensmustern zwecks Erstellung eines Risikoprofils. Wenn ein Flugreisender in ein bestimmtes Risikoprofil passt, kann er als Passagier mit hohem Gefahrenpotenzial eingestuft werden“ ([3]).

18. Verdächtige könnten sowohl anhand konkreter Verdachtsmomente in ihren PNR-Daten (z. B. Kontakte zu einem verdächtigen Reisebüro, Nummer einer gestohlenen Kreditkarte) als auch aufgrund von „Verhaltensmustern“ oder einem abstrakten Profil herausgefiltert werden. Aufgrund von Reisemustern könnten verschiedene Standardprofile für „normale“ bzw. „verdächtige“ Fluggäste erstellt werden. Diese Profile würden weitere Ermittlungen hinsichtlich der Fluggäste ermöglichen, die nicht unter die „Kategorie der normalen Fluggäste“ fallen, zumal denn, wenn ihr Profil mit anderen Verdachtsmomenten wie etwa einer gestohlenen Kreditkarte behaftet ist.

19. Auch wenn nicht davon ausgegangen werden kann, dass Fluggäste aufgrund ihrer Religionszugehörigkeit oder anderer sensibler Daten herausgefiltert werden, so hat es dennoch den Anschein, dass sie Gegenstand von Ermittlungen würden, die auf einer Mischung aus *konkreten* und *abstrakten* Informationen — *einschließlich* Standardverhaltensmustern und abstrakter Profile — beruhen.

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

([2]) Abschnitt 1 der Begründung des Vorschlags.

([3]) Folgenabschätzung Abschnitt 2.1 („Description of the problem“).

20. Es lässt sich darüber diskutieren, ob derartige Ermittlungen als „Profiling" betrachtet werden können. Das Profiling wäre ein „rechnergestütztes Verfahren, bei dem ein Datenlager (*data warehouse*) nach Daten abgesucht wird (‚Datenschürfung', *data mining*), um eine Person mit einiger Wahrscheinlichkeit — und folglich mit einer gewissen Fehlerquote — in eine bestimmte Kategorie einzustufen bzw. einstufen zu können und daraufhin bestimmte Einzelentscheidungen in Bezug auf diese Person zu treffen" ([1]).

21. Dem EDSB ist bekannt, dass die Definition des Begriffs „Profiling" Gegenstand von Erörterungen ist, die noch nicht abgeschlossen sind. Unabhängig von der Frage, ob offiziell anerkannt wird, dass der Vorschlag auf das *Profiling* von Fluggästen abzielt, betrifft die Kernfrage, um die es hier geht, nicht die Definition von Begriffen. Sie betrifft vielmehr die Auswirkungen auf Einzelpersonen.

22. Das Hauptbedenken des EDSB ist damit verknüpft, dass Entscheidungen in Bezug auf Einzelpersonen aufgrund von Verhaltensmustern und Kriterien getroffen werden, deren Festlegung anhand der Daten von Fluggästen im Allgemeinen erfolgt. Folglich könnten Entscheidungen über eine bestimmte Person getroffen werden, indem (zumindest teilweise) Verhaltensmuster verwendet werden, die aus den Daten *anderer* Personen abgeleitet wurden. Dies bedeutet, dass Entscheidungen, die erhebliche Auswirkungen auf die Betroffenen haben können, in einem abstrakten Zusammenhang getroffen werden. Es ist für die Betroffenen äußerst schwierig, sich gegen derartige Entscheidungen zur Wehr zu setzen.

23. Außerdem soll die Risikoanalyse ohne einheitliche Standards für die Identifizierung von Verdächtigen durchgeführt werden. Der EDSB stellt die Rechtssicherheit des gesamten Filterprozesses ernsthaft in Frage, weil die Kriterien, anhand deren jeder Fluggast gescannt wird, sehr unzulänglich definiert sind.

24. Der EDSB verweist auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte, wonach das innerstaatliche Recht so präzise sein muss, dass der Bürger weiß, unter welchen Umständen und Bedingungen die Behörden befugt sind, Daten über sein Privatleben zu archivieren und zu nutzen. Die Daten sollten dem Betroffenen zugänglich und in ihren Auswirkungen vorhersehbar sein. Eine Vorschrift ist vorhersehbar, wenn sie so präzise formuliert ist, dass jeder Einzelne — gegebenenfalls mit entsprechender Beratung — sein Verhalten danach einrichten kann ([2]).

25. Abschließend sei gesagt, dass der Vorschlag vor allem wegen dieser Arten von Risiken einer sorgfältigen Prüfung bedarf. Zwar ist der allgemeine Zweck der Bekämpfung von Terrorismus und organisierter Kriminalität als solcher deutlich und rechtmäßig, doch scheinen die Kernbestandteile der vorgesehenen Verarbeitung nicht ausreichend umschrieben und gerechtfertigt zu sein. Der EDSB fordert den EU-Gesetzgeber deshalb nachdrücklich auf, diese Frage eindeutig zu klären, bevor er den Rahmenbeschluss erlässt.

Notwendigkeit

26. Der Eingriffscharakter der Maßnahmen ist — wie vorstehend dargelegt — offensichtlich. Gleichzeitig jedoch ist ihr Nutzen noch bei weitem nicht nachgewiesen.

27. In der Folgenabschätzung zu dem Vorschlag liegt der Schwerpunkt eher auf der Frage, wie sich ein PNR-System der EU am besten verwirklichen lässt, als auf der Frage, ob ein solches System notwendig ist. In der Folgenabschätzung ([3]) wird auf bestehende PNR-Systeme in anderen Ländern (USA und Vereinigtes Königreich) hingewiesen. Bedauerlicherweise mangelt es jedoch an präzisen Fakten und Zahlen zu diesen Systemen. Bezüglich des britischen Systems „Semaphore" wird über „zahlreiche Festnahmen" hinsichtlich „verschiedener Straftaten" berichtet, allerdings fehlen nähere Angaben über den jeweiligen Zusammenhang mit Terrorismus oder organisierter Kriminalität. Zum dem Programm der USA werden mit Ausnahme der Feststellung, die EU habe sich „vom Nutzen der PNR-Daten und von den Möglichkeiten, die sie im Rahmen der Strafverfolgung bieten, ein Bild machen" können, keine näheren Einzelheiten genannt.

28. Nicht nur *im Vorschlag selbst* mangelt es an präzisen Informationen über die konkreten Ergebnisse derartiger PNR-Systeme, sondern auch in den *von anderen Behörden* (z. B. vom GAO der Vereinigten Staaten) veröffentlichten Berichten wird die Wirksamkeit der Maßnahmen bislang nicht bestätigt ([4]).

([1]) Diese Definition entstammt der folgenden Studie des Europarats zum Thema Profiling, die vor kurzem erstellt wurde: L'application de la Convention 108 au mécanisme de profilage, Eléments de réflexion destinés au travail futur du Comité consultatif (T-PD), Jean-Marc Dinant, Christophe Lazaro, Yves Poullet, Nathalie Lefever, Antoinette Rouvroy, November 2007 (noch nicht veröffentlicht). Siehe auch folgende Definition von Lee Bygrave: „Im Allgemeinen ist das Profiling ein Prozess, bei dem eine Reihe von charakteristischen Merkmalen (üblicherweise Verhaltensmerkmale) einer Einzelperson oder eines Kollektivs abgeleitet werden und die betreffende Person/das betreffende Kollektiv (oder weitere Personen/Kollektive) je nach diesen Merkmalen behandelt wird (werden). Das Profiling als solches hat zwei Hauptbestandteile: i) die Profilerstellung, d. h. das Ableiten eines Profils und ii) die Profilanwendung, d. h. die Behandlung von Einzelpersonen/Kollektiven anhand des erstellten Profils". L. A. BYGRAVE, Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling (Artikel 15 der EG-Datenschutzrichtlinie und automatisiertes Profiling), Computer Law & Security Report, 2001, Band 17, S. 17-24, http://www.austlii.edu.au/au/journals/PLPR/2000/40.html

([2]) Rotaru gegen Rumänien, Nr. 28341/95, Randnummern 50, 52 und 55.
Siehe auch Amann gegen Schweiz, Nr. 27798/95, Randnummer 50 ff.

([3]) Abschnitt 2.1 („Description of the problem").

([4]) Siehe beispielsweise den auf Antrag von Mitgliedern des Kongresses vorgelegten Bericht des United States Government Accountability Office vom Mai 2007 mit dem Titel „Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues remain", http://www.gao.gov/new.items/d07346.pdf

29. Der EDSB ist der Auffassung, dass Verfahren, bei denen das von einem Einzelnen ausgehende Risiko mit Hilfe von Datenschürfung und Verhaltensmustern analysiert wird, weiterer Prüfung bedürfen und dass ihr Nutzen im Rahmen der Terrorismusbekämpfung eindeutig nachgewiesen sein muss, bevor sie in einem derart großen Umfang angewandt werden.

Verhältnismäßigkeit

30. Zur Beurteilung der Ausgewogenheit zwischen dem Eindringen in die Privatsphäre des Einzelnen und der Notwendigkeit der Maßnahme ([1]) werden folgende Aspekte berücksichtigt:

— die Maßnahmen gelten für alle Fluggäste ungeachtet der Frage, ob die Strafverfolgungsbehörden bereits gegen sie ermitteln oder nicht. Es handelt sich um proaktive Nachforschungen in einem bisher nicht gekannten Ausmaß,

— Entscheidungen in Bezug auf Einzelpersonen können auf abstrakten Profilen beruhen und daher mit einer erheblichen Fehlerquote behaftet sein,

— die gegen den Einzelnen zu ergreifenden Maßnahmen sind ihrer Art nach Strafverfolgungsmaßnahmen, d. h. ihre Auswirkungen unter dem Gesichtspunkt von Ausgrenzung oder Zwang sind hinsichtlich des Eindringens in die Privatsphäre erheblich einschneidender als in anderen Zusammenhängen, wie etwa Kreditkartenbetrug oder Marketing.

31. Die Wahrung des Verhältnismäßigkeitsgrundsatzes bedeutet nicht nur, dass die vorgeschlagene Maßnahme wirksam sein muss, sondern auch, dass das Ziel des Vorschlags nicht mit den weniger tief in die Privatsphäre eingreifenden Instrumenten erreicht werden kann. Die Wirksamkeit der beabsichtigten Maßnahmen ist nicht nachgewiesen worden. Es muss sorgfältig geprüft werden, ob Alternativen bestehen, bevor zusätzliche/neue Maßnahmen zur Verarbeitung personenbezogener Daten eingeführt werden. Nach Ansicht des EDSB ist eine solch umfassende Beurteilung nicht erfolgt.

32. Der EDSB weist auf die anderen groß angelegten Systeme zur Überwachung der Bewegungen von Personen innerhalb der EU oder an ihren Grenzen hin, die entweder bereits in Betrieb sind oder demnächst eingeführt werden, insbesondere auf das Visa-Informationssystem ([2]) und auf das Schengener Informationssystem ([3]). Zwar zielen diese Instrumente nicht in erster Linie auf die Bekämpfung von Terrorismus und organisierter Kriminalität ab, sie sind (bzw. werden) aber den Strafverfolgungsbehörden bis zu einem gewissen Grade für den weiter gefassten Bereich der Kriminalitätsbekämpfung zugänglich (sein) ([4]).

33. Ein weiteres Beispiel betrifft die Verfügbarkeit von personenbezogenen Daten — vor allem biometrischen Daten — in den einzelstaatlichen Polizeidatenbanken gemäß dem im Mai 2005 unterzeichneten Prümer Vertrag, dessen Geltungsbereich gegenwärtig auf alle EU-Mitgliedstaaten ausgeweitet wird ([5]).

34. Diesen verschiedenen Instrumenten ist gemein, dass sie — sei es auch unter unterschiedlichen Gesichtspunkten — eine globale Überwachung der Bewegungen von Einzelpersonen ermöglichen. Die Frage, wie diese Instrumente bereits heute zur Bekämpfung bestimmter Formen der Kriminalität, einschließlich des Terrorismus, beitragen können, sollte eingehend und umfassend untersucht werden, bevor beschlossen wird, eine neue Form der systematischen Erfassung und Durchleuchtung aller Passagiere auf Flügen in die EU oder aus der EU einzuführen. Der EDSB empfiehlt, dass die Kommission eine derartige Untersuchung als eine notwendige Maßnahme im Rahmen des Gesetzgebungsverfahrens durchführt.

Schlussfolgerung

35. In Anbetracht der obigen Ausführungen gelangt der EDSB zu folgenden Schlussfolgerungen hinsichtlich der Rechtmäßigkeit der vorgeschlagenen Maßnahmen: Ein auf verschiedenen Datenbanken aufbauendes Vorhaben, bei dem keine Gesamtbetrachtung der konkreten Ergebnisse und Mängel erfolgt:

— steht im Widerspruch zu einer rationalen Gesetzgebungspolitik, wonach erst dann neue Instrumente erlassen werden dürfen, wenn die bestehenden Instrumente vollständig umgesetzt wurden und sich als unzureichend erwiesen haben ([6]),

— könnte anderenfalls zu einem Schritt in die totale Überwachungsgesellschaft führen.

36. Die Bekämpfung des Terrorismus kann sicherlich ein berechtigter Grund dafür sein, dass Ausnahmen vom grundlegenden Recht auf Privatsphäre und Datenschutz

([1]) Gemäß Artikel 9 des Übereinkommens Nr. 108 ist „eine Abweichung von den Artikeln 5, 6 und 8 (…) zulässig, wenn sie durch das Recht der Vertragspartei vorgesehen und in einer demokratischen Gesellschaft eine notwendige Maßnahme ist:
1. zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit sowie der Währungsinteressen des Staates oder zur Bekämpfung von Straftaten;
2. zum Schutz des Betroffenen oder der Rechte und Freiheiten Dritter".

([2]) Entscheidung 2004/512/EG des Rates vom 8. Juni 2004 zur Einrichtung des Visa-Informationssystems (VIS) (ABl. L 213 vom 15.6.2004, S. 5); Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt, KOM(2004) 835 endg.; Vorschlag für einen Beschluss des Rates über den Zugang der für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Prävention, Aufdeckung und Untersuchung terroristischer und sonstiger schwerwiegender Straftaten, KOM(2005) 600 endg.

([3]) Siehe insbesondere den Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L 205 vom 7.8.2007).

([4]) Siehe diesbezüglich: Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für einen Beschluss des Rates über den Zugang der für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Prävention, Aufdeckung und Untersuchung terroristischer und sonstiger schwerwiegender Straftaten (KOM(2005) 600 endg.) (ABl. C 97 vom 25.4.2006, S. 6).

([5]) Siehe hierzu die Stellungnahmen des EDSB zu den Beschlüssen von Prüm: Stellungnahme vom 4. April 2007 zur Initiative von 15 Mitgliedstaaten zum Erlass eines Beschlusses des Rates zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. C 169 vom 21.7.2007, S. 2), sowie Stellungnahme vom 19. Dezember 2007 zur Initiative der Bundesrepublik Deutschland im Hinblick auf die Annahme eines Beschlusses des Rates zur Durchführung des Beschlusses 2007/…/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität; abrufbar unter:
http://www.edps.europa.eu

([6]) Dieses Argument hat der EDSB mehrmals vorgebracht, zuletzt in seiner Stellungnahme vom 25. Juli 2007 zur Durchführung der Datenschutzrichtlinie (ABl. C 255 vom 27.10.2007, S. 1).

angewendet werden. Derartige Rechtseingriffe sind jedoch nur dann berechtigt, wenn ihre Notwendigkeit durch eindeutige und unbestreitbare Tatsachen untermauert und die Verhältnismäßigkeit der Verarbeitung nachgewiesen wird. Dies ist um so mehr erforderlich, wenn — wie im Vorschlag vorgesehen — weit reichende Eingriffe in die Privatsphäre des Einzelnen erfolgen sollen.

37. Es muss festgestellt werden, dass der Vorschlag keine derartigen Rechtfertigungsgründe enthält und zudem die Anforderung der Notwendigkeit und der Verhältnismäßigkeit nicht erfüllt.

38. Der EDSB weist nachdrücklich darauf hin, dass die vorstehend dargelegten Kriterien hinsichtlich der Notwendigkeit und der Verhältnismäßigkeit der Maßnahme unbedingt erfüllt werden müssen. Dies ist eine unabdingbare Voraussetzung für das Inkrafttreten des Vorschlags. Alle weiteren Bemerkungen des EDSB in dieser Stellungnahme sind im Lichte dieser Grundvoraussetzung zu verstehen.

III. ANWENDBARES RECHT — WAHRNEHMUNG DER RECHTE DER BETROFFENEN

Anwendbares Recht

39. Im Mittelpunkt der nachstehenden Untersuchung stehen folgende drei Punkte:

— eine Beschreibung der verschiedenen Stufen der im Vorschlag vorgesehenen Verarbeitung mit dem Ziel, das in jeder Stufe anwendbare Recht zu ermitteln,

— die Einschränkungen des Vorschlags für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, hinsichtlich des Geltungsbereichs und der Rechte des Betroffenen,

— eine allgemeinere Untersuchung der Frage, inwieweit ein Instrument der dritten Säule für private Akteure gelten kann, die im Rahmen der ersten Säule Daten verarbeiten.

Anwendbares Recht in den verschiedenen Bearbeitungsstufen

40. In Artikel 11 des Vorschlags ist Folgendes vorgesehen: „Die Mitgliedstaaten sorgen dafür, dass der Rahmenbeschluss (…) des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, auf die gemäß diesem Rahmenbeschluss verarbeiteten personenbezogenen Daten Anwendung findet."

41. Trotz dieser Bestimmung ist jedoch nicht deutlich, inwieweit der Datenschutz-Rahmenbeschluss — ein Instrument im Rahmen der dritten Säule des EU-Vertrags — für Daten gelten soll, die von Fluggesellschaften verarbeitet, von PNR-Zentralstellen erhoben und von weiteren zuständigen Behörden verwendet werden.

42. Die erste Stufe der Verarbeitung personenbezogener Daten besteht laut Vorschlag in der Verarbeitung durch die Fluggesellschaften, die verpflichtet sind, PNR-Daten — grundsätzlich unter Nutzung eines Push-Systems — an die nationalen PNR-Zentralstellen weiterzugeben. Sowohl der Vorschlag als auch die Folgenabschätzung [1] erwecken den Eindruck, dass die Daten auch in Form von Massenübertragungen von Fluggesellschaften an Datenmittler übermittelt werden könnten. Die Fluggesellschaften sind vornehmlich in einem kommerziellen Umfeld tätig, das durch die einzelstaatlichen Datenschutzvorschriften zur Durchführung der Richtlinie 95/46/EC geregelt wird [2]. Fragen zum anwendbaren Recht stellen sich dann, wenn die erhobenen Daten zu Strafverfolgungszwecken verwendet werden [3].

43. Die Daten würden dann von einem Datenmittler gefiltert (zu Formatierungszwecken und zur Ausklammerung von PNR-Daten, deren Übermittlung gemäß dem Vorschlag nicht vorgesehen ist) oder direkt an die PNR-Zentralstellen gesandt. Datenmittler könnten auch privatwirtschaftliche Akteure sein, wie etwa das Unternehmen SITA, das diese Funktion im Rahmen des PNR-Abkommens mit Kanada wahrnimmt.

44. Was die PNR-Zentralstellen betrifft, die für die Risikoanalyse der gesamten Datenmenge zuständig sind, so ist nicht deutlich, wer für die Verarbeitung verantwortlich sein soll. Hier könnten die Zoll- und Grenzschutzbehörden — d. h. nicht notwendigerweise die Strafverfolgungsbehörden — einbezogen werden.

45. Die anschließende Weitergabe der gefilterten Daten an die „zuständigen" Behörden würde wahrscheinlich in einem Strafverfolgungskontext erfolgen. Dem Vorschlag zufolge darf es sich dabei „nur um Strafverfolgungsbehörden handeln, die im Bereich der Verhütung und Bekämpfung terroristischer Straftaten und der organisierten Kriminalität tätig sind".

46. Je weiter der Verarbeitungsprozess voranschreitet, desto enger sind die beteiligten Akteure und der verfolgte Zweck mit der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verknüpft. In dem Vorschlag wird jedoch nicht explizit erwähnt, wann genau der Datenschutz-Rahmenbeschluss zur Anwendung kommt. Der Text erweckt sogar den Eindruck, dass dieser Rahmenbeschluss für die gesamte Verarbeitung und selbst für die Fluggesellschaften gelten soll [4]. Allerdings enthält der Rahmenbeschluss über den Schutz personenbezogener Daten an sich bereits einige Einschränkungen.

---

[1] Artikel 6 Absatz 3 des Vorschlags und Anhang A („Method of transmission of the data by the carriers") der Folgenabschätzung.

[2] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

[3] Siehe diesbezüglich die Auswirkungen des PNR-Urteils: Urteil des Gerichtshofs vom 30. Mai 2006, Europäisches Parlament gegen Rat (C-317/04) und Kommission (C-318/04), verbundene Rechtssachen C-317/04 und C-318/04, Slg. (2006), S. 56.

[4] Artikel 11 des Vorschlags. Siehe auch den Erwägungsgrund 10 des Einleitungsteils: „Der Rahmenbeschluss (…) des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, muss auch für alle nach Maßgabe dieses Rahmenbeschlusses verarbeiteten Daten gelten. Die Rechte der betroffenen Personen in Bezug auf eine derartige Datenverarbeitung, insbesondere das Recht auf Information, Zugang, Berichtigung, Löschung oder Sperrung sowie das Recht auf Schadenersatz und Rechtsmittel, sollten die gleichen wie die in dem Rahmenbeschluss vorgesehenen sein".

47. In diesem Zusammenhang hat der EDSB grundsätzliche Zweifel, ob Titel VI des EU-Vertrags als Rechtsgrundlage für routinemäßige rechtliche Verpflichtungen privatwirtschaftlicher Akteure zum Zwecke der Strafverfolgung dienen kann. Von Bedeutung ist zudem die Frage, ob Titel VI des EU-Vertrags als Rechtsgrundlage für rechtliche Verpflichtungen von Behörden dienen kann, die grundsätzlich außerhalb des Rahmens der Zusammenarbeit im Strafverfolgungsbereich stehen. Diese Fragen sollen im Folgenden untersucht werden.

Einschränkungen im Datenschutz-Rahmenbeschluss

48. Der Text des Vorschlags für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, enthält mindestens zwei Einschränkungen, die hinsichtlich des Geltungsbereichs von Bedeutung sind.

49. Erstens ist der Geltungsbereich des Datenschutz-Rahmenbeschlusses in diesem Beschluss selbst genau festgelegt: Der Rahmenbeschluss „gilt nur für Daten, die von zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen erhoben oder verarbeitet werden“ ([1]).

50. Zweitens soll der Datenschutz-Rahmenbeschluss nicht für Daten gelten, die ausschließlich auf innerstaatlicher Ebene verarbeitet werden; er ist vielmehr auf den Datenaustausch zwischen Mitgliedstaaten und die Weitergabe an Drittstaaten beschränkt ([2]).

51. Im Vergleich zur Richtlinie 95/46/EC weist der Datenschutz-Rahmenbeschluss auch einige Nachteile auf, darunter insbesondere eine weit gefasste Ausnahme vom Grundsatz der Zweckbeschränkung. Hinsichtlich dieses Grundsatzes wird der Zweck der Verarbeitung in dem Vorschlag eindeutig auf die Bekämpfung von Terrorismus und organisierter Kriminalität beschränkt. Der Datenschutz-Rahmenbeschluss gestattet jedoch eine Verarbeitung für umfassendere Zwecke. In einem derartigen Fall sollte der Vorschlag (als *lex specialis*) Vorrang vor dem Datenschutz-Rahmenbeschluss (als *lex generalis*) haben ([3]). Dies sollte im Text des Vorschlags explizit zum Ausdruck kommen.

52. Der EDSB empfiehlt deshalb, folgende Bestimmung in den Vorschlag aufzunehmen: „Personenbezogene Daten, die von den Fluggesellschaften gemäß diesem Rahmenbeschluss übermittelt werden, dürfen nicht für andere Zwecke als den der Bekämpfung von Terrorismus und organisierter Kriminalität verarbeitet werden. Die Ausnahmen, die hinsichtlich des Grundsatzes der Zweckbeschränkung im Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, vorgesehen sind, finden keine Anwendung“.

53. Abschließend stellt der EDSB fest, dass ein gravierender Mangel an Rechtssicherheit hinsichtlich der Frage besteht, welche Datenschutzregelung für die verschiedenen an dem Vorhaben beteiligten Akteure — insbesondere für Fluggesellschaften und andere Akteure der ersten Säule — gelten soll: Sind dies die Vorschriften des Vorschlags, die Vorschriften des Datenschutz-Rahmenbeschlusses oder die einzelstaatlichen Vorschriften zur Durchführung der Richtlinie 95/46/EG? Der Gesetzgeber sollte eindeutig festlegen, zu genau welchem Zeitpunkt der Verarbeitung diese verschiedenen Vorschriften gelten sollen.

Bedingungen für die Anwendung der Vorschriften der ersten und der dritten Säule

54. Der EDSB äußert grundsätzliche Zweifel daran, dass ein Instrument der dritten Säule routinemäßige rechtliche Verpflichtungen zu Strafverfolgungswecken für Akteure des privaten oder öffentlichen Sektors, die grundsätzlich außerhalb des Rahmens der Zusammenarbeit im Strafverfolgungsbereich stehen, begründen kann.

55. Hier könnte ein Vergleich mit zwei anderen Fällen angestellt werden, in denen der Privatsektor in die Vorratsspeicherung oder Weitergabe von Daten zu Strafverfolgungszwecken einbezogen war:

— *die Rechtssache PNR-USA, wo eine systematische Weitergabe von PNR-Daten durch Fluggesellschaften an Strafverfolgungsbehörden vorgesehen war.* Der Gerichtshof schloss in seinem Urteil in der PNR-Rechtssache eine Zuständigkeit der Gemeinschaft für den Abschluss des PNR-Abkommens aus. Er begründete dies unter anderem damit, dass die Übermittlung der PNR-Daten an die Zoll- und Grenzschutzbehörde der USA (CBP) eine Verarbeitung darstellt, die die öffentliche Sicherheit und die Tätigkeiten des Staates im strafrechtlichen Bereich betrifft ([4]). In diesem Fall bestand die Verarbeitung in einer *systematisch erfolgenden* Übermittlung an das CBP, was einen Unterschied zum folgenden Fall darstellt,

— *die allgemeine Vorratsspeicherung von Daten durch Betreiber elektronischer Kommunikationsdienste.* Hinsichtlich der Zuständigkeit der Gemeinschaft für die Festlegung einer entsprechenden Speicherfrist lassen sich Unterschiede zur Rechtssache PNR-USA feststellen, da die Richtlinie 2006/24/EG ([5]) lediglich eine Verpflichtung zu einer Vorratsspeicherung vorsieht, bei der die Betreiber die Kontrolle über die Daten behalten. Eine systematische Übermittlung von Daten an Strafverfolgungsbehörden ist nicht vorgesehen. Es kann daher festgestellt werden, dass die Diensteanbieter insofern, als sie die Kontrolle über die Daten behalten, auch weiterhin gegenüber den Betroffenen für die Einhaltung der Verpflichtungen zum Schutz personenbezogener Daten verantwortlich sind.

([1]) Erwägungsgrund 5a (Fassung vom 11. Dezember 2007) des Datenschutz-Rahmenbeschlusses.

([2]) Siehe Artikel 1.

([3]) Hinsichtlich dieses Aspekts sollte der Text von Artikel 27b der letzten Fassung des Rahmenbeschlusses zum Datenschutz in der Dritten Säule sorgfältig geprüft und erörtert werden.

([4]) Urteil des Gerichtshofs vom 30. Mai 2006, Europäisches Parlament gegen Rat (C-317/04) und Kommission (C-318/04), verbundene Rechtssachen C-317/04 und C-318/04, Slg. (2006), S. 56.

([5]) Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. L 105 vom 13.4.2006, S. 54).

56. In dem hier zu prüfenden Vorschlag für ein PNR-System der EU sollen die Fluggesellschaften die PNR-Daten aller Fluggäste systematisch zur Verfügung stellen. Diese Daten werden den Strafverfolgungsbehörden jedoch nicht direkt in Form von Massenübertragungen übermittelt. Sie können an einen Datenmittler gesandt werden und werden von einem Dritten ausgewertet, dessen Status unklar bleibt, bevor herausgefilterte Informationen an die zuständigen Behörden weitergegeben werden.

57. Der Hauptteil der Verarbeitung liegt in einer Grauzone, wobei sowohl zur ersten als auch zur dritten Säule materielle Verbindungen bestehen. Wie in Kapitel IV noch näher ausgeführt wird, bestehen Unklarheiten hinsichtlich der Eigenschaft der die Daten verarbeitenden Akteure. Fluggesellschaften sind eindeutig keine Strafverfolgungsbehörden, und als Datenmittler könnten Akteure aus dem Privatsektor fungieren. Selbst hinsichtlich der Rolle der PNR-Zentralstellen, die von Behörden wahrgenommen werden soll, muss darauf hingewiesen werden, dass nicht jede Behörde über die Eigenschaft und die Fähigkeiten zur routinemäßigen Durchführung von Strafverfolgungsaufgaben verfügt.

58. Traditionell besteht eine klare Trennung zwischen Strafverfolgungs- und privatwirtschaftlichen Tätigkeiten, wobei die Strafverfolgungsaufgaben von eigens dafür vorgesehenen Behörden — insbesondere Polizeibehörden — wahrgenommen werden, während privatwirtschaftliche Akteure auf Einzelfallbasis aufgefordert werden, diesen Strafverfolgungsbehörden personenbezogene Daten zu übermitteln. Die Tendenz geht nun dahin, dass private Akteure systematisch zur Mitarbeit zum Zwecke der Strafverfolgung verpflichtet werden, was die Frage aufwirft, welcher Datenschutzrahmen (erste oder zweite Säule) die Bedingungen dieser Zusammenarbeit regelt. Sollten die Vorschriften auf der Eigenschaft des für die Datenverarbeitung Verantwortlichen (Privatsektor) oder auf dem verfolgten Zweck (Strafverfolgung) beruhen?

59. Der EDSB hat bereits an die Gefahr eines rechtlichen Schlupflochs zwischen den Tätigkeiten im Rahmen der ersten und der dritten Säule erinnert ([1]). Es ist bei weitem nicht klar, ob Tätigkeiten von Privatunternehmen, die in irgendeiner Weise mit der Durchsetzung strafrechtlicher Bestimmungen verknüpft sind, in das Tätigkeitsfeld des EU-Gesetzgebers gemäß den Artikeln 30, 31 und 34 EUV fallen.

60. Sollte der allgemeine Rahmen (der ersten Säule) keine Anwendung finden, müsste ein Diensteanbieter innerhalb seiner Datenbanken schwierige Unterscheidungen treffen. Nach der geltenden Regelung ist klar, dass der für die Datenverarbeitung Verantwortliche allen Betroffenen unabhängig davon, welche Zwecke die Datenvorratsspeicherung rechtfertigen, den gleichen Schutz gewährleisten muss. Ein Ergebnis, bei dem die Verarbeitung durch Diensteanbieter zu unterschiedlichen Zwecken Gegenstand unterschiedlicher Datenschutz-Rahmenbedingungen wäre, sollte daher vermieden werden.

([1]) Siehe die Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische Parlament und an den Rat „Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie“ (ABl. C 255 vom 27.10.2007, S. 1). Siehe auch den Jahresbericht 2006, S. 47.

Wahrnehmung der Rechte der Betroffenen

61. Die unterschiedlichen rechtlichen Regelungen, die auf einzelstaatlicher Ebene gelten würden, hätten größere Auswirkungen, die in erster Linie die Wahrnehmung der Rechte der Betroffenen berühren würden.

62. Im Einleitungsteil des Vorschlags heißt es, dass Information, Zugang, Berichtigung, Löschung oder Sperrung sowie Schadenersatz und Rechtsmittel gemäß dem Datenschutz-Rahmenbeschluss gewährt werden bzw. erfolgen sollen. Diese Aussage beantwortet jedoch nicht die Frage, wer als für die Verarbeitung Verantwortlicher für die Beantwortung der Anfragen von betroffenen Personen zuständig ist.

63. Während die Fluggesellschaften Auskunft über die Verarbeitung erteilen könnten, stellt sich die Situation komplexer dar, wenn es um den Zugang zu Daten oder deren Berichtigung geht. Diese Rechte sind nach dem Datenschutz-Rahmenbeschluss beschränkt. Wie vorstehend dargelegt, ist es zweifelhaft, dass ein Diensteanbieter wie etwa eine Fluggesellschaft dazu verpflichtet werden könnte, entsprechend dem verfolgten Zweck (gewerbliche Gründe oder Strafverfolgung) gestaffelte Zugangs- und Berichtigungsrechte für die in ihrem Besitz befindlichen Daten zu gewähren. Man könnte sich auf den Standpunkt stellen, dass diese Rechte gegenüber der PNR-Zentralstelle oder den anderweitig benannten zuständigen Behörden wahrzunehmen sind. Der Vorschlag enthält diesbezüglich jedoch keine näheren Angaben; wie bereits erwähnt, ist auch nicht klar, dass diese Behörden (zumindest die PNR-Zentralstellen) Strafverfolgungsbehörden sein werden, die üblicherweise mit eingeschränkten (unter Umständen indirekten) Zugangsverfahren betraut sind.

64. Die Betroffenen könnten — was die PNR-Zentralstellen betrifft — auch mit verschiedenen Datenempfängern konfrontiert sein. Es besteht nämlich die Möglichkeit, dass die Daten nicht nur der PNR-Zentralstelle des Landes, in dem der Flug beginnt bzw. endet, sondern auch — auf Einzelfallbasis — den PNR-Zentralstellen anderer Mitgliedstaaten übermittelt werden. Ferner wäre es möglich, dass mehrere Mitgliedstaaten eine einzige gemeinsame PNR-Zentralstelle einrichten oder benennen. In einem solchen Fall könnte es möglich sein, dass der Betroffene bei einer Behörde eines anderen Mitgliedstaats Rechtsmittel einlegen muss. Auch hier ist nicht klar, ob die einzelstaatlichen Datenschutzvorschriften (die innerhalb der EU harmonisiert werden sollen) gelten oder ob spezielles Strafverfolgungsrecht zu berücksichtigen ist (da es in der dritten Säule an einer umfassenden Harmonisierung der einzelstaatlichen Vorschriften mangelt).

65. Die gleiche Frage stellt sich hinsichtlich des Zugangs zu Daten, die von Datenmittlern verarbeitet werden, deren Status unklar ist, wobei ebenfalls ein gemeinsamer Datenmittler für Fluggesellschaften in verschiedenen EU-Staaten zuständig sein könnte.

66. Der EDSB bedauert die Ungewissheit, die weiterhin hinsichtlich der Wahrnehmung dieser grundlegenden Rechte durch die betroffenen Personen besteht. Er unterstreicht, dass diese Situation im Wesentlichen darauf zurückzuführen ist, dass Akteure, für die die Strafverfolgung keine Hauptaufgabe ist, mit derartigen Aufgaben betraut werden.

Schlussfolgerung

67. Der EDSB ist der Ansicht, dass aus dem Vorschlag deutlich werden muss, welche Rechtsvorschriften für die jeweilige Verarbeitungsstufe gelten, und dass festgelegt werden muss, bei welchem Akteur oder welcher Behörde der Zugang zu beantragen ist bzw. Rechtsmittel einzulegen sind. Der EDSB erinnert daran, dass die Datenschutzvorschriften nach Artikel 30 Absatz 1 Buchstabe b EUV angemessen sein müssen und die gesamte Palette der im Vorschlag vorgesehenen Verarbeitungsvorgänge erfassen müssen. Die bloße Bezugnahme auf den Datenschutz-Rahmenbeschluss ist angesichts seines begrenzten Geltungsbereichs und der in ihm enthaltenen Beschränkung von Rechten nicht ausreichend. Was die Strafverfolgungsbehörden betrifft, so sollten die Vorschriften des Datenschutz-Rahmenbeschlusses zumindest für die gesamte in dem Vorschlag vorgesehene Verarbeitung gelten, damit eine kohärente Anwendung der Datenschutzgrundsätze gewährleistet ist.

IV. EIGENSCHAFT DER DATENEMPFÄNGER

68. Der EDSB stellt fest, dass der Vorschlag keine Bestimmungen hinsichtlich der Eigenschaft der Empfänger der von Fluggesellschaften erhobenen personenbezogenen Daten enthält, d. h. weder für Datenmittler noch für PNR-Zentralstellen oder zuständige Behörden. Diesbezüglich muss darauf hingewiesen werden, dass die Eigenschaft des Empfängers in einem direkten Zusammenhang mit der Art der für diesen Empfänger geltenden Datenschutzgarantien steht. Auf die Unterschiede zwischen diesen Garantien, die sich vor allem aus den Regelungen der ersten und der dritten Säule ergeben, wurde bereits hingewiesen. Es ist unabdingbar, dass die anwendbaren Vorschriften für alle beteiligten Akteure, d. h. sowohl für die nationalen Regierungen, die Strafverfolgungsbehörden und die Datenschutzbehörden als auch für die für die Verarbeitung Verantwortlichen und die betroffenen Personen, eindeutig festgelegt werden.

Datenmittler

69. Der Vorschlag enthält keine Angaben zur Eigenschaft der Datenmittler ([1]). Er enthält auch keine Festlegungen zur Rolle der Datenmittler als verarbeitende oder für die Verarbeitung verantwortliche Stellen. Die Erfahrungen deuten darauf hin, dass Einrichtungen des Privatsektors (Computerreservierungssysteme oder sonstige Einrichtungen) durchaus mit der Aufgabe betraut werden könnten, PNR-Daten direkt bei den Fluggesellschaften zu erheben und an die PNR-Zentralstellen weiterzugeben. Auf genau diese Weise werden Daten im Rahmen des PNR-Abkommens mit Kanada verarbeitet. SITA ([2]) ist dabei das für die Verarbeitung der Daten zuständige Unternehmen. Der Datenmittler spielt eine entscheidende Rolle, da er für das Herausfiltern/Umformatieren von Daten, die von den Fluggesellschaften in Form von Massenübertragungen übermittelt werden, zuständig sein könnte ([3]). Auch wenn die Datenmittler verpflichtet sind, die verarbeiteten Information unmittelbar nach der Weitergabe an die PNR-Zentralstellen zu löschen, ist die Verarbeitung an sich schon ein äußerst sensibler Vorgang: Die Mitwirkung von Datenmittlern hat unter anderem zur Folge, dass eine zusätzliche Datenbank mit gewaltigen Datenmengen geschaffen wird, die sogar — gemäß dem Vorschlag — sensible Daten (die anschließend von den Datenmittlern zu löschen wären) enthalten würde. Aus diesen Gründen empfiehlt der EDSB, Datenmittler nur dann an der Verarbeitung von Fluggastdaten zu beteiligen, wenn ihre Eigenschaft und ihre Aufgaben genau festgelegt werden.

PNR-Zentralstellen

70. Die PNR-Zentralstellen spielen eine entscheidende Rolle bei der Identifizierung von Personen, die an terroristischen oder der organisierten Kriminalität zuzurechnenden Straftaten beteiligt sind bzw. sein könnten oder mit derartigen Straftaten in Verbindung stehen (könnten). Gemäß dem Vorschlag sollen die PNR-Zentralstellen für die Entwicklung von Risikoindikatoren und die Gewinnung von Erkenntnissen über Reisegewohnheiten zuständig sein ([4]). Insoweit die Risikoanalyse auf Standardreisemustern und nicht auf materiellen Beweisen im Zusammenhang mit einem konkreten Fall beruht, kann die Auswertung als eine proaktive Ermittlung betrachtet werden. Der EDSB weist darauf hin, dass diese Art der Verarbeitung im Prinzip durch Rechtsvorschriften der Mitgliedstaaten streng geregelt (oder gar untersagt) wird und Aufgabe ganz bestimmter Behörden ist, deren Arbeitsweise ebenfalls strengen Regelungen unterliegt.

71. Die PNR-Zentralstellen sind daher mit einer sehr sensiblen Verarbeitung von Daten betraut, wobei der Vorschlag keine näheren Angaben zu ihrer Eigenschaft und zu den Bedingungen, unter denen sie diese Zuständigkeit wahrnehmen sollen, enthält. Zwar ist damit zu rechnen, dass diese Aufgabe von einer staatlichen Stelle wahrgenommen wird (möglicherweise Zoll oder Grenzschutz), doch wird den Mitgliedstaaten in dem Vorschlag nicht ausdrücklich untersagt, nachrichtendienstliche Stellen oder gar beliebige Verarbeitungseinrichtungen damit zu beauftragen. Der EDSB weist darauf hin, dass die für nachrichtendienstliche Stellen geltenden Anforderungen hinsichtlich Transparenz und Datenschutzgarantien nicht immer mit denen identisch sind, die für die traditionellen Strafverfolgungsbehörden gelten. Detaillierte Festlegungen zur Eigenschaft der PNR-Zentralstellen sind von entscheidender Bedeutung, da sie sich unmittelbar auf den geltenden Rechtsrahmen und die Überwachungsbedingungen auswirken. Der EDSB ist der Auffassung, dass der Vorschlag eine zusätzliche Bestimmung enthalten muss, mit der die Merkmale der PNR-Zentralstellen genau festgelegt werden.

([1]) Artikel 6 des Vorschlags.

([2]) SITA wurde 1949 von elf angeschlossenen Fluggesellschaften gegründet. Der Luftverkehrsbranche werden durch das gewerbliche Unternehmen SITA INC (Information, Networking, Computing) Mehrwertlösungen sowie durch SITA SC im Verbund Netzwerkdienste angeboten.

([3]) Folgenabschätzung Anhang A („Method of transmission of the data by the carriers“).

([4]) Artikel 3 des Vorschlags.

Zuständige Behörden

72. Aus Artikel 4 des Vorschlags geht hervor, dass jede Behörde, die im Bereich der Verhütung und Bekämpfung von terroristischen Straftaten und organisierter Kriminalität tätig ist, das Recht hat, die Daten zu empfangen. Zwar ist der Zweck eindeutig festgelegt, doch fehlen Angaben zur Eigenschaft der Behörde. Eine Begrenzung des Empfängerkreises auf Strafverfolgungsbehörden ist in dem Vorschlag nicht vorgesehen.

Wie bereits im Hinblick auf die PNR-Zentralstellen ausgeführt wurde, ist es von entscheidender Bedeutung, dass die Verarbeitung der sensiblen Daten, um die es hier geht, in eindeutige rechtliche Rahmenvorschriften eingebettet wird. Dies gilt beispielsweise für Strafverfolgungsbehörden in erheblich stärkerem Maße als für nachrichtendienstliche Stellen. In Anbetracht der Tatsache, dass der Vorschlag die Anwendung von Instrumenten aus dem Bereich der Datenschürfung und proaktive Nachforschungen vorsieht, kann nicht ausgeschlossen werden, dass auch nachrichtendienstliche Stellen und sonstige Behörden gleich welcher Art in die Verarbeitung der Daten einbezogen werden.

Schlussfolgerung

73. Der EDSB stellt ganz allgemein fest, dass die Verwirklichung eines PNR-Systems der EU zusätzlich dadurch erschwert wird, dass die Strafverfolgungsbehörden mit unterschiedlichen Zuständigkeiten ausgestattet sind, die — je nach dem Recht des betreffenden Mitgliedstaats — nachrichtendienstliche sowie steuer-, einwanderungs- und polizeirechtliche Aufgaben umfassen beziehungsweise ausschließen können. Dies ist ein weiterer Grund für die Empfehlung, den Vorschlag sowohl hinsichtlich der Eigenschaft der genannten Akteure als auch hinsichtlich der Garantien für die Kontrolle der Durchführung ihrer Aufgaben erheblich präziser zu gestalten. Es sollten zusätzliche Bestimmungen in den Vorschlag aufgenommen werden, mit denen die Zuständigkeiten und die rechtlichen Verpflichtungen von Datenmittlern, PNR-Zentralstellen und weiteren zuständigen Behörden genau festgelegt werden.

V. BEDINGUNGEN FÜR DIE WEITERGABE VON DATEN AN DRITTSTAATEN

74. Der Vorschlag enthält einige Garantien im Zusammenhang mit der Weitergabe von PNR-Daten an Drittstaaten ([1]). Insbesondere ist ausdrücklich die Anwendung des Datenschutz-Rahmenbeschlusses auf derartige Datenübermittlungen sowie eine spezielle Zweckbeschränkung vorgesehen, und für eine Weitergabe durch den Drittstaat ist die Zustimmung des Mitgliedstaats erforderlich. Die Weitergabe muss überdies im Einklang mit den innerstaatlichen Rechtsvorschriften des betreffenden Mitgliedstaates und mit den geltenden internationalen Abkommen erfolgen.

75. Viele Fragen bleiben jedoch offen, vor allem hinsichtlich der Art der Zustimmung, der Bedingungen für die Anwendung des Datenschutz-Rahmenbeschlusses sowie der „Gegenseitigkeit“ bei der Weitergabe von Daten an Drittstaaten.

([1]) Artikel 8 des Vorschlags.

Art der Zustimmung

76. Der Ursprungsmitgliedstaat muss der Weitergabe von Daten durch einen Drittstaat an einen anderen Drittstaat ausdrücklich zustimmen. In dem Vorschlag ist nicht festgelegt, unter welchen Bedingungen und durch wen diese Zustimmung erteilt wird und ob die einzelstaatlichen Datenschutzbehörden in die Entscheidung einzubeziehen sind. Der EDSB ist der Auffassung, dass die Art der Zustimmungserteilung mindestens den einzelstaatlichen Rechtsvorschriften entsprechen muss, in denen die Bedingungen für die Weitergabe personenbezogener Daten an Drittstaaten geregelt sind.

77. Ferner sollte die Zustimmung eines Mitgliedstaats nicht Vorrang vor dem Grundsatz haben, dass der Empfängerstaat ein ausreichendes Schutzniveau für die beabsichtigte Verarbeitung gewährleisten muss. Diese Bedingungen sollten kumulativ sein, da sie im Datenschutz-Rahmenbeschluss (Artikel 14) enthalten sind. Der EDSB schlägt deshalb vor, Artikel 8 Absatz 1 um einen Buchstaben c mit folgendem Wortlaut zu ergänzen: „und c der Drittstaat ein ausreichendes Schutzniveau für die beabsichtigte Datenverarbeitung gewährleistet“. Der EDSB erinnert diesbezüglich daran, dass Mechanismen vorgesehen werden müssen, die gemeinsame Standards und koordinierte Entscheidungen hinsichtlich der Angemessenheit sicherstellen ([2]).

Anwendung des Datenschutz-Rahmenbeschlusses

78. In dem Vorschlag wird auf die im Datenschutz-Rahmenbeschluss enthaltenen Bedingungen und Garantien verwiesen, während gleichzeitig ausdrücklich einige Bedingungen — insbesondere die oben erwähnte Zustimmung des betroffenen Mitgliedstaats — festgelegt werden und der Zweck auf die Verhinderung und Bekämpfung von terroristischen Straftaten und organisierter Kriminalität beschränkt wird.

79. Der Datenschutz-Rahmenbeschluss selbst enthält Bedingungen für die Weitergabe von personenbezogenen Daten an Drittstaaten, die vor allem die Beschränkung des Zwecks, die Eigenschaft der Empfänger, die Zustimmung des betroffenen Mitgliedstaats und den Grundsatz der Angemessenheit betreffen. Er sieht jedoch auch Ausnahmen von diesen Weitergabebedingungen vor. Danach können überwiegende berechtigte Interessen, insbesondere wichtige öffentliche Interessen, auch dann eine ausreichende Grundlage für die Weitergabe darstellen, wenn die vorstehend genannten Bedingungen nicht erfüllt sind.

80. Wie bereits in Kapitel III dieser Stellungnahme erwähnt, ist der EDSB der Auffassung, dass im Text des Vorschlags deutlich zum Ausdruck kommen muss, dass die präziseren Garantien des Vorschlags Vorrang vor den allgemeinen Bedingungen — und Ausnahmen — des Datenschutz-Rahmenbeschluss haben, soweit er Anwendung findet.

([2]) Stellungnahme des EDSB vom 26. Juni 2007 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, Nummern 27 bis 30, ABl. C 139 vom 23.6.2007, S. 1.

Gegenseitigkeit

81. Im Vorschlag wird auf mögliche „Gegenanfragen" von Staaten eingegangen, die die EU um PNR-Daten für Flüge aus der EU in ihr Hoheitsgebet ersuchen könnten. Wenn die EU Daten aus Datenbanken von Fluggesellschaften aus Drittstaaten anfordert, weil diese Gesellschaften Flüge in die EU bzw. aus der EU durchführen, könnten die betroffenen Drittstaaten derartige Daten — einschließlich Daten von EU-Bürgern — von in der EU niedergelassenen Fluggesellschaften anfordern. Die Kommission betrachtet diese Möglichkeit zwar als „sehr unwahrscheinlich", zieht sie jedoch in Betracht. Im Vorschlag wird diesbezüglich darauf hingewiesen, dass die Abkommen mit den USA und Kanada eine derartige Verarbeitung nach dem Grundsatz der Gegenseitigkeit vorsehen, „die automatisch anwendbar ist" ([1]). Der EDSB wirft die Frage nach der Bedeutung dieser automatischen Gegenseitigkeit und nach den für eine derartige Weitergabe geltenden Datenschutzgarantien auf, vor allem im Hinblick auf das Bestehen eines ausreichenden Schutzniveaus in dem betreffenden Staat.

82. Hier sollte zwischen Drittstaaten, die bereits ein Abkommen mit der EU geschlossen haben, und Drittstaaten, mit denen kein derartiges Abkommen besteht, unterschieden werden.

Staaten, die kein Abkommen mit der EU geschlossen haben

83. Der EDSB stellt fest, dass die Gegenseitigkeit dazu führen könnte, dass personenbezogene Daten an Staaten weitergegeben werden, in denen weder demokratische Standards noch ein ausreichendes Datenschutzniveau garantiert werden können.

84. Die Folgenabschätzung enthält weitere Angaben zu den Bedingungen für die Weitergabe von Daten an Drittstaaten. Dort wird auf den Vorteil des PNR-Systems der EU, nämlich die Filterung der Daten durch PNR-Zentralstellen, hingewiesen. Es sollen nur ausgewählte Daten von verdächtigen Personen (d. h. keine Massendaten) an die zuständigen Behörden der Mitgliedstaaten und vermutlich auch an Drittstaaten weitergegeben werden ([2]). Der EDSB empfiehlt, diesen Punkt im Vorschlag präziser zu fassen. Durch einen bloßen Hinweis in der Folgenabschätzung lässt sich der notwendige Schutz nicht gewährleisten.

85. Auch wenn die Auswahl von Daten dazu beitragen würde, die Auswirkungen auf die Privatsphäre der Fluggäste auf ein Mindestmaß zu begrenzen, muss daran erinnert werden, dass die Datenschutzgrundsätze weit über die Datenminimierung hinausreichen und Grundsätze wie Notwendigkeit, Transparenz und die Wahrnehmung der Rechte der Betroffenen umfassen, wobei alle Grundsätze zu berücksichtigen sind, wenn festgestellt wird, ob ein Drittstaat ein ausreichendes Schutzniveau gewährleistet.

Staaten, die ein bilaterales Abkommen mit der EU geschlossen haben

86. In der Folgenabschätzung heißt es, dass die Verarbeitung der EU in diesem Fall die Möglichkeit biete, auf bestimmten Standards zu beharren und in einschlägigen bilateralen Abkommen mit Drittstaaten für Kohärenz zu sorgen. Ferner werde die Möglichkeit geboten, von Drittländern, mit denen die EU ein Abkommen geschlossen habe, eine Verarbeitung nach dem Grundsatz der Gegenseitigkeit einzufordern, was derzeit nicht möglich sei ([3]).

87. Aus diesen Bemerkungen erwächst die Frage, wie sich der Vorschlag auf die bestehenden Abkommen mit Kanada und den USA auswirkt. Die Bedingungen für den Zugang zu Daten sind in diesen Abkommen viel weiter gefasst, da die Daten keiner vergleichbaren Auswahl unterzogen werden, bevor sie an diese beiden Drittstaaten weitergegeben werden.

88. In der Folgenabschätzung heißt es, dass in den Fällen, in denen die EU ein internationales Abkommen mit einem Drittstaat über den Austausch bzw. die Weitergabe von PNR-Daten an diesen Drittstaat geschlossen habe, die betreffenden Abkommen gebührend zu berücksichtigen seien. Die Fluggesellschaften sollten die PNR-Daten gemäß dem normalen Verfahren im Rahmen der geltenden Maßnahme an die PNR-Zentralstellen senden. Die PNR-Zentralstelle, die diese Daten erhalte, habe sie an die zuständige Behörde des Drittstaats, mit dem ein entsprechendes Abkommen bestehe, weiterzuleiten ([4]).

89. Während es einerseits den Anschein hat, als ziele der Vorschlag darauf ab, dass *lediglich ausgewählte* Daten an zuständige Behörden inner- oder außerhalb der EU weitergegeben werden, wird andererseits in der Folgenabschätzung, im Einleitungsteil des Vorschlags (Erwägungsgrund 21) und in Artikel 11 darauf hingewiesen, dass bestehende Abkommen gebührend zu berücksichtigen sind. Dies könnte zu dem Schluss führen, dass die Datenfilterung unter Umständen nur für künftig zu schließende Abkommen gilt. Bei dieser Betrachtungsweise könnte vorgesehen werden, dass der Zugang zu ungefilterten Datenmengen weiterhin der Regelfall für den Zugang von z. B. US-Behörden zu PNR-Daten sein wird (entsprechend den Bestimmungen des Abkommens zwischen der EU und den USA), dass jedoch gleichzeitig auf Einzelfallbasis eine Übermittlung von Daten an die USA erfolgen könnte, was spezifische, von den PNR-Zentralstellen ermittelte Daten betrifft, wozu auch Daten für Flüge in die USA gehören, ohne dass die Übermittlung auf diese Daten beschränkt sein müsste.

90. Der EDSB bedauert, dass es dem Vorschlag in diesem entscheidenden Punkt an Klarheit mangelt. Er hält es für äußerst wichtig, dass die Bedingungen für die Weitergabe von PNR-Daten an Drittstaaten kohärent sind und hinsichtlich des Schutzniveaus einheitlich gestaltet werden. Außerdem sollten der Rechtssicherheit wegen die für die Weitergabe von Daten geltenden Garantien im Vorschlag selbst präzisiert werden und nicht nur in der Folgenabschätzung, wie es derzeit der Fall ist.

([1]) Abschnitt 2 der Begründung des Vorschlags.
([2]) Folgenabschätzung Abschnitt 5.2 („Protection of privacy").
([3]) Folgenabschätzung Abschnitt 5.2 („Relations with third countries").
([4]) Folgenabschätzung Anhang A („Bodies receiving data from the Passenger Information Units").

VI. WEITERE WICHTIGE PUNKTE

Automatisierte Verarbeitung

91. Der EDSB stellt fest, dass im Vorschlag ausdrücklich festgelegt ist, dass die PNR-Zentralstellen und die zuständigen Behörden der Mitgliedstaaten Strafverfolgungsmaßnahmen nicht allein auf der Grundlage der automatisierten Verarbeitung von PNR-Daten oder der rassischen oder ethnischen Herkunft einer Person, ihrer religiösen oder philosophischen Überzeugungen, ihrer politischen Meinungen oder ihrer sexuellen Ausrichtung einleiten dürfen ([1]).

92. Diese Präzisierung ist zu begrüßen, weil dadurch die Gefahr verringert wird, dass willkürliche Maßnahmen gegen einzelne Personen ergriffen werden. Der EDSB stellt jedoch fest, dass der Geltungsbereich dieser Bestimmung auf *Strafverfolgungsmaßnahmen* von PNR-Zentralstellen oder zuständigen Behörden beschränkt ist. In der derzeitigen Fassung wird weder das automatisierte Herausfiltern von Einzelnen anhand von Standardprofilen ausgeschlossen, noch werden die automatisierte Erstellung von Listen mit Verdächtigen oder Maßnahmen wie etwa Dauerobservationen untersagt, so lange diese Maßnahmen nicht als Strafverfolgungsmaßnahmen betrachtet werden.

93. Der EDSB ist der Ansicht, dass der Begriff *Strafverfolgungsmaßnahmen* zu ungenau ist und dass grundsätzlich *keine Entscheidung* in Bezug auf Einzelpersonen *ausschließlich* auf der Grundlage der automatisierten Verarbeitung ihrer Daten getroffen werden sollte ([2]). Der EDSB empfiehlt, den Text entsprechend zu ändern.

Art der Daten

94. Der Vorschlag enthält in Artikel 5 Absatz 2 insofern eine wichtige Präzisierung, als deutlich gemacht wird, dass die Fluggesellschaften nicht verpflichtet sind, neben den für den ursprünglichen kommerziellen Zweck erfassten Daten weitere Daten zu erfassen oder auf Vorrat zu speichern.

95. Zu mehreren Aspekten der Verarbeitung dieser Daten sind weitere Bemerkungen angebracht:

— die zu übermittelnden, in Anhang 1 des Vorschlags aufgeführten Daten sind sehr umfangreich, und die betreffende Auflistung ähnelt der Liste der Daten, die den US-Behörden gemäß dem Abkommen zwischen der EU und den USA übermittelt werden. Die Datenschutzstellen, insbesondere die Datenschutzgruppe, haben bereits mehrmals Zweifel hinsichtlich der Art eines Teils der geforderten Daten geäußert ([3]),

— sowohl die Folgenabschätzung ([4]) als auch Artikel 6 Absatz 3 des Vorschlags erwecken den Eindruck, dass die Daten auch in großen Mengen von den Fluggesellschaften an die Datenmittler übermittelt werden könnten. Anfänglich wären die an einen Dritten weitergeleiteten Daten noch nicht einmal auf die in Anhang 1 des Vorschlags aufgeführten PNR-Daten beschränkt,

— hinsichtlich der Verarbeitung sensibler Daten stellt sich selbst dann, wenn diese Daten von den Datenmittlern herausgefiltert würden, weiterhin die Frage, ob die Weitergabe der Daten des Freitextfeldes durch die Fluggesellschaften unbedingt notwendig ist.

Der EDSB schließt sich den Argumenten an, die diesbezüglich in der Stellungnahme der Datenschutzgruppe vorgebracht wurden.

Verfahren für die Übermittlung von PNR-Daten

96. Die außerhalb der EU niedergelassenen Fluggesellschaften sind gehalten, die Daten unter Anwendung der *Push*-Methode an PNR-Zentralstellen oder Datenmittler zu senden, wenn sie über die dafür erforderliche Systemarchitektur verfügen. Ist dies nicht der Fall, müssen sie die Extraktion der Daten im Wege der *Pull*-Methode gestatten.

97. Die Zulassung verschiedener Datenübermittlungsmethoden je nach Fluggesellschaft führt lediglich dazu, dass die Kontrolle der Einhaltung der Datenschutzvorschriften bei der Übermittlung von PNR-Daten zusätzlich erschwert wird. Dies könnte außerdem den Wettbewerb zwischen EU-Fluggesellschaften und Fluggesellschaften aus Drittstaaten verzerren.

98. Der EDSB weist darauf hin, dass die Push-Methode, bei der die Fluggesellschaften die Kontrolle über die Art der übermittelten Daten und die Umstände der Übermittlung behalten können, unter dem Gesichtspunkt der Verhältnismäßigkeit der Verarbeitung die einzig zulässige Verfahrensweise darstellt. Außerdem muss es sich um ein wirkliches Push-Verfahren handeln, d. h. die Daten dürfen nicht in Form von Massenübertragungen an Datenmittler gesandt werden, sondern müssen gleich zu Beginn der Verarbeitung gefiltert werden. Es ist nicht zulässig, dass nicht notwendige Daten — sowie nicht in Anhang 1 des Vorschlags aufgeführte Daten — an einen Dritten gesandt werden, und zwar auch dann nicht, wenn der Dritte diese Daten unverzüglich zu löschen hat.

Vorratsspeicherung von Daten

99. In Artikel 9 des Vorschlags ist vorgesehen, dass PNR-Daten für einen Zeitraum von fünf Jahren gespeichert werden, nach dessen Ablauf die Daten für weitere acht Jahre in einer ruhenden Datenbank vorgehalten werden, auf die unter eingeschränkten Bedingungen zugegriffen werden kann.

([1]) Erwägungsgrund 20 und Artikel 3 Absätze 3 und 5 des Vorschlags.

([2]) Siehe diesbezüglich Artikel 15 Absatz 1 der Richtlinie 95/46/EG. Gemäß der Richtlinie sind derartige automatisierte Entscheidungen in Fällen, in denen die betroffene Person durch die Entscheidung beeinträchtigt würde, untersagt. Angesichts des Kontexts des Vorschlags dürften Entscheidungen im Rahmen der Strafverfolgung die betroffenen Personen in jeden Fall erheblich beeinträchtigen. Auch Sekundärkontrollen können die betroffene Person beinträchtigen, vor allem dann, wenn sie wiederholt erfolgen.

([3]) Siehe insbesondere die Stellungnahme Nr. 5/2007 vom 17. August 2007 zu dem im Juli 2007 geschlossenen Folgeabkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records — PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security, WP 138.

([4]) Folgenabschätzung Anhang A („Method of transmission of the data by the carriers“).

100. Der EDSB meldet hinsichtlich des Unterschieds zwischen den beiden Datenbanktypen folgende Zweifel an: Es ist zweifelhaft, ob die ruhende Datenbank ein wirkliches Archiv mit unterschiedlichen Verfahren für das Aufbewahren und Wiederauffinden von Daten darstellt. Die meisten Voraussetzungen für den Zugriff auf die ruhende Datenbank bestehen in Sicherheitsanforderungen, die ebenso für die Datenbank mit fünfjähriger Speicherfrist gelten könnten.

101. Die Gesamtdauer der Speicherung (13 Jahre) ist auf jeden Fall viel zu lang. Er wird in der Folgenabschätzung damit gerechtfertigt, dass es erforderlich sei, Risikoindikatoren zu entwickeln und Reise- und Verhaltensmuster zu erstellen ([1]), deren Wirksamkeit weiterer Nachweise bedarf. Während es einleuchtet, dass Daten in einem bestimmten Fall bei laufenden Ermittlungen so lange wie notwendig gespeichert werden, ist eine 13 Jahre währende Vorratsspeicherung der Daten sämtlicher Fluggäste ohne jeglichen Verdacht durch nichts zu begründen.

102. Der EDSB stellt außerdem fest, dass diese Speicherfrist durch die Antworten der Mitgliedstaaten auf den Fragebogen der Kommission, denen zufolge die erforderliche Speicherfrist im Durchschnitt 3,5 Jahre betragen würde, nicht gestützt wird ([2]).

103. Außerdem ist die Frist von 13 Jahren mit der im jüngsten Abkommen mit den USA vorgesehenen Speicherfrist von 15 Jahren vergleichbar. Der EDSB ist stets davon ausgegangen, dass diese lange Speicherfrist nur wegen des starken Drucks der US-Regierung, eine deutlich längere Frist als 3,5 Jahre festzulegen, vereinbart wurde und nicht etwa deswegen, weil sich der Rat oder die Kommission zu irgendeinem Zeitpunkt dafür stark gemacht hätten. Es besteht kein Grund, einen solchen Kompromiss, der lediglich als notwendiges Verhandlungsergebnis gerechtfertigt wurde, innerhalb der EU selbst in einen Rechtsakt zu übernehmen.

Rolle des Ausschusses der Mitgliedstaaten

104. Der nach Artikel 14 des Vorschlags einzusetzende Ausschuss der Mitgliedstaaten soll nicht nur für Sicherheitsaspekte einschließlich der Protokollierung und Verschlüsselung von PNR-Daten zuständig sein, sondern auch für Leitlinien für gemeinsame allgemeine Kriterien, Methoden und Verfahren im Zusammenhang mit der Risikobewertung.

105. Abgesehen von diesen Hinweisen enthält der Vorschlag keinerlei Angaben oder Kriterien hinsichtlich der konkreten Rahmen- und sonstigen Bedingungen für die Durchführung von Risikoanalysen. In der Folgenabschätzung heißt es, dass die Kriterien letztendlich durch die (sich ständig ändernden) Erkenntnisse der einzelnen Mitgliedstaaten bestimmt würden. Die Risikoanalyse soll ohne einheitliche Standards für die Identifizierung von Verdächtigen durchgeführt werden. Es erscheint mithin fraglich, inwieweit der Ausschuss der Mitgliedstaaten vor diesem Hintergrund eine Rolle spielen kann.

Sicherheit

106. Der Vorschlag sieht eine Reihe von Sicherheitsmaßnahmen ([3]) vor, die die PNR-Zentralstellen, die Datenmittler und andere zuständige Behörden zum Schutz der Daten treffen sollen. In Anbetracht der Bedeutung der Datenbank und der Sensibilität der Verarbeitung vertritt der EDSB die Ansicht, dass zusätzlich zu den vorgesehenen Maßnahmen die Einrichtung, die die Daten verarbeitet, auch verpflichtet sein sollte, jede Verletzung der Sicherheit offiziell zu melden.

107. Der EDSB hat Kenntnis von dem Vorhaben, ein derartiges Meldeverfahren für den Bereich der elektronischen Kommunikation auf europäischer Ebene festzulegen. Er empfiehlt, diese Sicherheitsmaßnahme auch in den hier vorliegenden Vorschlag aufzunehmen, und verweist diesbezüglich auf das Verfahren bei Sicherheitsverletzungen, das in den USA für staatliche Stellen eingeführt wurde ([4]). Zu Sicherheitsverletzungen kann es in allen Bereichen des privaten und des öffentlichen Sektors kommen, wie der jüngste Verlust einer kompletten behördlichen Datenbank mit Bürgerdaten in Großbritannien gezeigt hat ([5]). Große Datenbanken wie die in dem Vorschlag vorgesehene müssten vorrangig in den Genuss eines derartigen Warnsystems kommen.

Überprüfungs- und Verfallsklausel

108. Der EDSB nimmt zur Kenntnis, dass innerhalb von drei Jahren nach Inkrafttreten des Rahmenbeschlusses eine Überprüfung anhand eines von der Kommission erstellten Berichts erfolgen soll. Er erkennt an, dass in diesem Bericht, der auf Informationen der Mitgliedstaaten beruhen wird, den Datenschutzgarantien besondere Aufmerksamkeit gewidmet und außerdem auf die Anwendung der Push-Methode, die Vorratsspeicherung und die Qualität der Risikobewertungen eingegangen werden soll. Diese Überprüfung sollte im Sinne der Vollständigkeit auch die Ergebnisse einer Auswertung der statistischen Daten beinhalten, die bei der Verarbeitung der PNR-Daten erzeugt werden. Diese Statistiken sollten neben den in Artikel 18 des Vorschlags genannten Angaben auch statistische Daten zur Ermittlung von Personen mit hohem Gefahrenotenzial, wie etwa die Kriterien für diese Ermittlung und die konkreten Ergebnisse aller zur Ermittlung führenden Strafverfolgungsmaßnahmen umfassen.

([1]) Folgenabschätzung Anhang A („Data retention period").
([2]) Folgenabschätzung Anhang B.
([3]) Artikel 12 des Vorschlags.
([4]) Siehe insbesondere die Arbeiten der US-amerikanischen „Identity Theft Task Force" unter: http://www.idtheft.gov
([5]) Siehe folgenden Link zur Website der britischen Steuer- und Zollbehörde: http://www.hmrc.gov.uk/childbenefit/update-faqs.htm Siehe auch unter: http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

109. Der EDSB hat in dieser Stellungnahme bereits nachdrücklich darauf hingewiesen, dass es an konkreten Nachweisen für die Notwendigkeit des vorgeschlagenen Systems mangelt. Er ist gleichwohl der Ansicht, dass der Rahmenbeschluss im Falle seines Inkrafttretens zumindest eine Verfallsklausel enthalten sollte. Nach Ablauf des Zeitraums von drei Jahren sollte der Rahmenbeschluss aufgehoben werden, wenn kein Nachweis zur Rechtfertigung seiner Aufrechterhaltung vorliegt.

Auswirkung auf andere Rechtsakte

110. Die Schlussbestimmungen des Vorschlags enthalten eine Bedingung für die weitere Anwendung bereits bestehender bilateraler oder multilateraler Übereinkünfte oder Vereinbarungen. Diese Instrumente können nur insoweit angewandt werden, als sie mit den Zielen des vorgeschlagenen Rahmenbeschlusses vereinbar sind.

111. Der EDSB fragt sich, welche Tragweite diese Bestimmung hat. Wie bereits in Kapitel V unter dem Stichwort „Gegenseitigkeit" erwähnt, ist nicht klar, wie sich diese Bestimmung auf den Inhalt von Abkommen mit Drittstaaten (z. B. auf das Abkommen mit den USA) auswirken wird. Daneben ist auch nicht klar, ob sich diese Bestimmung auf die Bedingungen für die Anwendung von Instrumenten mit einem weiter gefassten Geltungsbereich, wie etwa das Übereinkommen Nr. 108 des Europarates, auswirken könnte. Auch wenn dies in Anbetracht der Unterschiede hinsichtlich des institutionellen Kontexts und der beteiligten Akteure unwahrscheinlich erscheint, sollte jeglicher Fehlinterpretation vorgebeugt und im Vorschlag deutlich gemacht werden, dass dieser keine Auswirkungen auf Instrumente mit einem breiteren Geltungsbereich — insbesondere solche, die auf den Schutz grundlegender Rechte abzielen — hat.

VII. **SCHLUSSFOLGERUNG**

112. Der EDSB weist auf die erheblichen Auswirkungen des Vorschlags unter dem Gesichtspunkt des Datenschutzes hin. Er hat sich bei seiner Untersuchung auf vier grundlegende Fragen, die durch den Vorschlag aufgeworfen werden, konzentriert und unterstreicht, dass diese Fragen im Rahmen eines umfassenden Ansatzes angegangen werden müssen. In seiner derzeitigen Fassung ist der Vorschlag nicht mit grundlegenden Rechten vereinbar, was insbesondere für Artikel 8 der Charta der Grundrechte der Europäischen Union gilt, und sollte deshalb nicht angenommen werden.

113. Für den Fall, dass den vorstehenden Bemerkungen — insbesondere den Anforderungen hinsichtlich der Rechtmäßigkeit — entsprochen wird, enthält diese Stellungnahme einige Formulierungsvorschläge, die vom Gesetzgeber berücksichtigt werden sollten. In diesem Zusammenhang wird insbesondere auf die Nummern 67, 73, 77, 80, 90, 93, 106, 109 und 111 der Stellungnahme verwiesen.

Rechtmäßigkeit der vorgeschlagenen Maßnahmen

114. Obschon der allgemeine Zweck der Bekämpfung von Terrorismus und organisierter Kriminalität als solcher deutlich und legitim ist, werden die Kernbestandteile der vorgesehenen Verarbeitung nicht ausreichend umschrieben und gerechtfertigt.

115. Der EDSB ist der Auffassung, dass Verfahren, bei denen das von einem Einzelnen ausgehende Risiko mit Hilfe von Datenschürfung und Verhaltensmustern analysiert wird, weiterer Prüfung bedürfen und dass ihr Nutzen im Rahmen der Terrorismusbekämpfung eindeutig nachgewiesen sein muss, bevor sie in einem derart großen Umfang angewandt werden.

116. Ein auf verschiedenen Datenbanken aufbauendes Vorhaben, bei dem keine Gesamtbetrachtung der konkreten Ergebnisse und Mängel erfolgt:

— steht im Widerspruch zu einer rationalen Gesetzgebungspolitik, wonach erst dann neue Instrumente erlassen werden dürfen, wenn die bestehenden Instrumente vollständig umgesetzt wurden und sich als unzureichend erwiesen haben,

— könnte anderenfalls zu einem Schritt in die totale Überwachungsgesellschaft führen.

117. Die Bekämpfung des Terrorismus kann sicherlich ein berechtigter Grund dafür sein, dass Ausnahmen vom grundlegenden Recht auf Privatsphäre und Datenschutz angewendet werden. Derartige Rechtseingriffe sind jedoch nur dann berechtigt, wenn ihre Notwendigkeit durch eindeutige und unbestreitbare Tatsachen untermauert und die Verhältnismäßigkeit der Verarbeitung nachgewiesen wird. Dies ist um so mehr erforderlich, wenn — wie im Vorschlag vorgesehen — weit reichende Eingriffe in die Privatsphäre des Einzelnen erfolgen sollen.

118. Der Vorschlag enthält keine derartigen Rechtfertigungsgründe und erfüllt zudem nicht die Anforderung der Notwendigkeit und der Verhältnismäßigkeit.

119. Der EDSB weist nachdrücklich darauf hin, dass die vorstehend dargelegten Kriterien hinsichtlich der Notwendigkeit und der Verhältnismäßigkeit der Maßnahme unbedingt erfüllt werden müssen. Die Erfüllung dieser Kriterien ist eine unabdingbare Voraussetzung für das Inkrafttreten des Vorschlags.

Geltender Rechtsrahmen

120. Der EDSB stellt fest, dass ein gravierender Mangel an Rechtssicherheit hinsichtlich der Frage besteht, welche Regelung für die verschiedenen an dem Vorhaben beteiligten Akteure — insbesondere für Fluggesellschaften und andere Akteure der ersten Säule — gelten soll: Sind dies die Vorschriften des Vorschlags, die Vorschriften des Datenschutz-Rahmenbeschlusses oder die einzelstaatlichen Vorschriften zur Durchführung der Richtlinie 95/46/EG? Der Gesetzgeber sollte eindeutig festlegen, in welchen Stufen der Verarbeitung diese verschiedenen Vorschriften gelten sollen.

121. Die derzeitige Tendenz, private Akteure systematisch zur Mitarbeit zum Zwecke der Strafverfolgung zu verpflichten, wirft die Frage auf, welcher Datenschutzrahmen (erste oder zweite Säule) die Bedingungen dieser Zusammenarbeit regelt. Es ist nicht klar, ob die Vorschriften auf der Eigenschaft des für die Datenverarbeitung Verantwortlichen (Privatsektor) oder auf dem verfolgten Zweck (Strafverfolgung) beruhen sollen.

122. Der EDSB hat bereits auf die Gefahr eines rechtlichen Schlupflochs zwischen den Tätigkeiten im Rahmen der ersten und der dritten Säule hingewiesen ([1]). Es ist bei weitem nicht klar, ob Tätigkeiten von Privatunternehmen, die in irgendeiner Weise mit der Durchsetzung strafrechtlicher Bestimmungen verknüpft sind, in das Tätigkeitsfeld des EU-Gesetzgebers gemäß den Artikeln 30, 31 und 34 EUV fallen.

123. Ein Ergebnis, bei dem die Verarbeitung durch Diensteanbieter zu unterschiedlichen Zwecken Gegenstand unterschiedlicher Datenschutz-Rahmenbedingungen wäre, sollte vermieden werden, vor allem in Anbetracht der Probleme, die dies hinsichtlich der Wahrnehmung der Rechte der Betroffenen aufwerfen würde.

Eigenschaft der Datenempfänger

124. Der Vorschlag sollte Bestimmungen hinsichtlich der Eigenschaft der Empfänger der von Fluggesellschaften erhobenen personenbezogenen Daten enthalten, und zwar unabhängig davon, ob es sich hierbei um einen Datenmittler, eine PNR-Zentralstelle oder eine zuständige Behörde handelt.

125. Die Eigenschaft des Empfängers, der in einigen Fällen ein privatwirtschaftlicher Akteur sein kann, steht in einem direkten Zusammenhang mit der Art der für diesen Empfänger geltenden Datenschutzgarantien. Es ist unabdingbar, dass die geltenden Vorschriften für alle beteiligten Akteure, d. h. sowohl für den Gesetzgeber und die Datenschutzbehörden als auch für die für die Verarbeitung Verantwortlichen und die betroffenen Personen, eindeutig festgelegt werden.

Weitergabe von Daten an Drittstaaten

126. Der EDSB weist darauf hin, dass im Empfängerstaat ein angemessenes Schutzniveau gewährleistet sein muss. Er stellt ferner die Bedeutung des im Vorschlag erwähnten Grundsatzes der „Gegenseitigkeit“ und dessen Anwendung auf Staaten, die bereits durch ein Abkommen mit der EU gebunden sind, wie Kanada und die USA, in Frage. Er hält es für äußerst wichtig, dass die Bedingungen für die Weitergabe von PNR-Daten an Drittstaaten kohärent sind und hinsichtlich des Schutzniveaus einheitlich gestaltet werden.

Weitere wichtige Punkte

127. Der EDSB weist den Gesetzgeber ferner auf bestimmte Aspekte des Vorschlags hin, bei denen präzisere Festlegungen oder eine bessere Berücksichtigung der Datenschutzgrundsätze erforderlich sind. Dies betrifft insbesondere folgende Aspekte:

— die Bedingungen, unter denen automatisierte Entscheidungen getroffen werden dürfen, sollten eingeschränkt werden,

— die Menge der verarbeiteten Daten sollte eingeschränkt werden,

— die Weitergabe von Daten sollte ausschließlich nach der *Push*-Methode erfolgen,

— die Datenspeicherfrist wird als viel zu lang und nicht gerechtfertigt erachtet,

— die Rolle des Ausschusses der Mitgliedstaaten könnte hinsichtlich der von ihm zu erarbeitenden Leitlinien für die Risikobewertung genauer festgelegt werden,

— die Sicherheitsmaßnahmen sollten ein Verfahren für die Meldung von Sicherheitsverletzungen umfassen,

— die Überprüfung des Beschlusses sollte eine Verfallsklausel einschließen,

— es sollte deutlich festgelegt werden, dass sich der Vorschlag in keiner Weise auf Instrumente mit einem breiteren Geltungsbereich auswirkt, die insbesondere auf den Schutz grundlegender Rechte abstellen.

Schlussbemerkungen

128. Der EDSB stellt fest, dass der Vorschlag zu einem Zeitpunkt vorgelegt wird, zu dem grundlegende Änderungen des institutionellen Rahmens der Europäischen Union anstehen. Der Vertrag von Lissabon wird fundamentale Auswirkungen auf die Beschlussfassung haben, vor allem hinsichtlich der Rolle des Europäischen Parlaments.

129. Da sich der Vorschlag in einer bisher nicht gekannten Weise auf die Grundrechte auswirkt, empfiehlt der EDSB, den Vorschlag nicht im Rahmen des derzeitigen Vertrags anzunehmen, sondern dafür zu sorgen, dass er nach dem im neuen Vertrag vorgesehenen Mitentscheidungsverfahren behandelt wird. Dies würde die rechtlichen Grundlagen stärken, auf denen die entscheidenden Maßnahmen, die in dem Vorschlag vorgesehen sind, getroffen werden sollen.

([1]) Siehe die Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische Parlament und an den Rat „Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie“, ABl. C 255 vom 27.10.2007, S. 1. Siehe auch den Jahresbericht 2006, S. 47.

Bundesrat **Drucksache 826/07 (Beschluss)**

15.02.08

Beschluss
des Bundesrates

Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken

KOM(2007) 654 endg.; Ratsdok. 14922/07

Der Bundesrat hat in seiner 841. Sitzung am 15. Februar 2008 gemäß §§ 3 und 5 EUZBLG die folgende Stellungnahme beschlossen:

1. Der Bundesrat teilt das mit dem Rahmenbeschluss verfolgte Anliegen, EU-weite Maßnahmen zur Bekämpfung von Terrorismus und organisierter Kriminalität zu entwickeln. Der Bundesrat unterstützt ferner die Absicht der Kommission, hierzu einheitliche Handlungsvorgaben zu erarbeiten, die ein hohes Maß an Sicherheit in den Mitgliedstaaten gewährleisten.

2. Bei der Verfolgung dieses Ziels ist das Verhältnis zwischen der Wahrung der Freiheitsrechte und dem Schutz der öffentlichen Sicherheit in ein Gleichgewicht zu bringen. Der Vorschlag des Rahmenbeschlusses stellt dieses Gleichgewicht nicht ausreichend her.

3. Der Verabschiedung des Rahmenbeschlusses stehen aus Sicht des Bundesrates derzeit einige gewichtige Gesichtspunkte entgegen. Der Vorschlag setzt in folgenden Hinsichten falsche Akzente:

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln
Telefon: (02 21) 97 66 83 40, Telefax: (02 21) 97 66 83 44
ISSN 0720-2946

4. Der vorliegende Rahmenbeschluss verweist in den Artikeln 2 und 11 auf andere Rahmenbeschlüsse, die noch nicht verabschiedet sind. Insbesondere können so die Regelungen zum Schutz personenbezogener Daten nicht hinreichend beurteilt werden. Es bestehen erhebliche Zweifel, ob der beabsichtigte Rahmenbeschluss über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, überhaupt auf den Datenaustausch zwischen privaten Fluggesellschaften und den vorgeschlagenen PNR-Zentralstellen Anwendung finden würde. Nach seiner derzeitigen Entwurfsfassung bezieht er sich jedenfalls nur auf den Datenaustausch zwischen Behörden. Der Bundesrat empfiehlt, den genannten Rahmenbeschluss des Rates über den Schutz personenbezogener Daten zunächst abzuwarten.

5. Die Verarbeitung von PNR-Daten stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung bzw. Achtung des Privatlebens dar. Ein solcher Eingriff ist nur zulässig, wenn im Hinblick auf den verfolgten Zweck, Terrorismus und organisierte Kriminalität zu bekämpfen, ein Bedürfnis für den Zugang zu diesen Daten besteht. Aus Sicht des Bundesrates ist der Nachweis hierfür weder im vorliegenden Rahmenbeschluss noch in der Folgenabschätzung der Kommission - SEK(2007) 1453 - erbracht.

6. Bereits mit der Richtlinie 2004/82/EG wurden Fluggesellschaften verpflichtet, den zuständigen Behörden der Mitgliedstaaten erweiterte Fluggastdaten (API-Daten) zu übermitteln. Damit wurde ein Instrument zur Verbesserung der Einreisekontrolle und zur Bekämpfung der illegalen Einwanderung geschaffen, das auch einen Nutzen zur Bekämpfung des internationalen Terrorismus und sonstiger schwerer Straftaten darstellt. Aus Sicht des Bundesrates sollte eine Ausweitung der Erhebung und Speicherung von Fluggastdaten nicht beschlossen werden, solange nicht feststeht, dass sich die bisherigen Rechtsinstrumente als unzureichend erwiesen haben. Es wird deshalb angeregt, zunächst die Wirkungen der Richtlinie 2004/82/EG zu untersuchen.

7. Nach der Rechtsprechung des Bundesverfassungsgerichts (vgl. BVerfGE 65, 1, 47) besteht außerhalb statistischer Zwecke ein "striktes Verbot der Sammlung personenbezogener Daten auf Vorrat". Es ist danach nicht zulässig, solche Daten zu erheben und zu speichern, die zur Erfüllung der konkreten und aktuellen Aufgabe nicht benötigt werden, die aber zu einem späteren Zeitpunkt gebraucht werden könnten. Nach der Rechtsprechung des EGMR stellt das systematische, rechtlich unbegrenzte Sammeln von Daten eine Verletzung von Artikel 8 EMRK dar (vgl. EGMR, Urteil vom 4. Mai 2000 - 28341/95 - Rotaru, Tz. 57 ff.). Vor diesem Hintergrund bestehen aus Sicht des Bundesrates erhebliche Bedenken gegen die in den Artikeln 5 und 9 des Rahmenbeschlusses vorgesehene anlass- und verdachtsunabhängige Erhebung und Speicherung von PNR-Daten sämtlicher die EU-Grenzen überquerender Fluggäste.

8. Der Grundsatz der Zweckbindung ist eines der Grundprinzipien des Datenschutzes. Danach dürfen personenbezogene Daten nur für bereichsspezifisch und präzise festgelegte Zwecke gespeichert werden und nur im Rahmen dieser Zwecke verwendet werden. Zudem muss das Recht so hinreichend deutlich sein, dass es dem Bürger angemessene Hinweise gibt, unter welchen Voraussetzungen die Behörden befugt sind, Informationen aus seinem Privatleben zu sammeln und zu benutzen. Aus Sicht des Bundesrates bestehen Zweifel, ob der vorgeschlagene Rahmenbeschluss mit den Regelungen in Artikel 3 Abs. 5, Artikel 8 Abs. 1 und Artikel 11 Abs. 2 diesen Anforderungen hinreichend Rechnung trägt.

9. Die Speicherungsdauer von insgesamt 13 Jahren überschreitet die in Deutschland allgemein übliche Regelfrist für polizeiliche Speicherungen um drei Jahre.

   Aus Sicht des Bundesrates ist die verdachtslose Speicherung der PNR-Daten sämtlicher die EU-Grenzen überquerender Fluggäste über einen Zeitraum von 13 Jahren unabhängig davon, dass die Daten acht Jahre in einer "ruhenden Datenbank" vorgehalten werden, mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar. Der Bundesrat weist zudem darauf hin, dass die vorgesehene Frist nicht den Antworten entspricht, die die Mitgliedstaaten im von der Kommission versandten Fragenbogen gegeben haben; darin wurde auf die Frage nach der Speicherdauer durchschnittlich ein Zeitraum von drei einhalb Jahren angegeben.

Auch die erste Speicherungsphase nach Artikel 9 Abs. 1 geht mit fünf Jahren noch über das fachliche Gebotene hinaus.

10. Es erscheint bedenklich, dass der Rahmenbeschlussvorschlag keine Möglichkeit für betroffene Bürger vorsieht, Auskunft zu den über ihre Person gespeicherten Daten sowie die Berichtigung oder Löschung falscher, z. B. fehlerhaft übermittelter, Daten zu verlangen. Der Vorschlag sieht auch keine zumindest nachträgliche Benachrichtigung betroffener Fluggäste über eine erfolgte Datenweitergabe und Gefährlichkeitseinstufung und auch keinen diesbezüglichen Rechtsbehelf vor.

11. Die Sammlung und Auswertung der genannten Datensätze dient nicht nur der Verhütung und Bekämpfung von terroristischen Straftaten, sondern auch der strafrechtlichen Verfolgung der organisierten Kriminalität. Aus Sicht des Bundesrates muss deshalb bei der Vereinbarung europäischer Vorgaben für die Einrichtung einer Zentralstelle sichergestellt sein, dass durch deren spätere Umsetzung die grundsätzlich bestehende Zuständigkeit der Strafverfolgungsbehörden der Länder für die Verfolgung von Straftaten, die der organisierten Kriminalität zuzurechnen sind, nicht tangiert wird.

12. Der Vorschlag geht ersichtlich davon aus, dass den nationalen Zentralstellen die Möglichkeit einzuräumen ist, selbst Strafverfolgungsmaßnahmen einzuleiten. Der Bundesrat weist darauf hin, dass eine derartige Befugnis im Widerspruch zur gesetzlichen Aufgabenverteilung zwischen Staatsanwaltschaft und Polizei stünde und letztlich die staatsanwaltschaftliche Sachleitungsbefugnis in Frage stellen würde.

13. Es erscheint zweifelhaft, ob die Artikel 29, 30 Abs. 1 Buchstabe b und Artikel 34 Abs. 2 Buchstabe b EUV eine ausreichende Rechtsgrundlage für sämtliche Vorschriften des Vorschlags bieten. Die herangezogenen Rechtsgrundlagen im EUV betreffen die polizeiliche und justizielle Zusammenarbeit

zwischen den (Behörden der) Mitgliedstaaten. Soweit privaten Fluggesellschaften und Datenmittlern Pflichten auferlegt werden, dürften als Rechtsgrundlage eher die Artikel 80 Abs. 2 und 95 EGV in Betracht kommen. Dies macht, unbeschadet der vorgenannten grundsätzlichen Bedenken, zumindest eine Aufspaltung des Vorschlags in ein Instrument der Ersten Säule und eines der Dritten Säule erforderlich.

14. Der Rahmenbeschluss sollte eine Kostenfolgenabschätzung insbesondere über den Bedarf an Personal- und Sachmitteln (Aufgabenbindung) für die voraussichtlich bei den Mitgliedstaaten durchzuführenden Maßnahmen vorsehen.

15. Die Bundesregierung wird gebeten, auf eine entsprechende Änderung des Rahmenbeschlusses zu dringen.