Artikel 29-Datenschutzgruppe
Arbeitsgruppe Polizei und Justiz

02422/07/DE
Art 29 WP Ref: WP 145
WPPJ Ref: 01/07

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

Annahme durch die Artikel 29-Arbeitsgruppe am 5. Dezember 2007

Annahme durch die Arbeitsgruppe Polizei und Justiz am 18. Dezember 2007

Zusammenfassung

In der Stellungnahme soll untersucht werden, inwieweit sich der Kommissionsvorschlag vom 6. November 2007 für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken auf die Grundrechte und Grundfreiheiten auswirkt.

Der Vorschlag ist dem von der EU und den USA im Juli 2007 unterzeichneten PNR-Abkommen nachempfunden, das viele Ähnlichkeiten mit dem vorliegenden Vorschlag aufweist. Die datenschutzrechtlichen Bedenken, die die Artikel 29-Datenschutzgruppe in Bezug auf das PNR-Abkommen geäußert hat, decken sich in einigen Punkten mit den in dieser Stellungnahme geäußerten Bedenken. Ebenfalls berücksichtigt sind die Feststellungen der Gruppe in der Stellungnahme 9/2006 vom 27. September 2006 zur Richtlinie 2004/82/EG des Rates, die ebenfalls eine Regelung zur Übermittlung von Fluggastdaten durch Fluggesellschaften an staatliche Stellen enthält.

Die EU-Datenschutzbehörden betonen nochmals, dass sie den Kampf gegen den internationalen Terrorismus und das organisierte Verbrechen stets unterstützt haben. Es handelt sich hierbei um ein notwendiges und legitimes Anliegen und personenbezogene Daten und insbesondere Fluggastdaten können ein wertvolles Instrument zur Risikoabschätzung und zur Verhütung und Bekämpfung von Terrorismus und organisierter Kriminalität sein.
Allerdings muss bei einer europäischen Fluggastdatenregelung die Beschneidung von Grundrechten und Grundfreiheiten wohlbegründet sein und es muss das richtige Gleichgewicht zwischen dem Schutz der öffentlichen Sicherheit einerseits und der Beschränkung des Rechts auf Schutz der Privatsphäre andererseits gefunden werden.

Der geplante Rahmenbeschluss sieht die Erfassung einer großen Menge personenbezogener Daten von Flugreisenden in die und aus der EU vor, gleich, ob es sich dabei um verdächtige Personen oder unbescholtene Bürger handelt. Diese Daten werden anschließend dreizehn Jahre lang gespeichert, um unter anderem die Erstellung von Risikoprofilen zu ermöglichen. Der Vorschlag ist nicht der einzige dieser Art: neben der Vorratsspeicherung ihrer elektronischen Verbindungsdaten müssen die EU-Bürger außerdem bei Beantragung eines Passes ihre Fingerabdrücke hinterlassen[1].

Der vorliegende Vorschlag ist ein weiterer Meilenstein auf dem Weg zu einer europäischen Überwachungsgesellschaft im Namen der Terrorismus- und Kriminalitätsbekämpfung.

Nach Auffassung der EU-Datenschutzbehörden ist der Vorschlag in seiner jetzigen Form nicht nur unverhältnismäßig, sondern er verletzt auch anerkannte Datenschutzgrundsätze, wie sie in Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und in dem Europarat-Übereinkommen 108 verankert sind. Ob der Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, auf die Rechte der von dem Vorschlag betroffenen Personen anwendbar ist, ist zweifelhaft, da dieser Beschluss lediglich die Übermittlung von personenbezogenen Daten zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten, aber nicht den Datentransfer von Fluggesellschaften an die PNR-Zentralstellen der EU regelt.

[1] Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, ABl. L 385 vom 29.12.2004, S. 1.
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.
Die Richtlinien sind noch nicht in allen Mitgliedstaaten vollständig umgesetzt.

Der vorliegende Vorschlag wirft folgende datenschutzrechtlichen Fragen auf:

1 Es besteht keine akute Notwendigkeit, über die API-Daten hinaus Daten zu erfassen.
2 Die Menge der von den Fluggesellschaften zu übermittelnden Daten ist unverhältnismäßig hoch.
3 Das Herausfiltern sensibler Daten sollte den für die Datenverarbeitung Verantwortlichen überlassen bleiben.
4 Alle Fluggesellschaften sollten nach der Push-Methode verfahren.
5 Die Speicherfrist ist unangemessen lang.
6 Die Datenschutzvorschriften sind absolut unzureichend: die Rechte der betroffenen Personen und die Pflichten des für die Datenverarbeitung Verantwortlichen sind nirgends spezifiziert.
7 Die Mitgliedstaaten verfügen über einen weit reichenden Ermessensspielraum, der zu unterschiedlichen Auslegungen des Rahmenbeschlusses führen kann.
8 Unklar ist, welcher Regelung die Daten unterliegen, wenn sie an Drittstaaten weitergegeben werden.

Die EU-Datenschutzbehörden appellieren an den Rat, die Erkenntnisse und Empfehlungen dieser Stellungnahme bei der Debatte über die Annahme des Vorschlags zu berücksichtigen. Eine offene und freimütige Debatte mit allen Beteiligten, d.h. den Fluggesellschaften, den für die Buchungssysteme Verantwortlichen, den Datenschutzbehörden, dem Europäischen Parlament und den nationalen Parlamenten, ist für ein ausgewogenes Vorgehen unerlässlich.

Eine EU-Regelung zu PNR-Daten darf nicht zu einer generellen Überwachung aller Reisenden führen.

Stellungnahme der EU-Datenschutzbehörden
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

I. Allgemeine Bemerkungen

Am 6. November 2007 legte die Kommission ihren Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken vor.
Die unabhängigen Datenschutzbehörden und der Europäische Datenschutzbeauftragte halten eine sorgfältige Analyse dieses Vorschlags für erforderlich, der weit reichende Konsequenzen nicht nur für Reisende nach Europa oder aus der EU heraus, sondern auch für Fluggesellschaften, Buchungssysteme und Strafverfolgungsbehörden haben wird.

In der Vergangenheit hatte die Artikel 29-Datenschutzgruppe mehrfach Gelegenheit, sich zur Verwendung von Fluggastdaten zu Strafverfolgungszwecken zu äußern, zuletzt im Rahmen der Verhandlungen mit den USA und Kanada über ein PNR-Abkommen mit diesen Ländern. Im September 2006 äußerte sie sich außerdem ausführlich (WP 127) zu der Verpflichtung von Beförderungsunternehmen, vorab Angaben über die beförderten Personen zu übermitteln; auf diese Stellungnahme wird an dieser Stelle wiederholt zurückgegriffen werden, da der vorliegende Vorschlag und die Richtlinie 2004/82/EG deutliche Parallelen aufweisen.

Die Datenschutzgruppe unterstützte auch aktiv die während der 29. Internationalen Datenschutzkonferenz vom 26. – 28. September 2007 in Montreal, Kanada, angenommene Resolution über den dringenden Bedarf an weltweiten Standards zum Schutz von Passagierdaten, die von Regierungsstellen zu Justizvollzugs- und Grenzschutzzwecken herangezogen werden.

Im Vorfeld ihres Vorschlags konsultierte die Europäische Kommission mehrere Beteiligte wie zum Beispiel die Fluggesellschaften. Im Januar 2007 erhielt auch die Datenschutzgruppe Gelegenheit, mittels eines Fragebogens ihre Ansichten und Bedenken zum Ausdruck zu bringen. Einige der dort geäußerten Bedenken wurden in dem jetzt vorliegenden Vorschlag aufgegriffen, andere dort und in dieser Stellungnahme genannte Bedenken warten hingegen noch auf eine Reaktion und bedürfen in der Zukunft weiterhin besonderer Aufmerksamkeit.

Die EU-Datenschutzbehörden weisen darauf hin, dass bei der Bekämpfung von Terrorismus und damit zusammenhängenden Straftaten die Achtung der Grundrechte und Grundfreiheiten von Personen gewährleistet sein muss, wozu auch das Recht auf Schutz der Privatsphäre und von personenbezogenen Daten gehört. Diese Rechte sind unabdingbar. Jedwede Beschneidung dieser Rechte und Freiheiten muss wohlbegründet sein, wobei das richtige Gleichgewicht zwischen dem notwendigen Schutz der öffentlichen Sicherheit und anderen Interessen der Allgemeinheit wie dem Recht auf Schutz der Privatsphäre gefunden werden muss.

Die EU-Datenschutzbehörden möchten überdies darauf hinweisen, dass die Verwendung und Speicherung von Fluggastdaten zwar der Strafverfolgung dient, die eine unter die dritte Säule fallende Tätigkeit ist, die Fluggesellschaften diese Daten jedoch zunächst einmal für eigene, rein geschäftliche Zwecke sammeln, was wiederum Teil der ersten Säule ist.

Schließlich sei erwähnt, dass die EU-Datenschutzbeauftragten für die Beaufsichtigung der Fluggesellschaften und künftigen PNR-Zentralstellen zuständig sind und daher auch die Umsetzung des Rahmenbeschlusses überwachen müssen.

Da der Vorschlag jährlich Millionen von Reisenden berühren wird und mit weit reichenden Eingriffen in die Rechte aller Reisenden auf Schutz ihrer persönlichen Daten verbunden ist, wird das von ihm garantierte Datenschutzniveau in dieser Stellungnahme einer sorgfältigen Prüfung unterzogen. Die EU-Datenschutzbehörden stützen sich bei ihren Kommentaren zum Datenschutzniveau des Vorschlags auf anerkannte Datenschutzgrundsätze, wie sie in Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte (EMRK), in der Richtlinie 95/46/EG[2] und in dem Übereinkommen 108 des Europarates[3] verankert sind, sowie auf die von der Datenschutzgruppe zu ähnlichen Sachverhalten abgegebenen Stellungnahmen[4].

Die EU-Datenschutzbehörden stellen auch fest, dass die beabsichtigte Profilerstellung für **alle** Reisenden in einigen Mitgliedstaaten zu verfassungsrechtlichen Problemen führen könnte.

Die anerkannten Datenschutzgrundsätze gelten für den vorliegenden Vorschlag ebenso wie für jede andere Regelung, die in die Privatsphäre des Einzelnen eingreift. Die einzelnen Vorschriften des Vorschlags müssen daher

- als Reaktion auf ein bestimmtes Problem erwiesenermaßen notwendig sein
- erwiesenermaßen geeignet sein, das Problem in den Griff zu bekommen
- in einem angemessenen Verhältnis zum angestrebten Nutzen (Sicherheit) stehen
- nachweislich weniger in die Privatsphäre eingreifen als andere Optionen und
- regelmäßig darauf hin überprüft werden, ob sie noch verhältnismäßig sind.

Außerdem sollte jeder Vorschlag dieser Art den Grundsatz der Datensparsamkeit beachten, der Verwendbarkeit der Daten ausdrückliche Grenzen setzen, dem Zweck angemessene Offenlegungs- und Vorhaltungsbestimmungen enthalten, für Datengenauigkeit und die Einräumung eines Auskunfts- und Berichtigungsrechts sorgen sowie eine unabhängige Überprüfung vorsehen.

II Der Vorschlag

Vorbemerkungen

Der Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken schreibt vor, dass sämtliche Fluggesellschaften mit einem Ziel- oder Abflugflughafen in der EU die aufgelisteten

---

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.

3 Straßburger Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981.

4 Stellungnahme 5/2007 zu dem im Juli 2007 zwischen der Europäischen Union und den Vereinigten Staaten von Amerika geschlossenen Folgeabkommen über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records — PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS – US-Heimatschutzministerium) und Stellungnahme 6/2004 zur Durchführung der Kommissionsentscheidung vom 14. Mai 2004 über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Flugdatensätzen (Passenger Name Records – PNR) enthalten sind, welche dem United States Bureau of Customs and Border Protection (USCBP – Zoll- und Grenzschutzbehörde der Vereinigten Staaten) übermittelt werden, und des Abkommens zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection des United States Department of Homeland Security (US-Ministerium für Heimatschutz).

Datenelemente, sofern sie in ihrem(n) Buchungssystem(en) gespeichert sind, an die PNR-Zentralstellen übermitteln müssen, damit gegebenenfalls zu einem späteren Zeitpunkt auf sie zurückgegriffen werden kann.

Dieser Vorschlag ergänzt die Richtlinie 2004/82/EG, wonach die Fluggesellschaften bei Flügen in die EU schon jetzt verpflichtet sind, vorab Fluggastdaten (Advance Passenger Information - API) an die für die Verbesserung der Grenzkontrollen und Bekämpfung der illegalen Einwanderung zuständigen nationalen Behörden weiterzuleiten. Diese so genannte API-Richtlinie
gilt ebenfalls nicht für innereuropäische Flüge.

Die EU-Datenschutzbehörden begrüßen die Initiative der Kommission, eine Harmonisierung der Vorschriften zu erreichen, da Drittstaaten und einzelne Mitgliedstaaten bereits ihre eigenen Systeme zur Überprüfung von Passagierdaten eingeführt haben, was letztlich zu unterschiedlichen technischen Lösungen, die sich nicht miteinander vereinbaren lassen, und zu unterschiedlichen Datenschutzvorschriften führen kann. Der Vorschlag ergänzt die Vorschriften des Schengener Übereinkommens und des Visa-Informations-Systems II, beides EU-weite Instrumente zur Eindämmung krimineller Aktivitäten.

Ein Vorschlag, der Rechte und Grundfreiheiten beschneidet, muss jedoch so gestaltet sein, dass die darin vorgeschlagenen Maßnahmen nachweislich notwendig sind. Gemäß Artikel 8 der Europäischen Menschenrechtskonvention ist eine solche nachweisliche Notwendigkeit nur gegeben, wenn die geplanten Eingriffe durch ein zwingendes gesellschaftliches Erfordernis gerechtfertigt sind und mit den Grundsätzen der Verhältnismäßigkeit und Subsidiarität in Einklang stehen. Das bedeutet, dass jeder Eingriff in Rechte in Beziehung zum Zweck der Maßnahmen stehen muss und dass dieser Zweck nicht durch andere, weniger einschneidende Mittel erreicht werden kann. Die EU-Datenschutzbehörden wiederholen ihren Standpunkt, wonach die Prüfung der Notwendigkeit und Zweckgebundenheit der Maßnahmen überzeugende Argumente für den Vorschlag liefern muss. Das zwingende gesellschaftliche Erfordernis für die Erfassung und Auswertung von PNR-Daten zur Verhütung und Bekämpfung des Terrorismus und der organisierten Kriminalität ist in den Zielen des Vorschlags nicht ausführlich genug dargelegt worden. Die auf Seite 10 der Folgenabschätzung angeführten Beispiele reichen als Argumente nicht aus, um die Notwendigkeit der Erfassung und Auswertung von PNR-Daten nachzuweisen.

Die Prüfung der Notwendigkeit und Verhältnismäßigkeit des Vorschlags stützt sich bis jetzt einzig und allein auf die Erfahrungen mit der PNR-Regelung in den USA und im Vereinigten Königreich. Da das US-Abkommen bisher nur einer einzigen gemeinsamen Überprüfung unterzogen wurde und die USA nie schlüssig nachweisen konnten, dass es für die Terrorismus- und Verbrechensbekämpfung tatsächlich nötig ist, eine derart große Menge an Fluggastdaten zu erfassen, fehlt es an entsprechenden Informationen, die es problematisch, wenn nicht unmöglich machen, eine verlässliche Aussage zur Notwendigkeit, Wirksamkeit und Verhältnismäßigkeit des Vorschlags zu machen. Die einzigen gesicherten Informationen, die diesbezüglich vorliegen, deuten darauf hin, dass weniger PNR-Daten als vielmehr API-Daten verwendet werden. Außerdem soll gemäß Artikel 17 des Vorschlags der Rahmenbeschluss erst zum 31. Dezember 2010 umgesetzt werden, was nicht auf eine besondere Dringlichkeit der EU-PNR-Regelung schließen lässt.

Zu klären ist in jedem Fall, welche praktische Notwendigkeit für die Verwendung der PNR-Daten besteht und worin der Mehrwert gegenüber den drei bereits vorhandenen Varianten – SIS-, VIS- und API-Daten – besteht. Bis heute fehlt ein Beleg dafür, dass für die Bekämpfung von Terrorismus und organisierter Kriminalität andere als API-Daten nötig sind. Die EU-Datenschutzbehörden sehen sich daher außerstande, die Notwendigkeit einer EU-weiten PNR-Regelung festzustellen. Dies gilt umso mehr angesichts der Tatsache, dass die Richtlinie 2004/82/EG Fluggesellschaften die Verpflichtung auferlegt, zur Bekämpfung der illegalen Einwanderung unter anderem API-Daten zu erfassen und zu übermitteln, was in den meisten Mitgliedstaaten als Strafverfolgungsmaßnahme

eingestuft wird. Diese Richtlinie ist in einigen Mitgliedstaaten noch immer nicht voll umgesetzt, so dass bisher keine Folgenabschätzung durchgeführt werden konnte, die den Bedarf an anderen als den in Pässen enthaltenen Angaben zur Person untermauern könnte. Die EU-Datenschutzbehörden hätten sich gewünscht, dass zunächst sorgfältig analysiert wird, wie die API-Daten von den zuständigen Behörden zu den in der Richtlinie genannten Zwecken genutzt werden, bevor Bedarf an weiteren Daten angemeldet wird. Im Vorschlag selbst ist auf Seite 3 der Begründung die Rede davon, dass die API-Daten „auch dazu beitragen [**können]**, bekannte Terroristen und Straftäter (…) ausfindig zu machen". Wenn noch nicht einmal der Nutzen der API-Daten nachgewiesen werden kann, wie lässt sich dann der Rückgriff auf noch mehr Daten rechtfertigen?

Die EU-Datenschutzbehörden sind daher von der Notwendigkeit dieser folgenschweren Entwicklung nach wie vor nicht überzeugt.

In Anbetracht ihrer beratenden Funktion werden die EU-Datenschutzbehörden trotz ihres Standpunktes den Inhalt des Vorschlags analysieren, um dem Rat und anderen beteiligten Institutionen eine ausführliche Debatte hierüber zu erleichtern.

1. Wirksamkeit

Der Vorschlag beschränkt sich auf Fluggesellschaften, die Flughäfen in der EU anfliegen oder von ihnen aus starten. Alle übrigen Beförderungswege, ob per Straße, Bahn oder Schiff, beleiben ausgeklammert. Flüge innerhalb der EU sind ebenfalls ausgenommen, es sei denn, sie sind Teil eines internationalen Flugs. Dem Vorschlag zufolge liegt es nicht im Ermessen der Mitgliedstaaten, den Geltungsbereich auf nationale Flüge auszudehnen. Erfasst werden PNR-Daten von Flugreisenden, soweit sie in den elektronischen Buchungs- und Abfertigungssystemen von Fluggesellschaften gespeichert sind, was im Umkehrschluss bedeutet, dass der Vorschlag nicht für Fluggesellschaften ohne elektronische Buchungssysteme gilt. Die EU-Datenschutzbehörden fragen sich, wie der Vorschlag verhältnismäßig und effizient sein kann, wenn er nicht generell für alle Fluggesellschaften und alle sonstigen Transportmittel gilt.
Zusätzliche Angaben werden für unbegleitete Minderjährige unter 18 Jahren verlangt (siehe unten (Ziffer 8)).

2. Eingrenzung des Verwendungszecks

Der Vorschlag ermöglicht die Weitergabe von PNR-Daten über Fluggäste auf internationalen Flügen (d.h. nicht auf Flügen innerhalb der EU) durch Fluggesellschaften an die zuständigen Behörden der EU-Mitgliedstaaten zum Zwecke der Verhütung und Bekämpfung terroristischer Straftaten und von Straftaten im Rahmen der organisierten Kriminalität. Ferner ermöglicht er die Sammlung und Speicherung dieser Daten durch die genannten Behörden sowie den gegenseitigen Austausch der Daten. (Artikel 1). Eine Definition von terroristischen Straftaten und organisierter Kriminalität findet sich in Artikel 2 Buchstaben h und i).

Der Begründung und Artikel 3 des Vorschlags zufolge sind die Daten ein außerordentlich wichtiges Instrument, um Risikoanalysen vorzunehmen und neue Erkenntnisse zu sammeln. Unklar ist jedoch, wie die Daten für derartige Risikobewertungen verwendet und ob sie mit anderen den Strafverfolgungsbehörden und Nachrichtendiensten zur Verfügung stehenden Daten verglichen werden. Hierzu sind weitere Angaben nötig. Anzumerken ist ferner, dass in vielen Mitgliedstaaten Nachrichtendienste aus verfassungsrechtlichen Gründen nicht den Status einer Strafverfolgungsbehörde haben und es unklar ist, ob sie Zugriff auf die PNR-Daten haben.

3. PNR-Zentralstelle

Der Vorschlag favorisiert für die Entgegennahme personenbezogener Daten eine dezentrale Lösung gegenüber einer einzigen Stelle, an der alle Daten zusammenlaufen. Aus datenschützerischer Sicht mag eine solche dezentrale Lösung der bessere Ansatz sein; er könnte aber auch unterschiedliche Datenschutzniveaus und von Mitgliedstaat zu Mitgliedstaat divergierende technische Systeme nach sich ziehen. Bei einem dezentralen System muss sichergestellt sein, dass geeignete und übereinstimmende Schutzvorkehrungen unter Einbindung der zuständigen Aufsichtsbehörden getroffen werden. Weiterer Klärungsbedarf besteht in Bezug auf die Verteilung der Zuständigkeiten der Datenschutzbehörden in Fällen, in denen mehrere Mitgliedstaaten zusammen eine Zentralstelle einrichten.

Gemäß der in Artikel 3 des Vorschlags vorgesehenen dezentralen Lösung soll in jedem Mitgliedstaat eine PNR-Zentralstelle eingerichtet werden, die die PNR-Daten, die sie von den Fluggesellschaften oder den Datenmittlern erhält, sammelt und auswertet und die bereits erwähnte Risikoanalyse durchführt. Die Risikoanalyse soll unter Beachtung der nach innerstaatlichem Recht geltenden Kriterien und Garantien erfolgen. Es ist unklar, auf welches innerstaatliche Recht hier Bezug genommen wird und ob es sich dabei um neue oder bestehende Vorschriften handelt. Die EU-Datenschutzbehörden warnen wie schon gesagt davor, dass dieser Verweis auf nationales Recht zu einer unterschiedlichen Handhabung auf nationaler Ebene führen und das mit dem Rahmenbeschluss angestrebte Ziel einer Harmonisierung konterkarieren könnte. Nach Ansicht der EU-Datenschutzbehörden ist es daher unbedingt erforderlich, dass die Datenschutzbestimmungen der Mitgliedstaaten mit berücksichtigt und sie selbst in die Erörterung aller dieser Fragen miteinbezogen werden.

4. Zuständige Behörden

Artikel 4 verlangt von jedem Mitgliedstaat, eine Liste der zuständigen Behörden zu erstellen, die berechtigt sind, PNR-Daten von den PNR-Zentralstellen zu empfangen und zu verarbeiten. Dabei darf es sich nach Ansicht der EU-Datenschutzbehörden nur um **Strafverfolgungs**behörden handeln, die im Bereich der Verhütung und Bekämpfung von terroristischen Straftaten und der organisierten Kriminalität tätig sind. Die EU-Datenschutzbehörden weisen darauf hin, dass die zuständigen Behörden auch mehrere Funktionen, nämlich Strafverfolgungs- und nachrichtendienstliche Aufgaben, gleichzeitig wahrnehmen können. Der Vorschlag muss daher vorsehen, dass die Behörden Vorkehrungen treffen, die sicherstellen, dass nichts geschieht, was über die Zwecke des Vorschlags hinausgeht.

5. Übermittlungsverfahren

Die EU-Datenschutzbehörden begrüßen die Bestimmung in Artikel 5 des Vorschlags, wonach die Fluggesellschaften die PNR-Daten nach der Push-Methode übermitteln sollen. Dabei wäre es wichtig, dass man sich auf eine einheitliche Technik bei der Push-Methode einigt. Die Fluggesellschaften müssten dabei in jedem Fall ein Mitspracherecht haben und außerdem sollte die Meinung von Datenschutzbehörden und IT-Fachleuten eingeholt werden. Unklar ist, wie die einzelnen PNR-Zentralstellen mit außerhalb der EU niedergelassenen Fluggesellschaften umgehen sollen, die noch nicht über die technischen Möglichkeiten für ein Push-Verfahren verfügen, so dass die Daten aus vielen verschiedenen Systemen extrahiert werden müssen. Ebenso wenig ist klar, wie sie Daten von Fluggesellschaften erhalten wollen, die nicht mit elektronischen Buchungssystemen arbeiten. Auch muss geregelt werden, was geschieht, wenn Daten extrahiert werden müssen, die Fluggesellschaft eines Drittlandes der PNR-Zentralstelle eines Mitgliedstaates jedoch den Zugriff verweigert.

Der Einheitlichkeit halber sollten Fluggesellschaften verpflichtet werden, ihre Technik so bald wie möglich auf ein bestimmtes Push-System umzustellen. Die Push-Methode ist aus datenschützerischer Sicht die einzig annehmbar Vorgehensweise, weshalb die Pull-Methode auf keinen Fall parallel zum Push-System bestehen sollte. Nach Auffassung der EU-Datenschutzbehörden ist es außerdem wichtig, beim Ausbaus des Push-Systems die negativen Erfahrungen zu berücksichtigen, die die EU im Rahmen des PNR-Abkommens mit den USA bisher mit der Umstellung von der Pull- auf die Push-Methode gemacht hat. Alle technischen Fragen sollten mit sämtlichen Beteiligten vor der endgültigen Einführung des Push-Systems gelöst werden. Der Rückgriff auf das Pull-System bis zur Einführung des Push-Systems ist unbedingt zu vermeiden.

Alternative Verfahren, die weniger stark in die Privatsphäre eingreifen, wie z.B. Risikoanalysen anhand von pseudonomysierten Daten, wurden nicht in Erwägung gezogen, obwohl die Menge der an die zuständigen Behörden übermittelten personenbezogenen Daten mit Hilfe dieser Systeme drastisch reduziert werden könnte. Wenn es denn solche Verfahren schon gibt, dann sollten sie auch berücksichtigt werden.

6. Datenaustausch

Die Datenschutzbehörden halten den Verweis auf internationale Abkommen in Artikel 8 Absatz 2 und die möglichen Folgen der automatischen Gegenseitigkeit im Verhältnis zu Drittstaaten, die ein PNR-System verwenden, ebenfalls für bedenklich. Es lässt sich nicht abstreiten, dass eine europäische PNR-Regelung aufgrund des Gegenseitigkeitsprinzips auch zu PNR-Anfragen seitens undemokratischer oder korrupter Regime führen kann. Solchen Anfragen lässt sich nur schwer etwas entgegensetzen. Von daher stellt sich die Frage, ob die Folgen der Gegenseitigkeit ausreichend berücksichtigt wurden. (So können z.B. Kreditkarteninformationen, die oft Teil eines Fluggastdatensatzes sind, in den Händen eines Beamten eines Staates, der der Korruption in seinem Land nicht Herr wird, zu einem echten Problem werden. Des Weiteren können einige Staaten ein völlig anderes Verständnis vom Begriff der „Terrorismusbekämpfung“ haben als die Europäer. Das Gegenseitigkeitsprinzip könnte einer Diktatur die Möglichkeit geben, anhand von PNR-Daten eine Risikoanalyse zu Dissidenten durchzuführen. Schließlich ist nicht absehbar, wie nichtdemokratische Staaten mit den Ergebnissen einer Risikoanalyse anhand von PNR-Daten umgehen und ob die Flugreisenden diesbezüglich irgendwelche Rechte (nicht nur in punkto Datenschutz) haben.

Der Vorschlag lässt auch die Frage unbeantwortet, ob die PNR-Daten en bloc oder nur auf Einzelfallbasis an Drittstaaten übermittelt werden dürfen. Unklar ist auch, welchen Datenschutzvorschriften (in Bezug auf Speicherfristen, Weiterverbreitung, Überprüfungen und technische Sicherheit) die Daten in Drittländern unterliegen. Die Frage, wie die Personen, deren Daten erfasst werden, von der Übermittlung ihrer Daten an ein Drittland in Kenntnis gesetzt werden und wie sie ihre legitimen Rechte ausüben können, bleibt offen. Der Zugriff auf in europäischen Buchungssystemen gespeicherte Fluggastdaten durch ein Drittland mittels der Pull-Methode aufgrund des Gegenseitigkeitsprinzips ist inakzeptabel. Es wäre beispielsweise undenkbar, dass ein Land ohne Datenschutzvorkehrungen unter Berufung auf das Gegenseitigkeitsprinzip alle verfügbaren Daten über ankommende und abgehende Flüge aus dem europäischen Buchungssystem Amadeus extrahiert. All diese Probleme sollten vor der Annahme des Rahmenbeschlusses behandelt und gelöst werden. Aus datenschützerischer Sicht sollte der Datenaustausch nur auf Einzelfallbasis möglich sein.

7. Speicherfrist

Die EU-Datenschutzbehörden weisen nochmals daraufhin, dass jede Speicherfrist auf nachweislichen Datenverarbeitungsbedürfnissen beruhen, verhältnismäßig sein und im Einklang mit anerkannten Datenschutzgrundsätzen stehen muss. Letztere verlangen, dass Daten nicht länger

gespeichert werden dürfen, als dies für die Zwecke, für die sie erhoben und weiterverarbeitet werden, nötig ist. Gemäß Artikel 9 des Vorschlags werden der PNR-Zentralstelle zur Verfügung gestellte Daten für einen Zeitraum von fünf Jahren gespeichert und dann nochmals für weitere acht Jahre vorgehalten. Das macht insgesamt dreizehn Jahre. Die EU-Datenschutzbehörden sind der Ansicht, dass die Notwendigkeit der vorgeschlagenen Speicherfrist nicht hinreichend begründet wurde und dass auf den Aspekt der Verhältnismäßigkeit überhaupt nicht eingegangen wurde. Die 13jährige Speicherfrist ist somit gemessen am Zweck unverhältnismäßig und nicht akzeptabel.

Die Speicherfrist steht noch nicht einmal im Einklang mit anderen EG-Rechtsinstrumenten, die Speicherfristen für ähnliche Zwecke einführen. So müssen gemäß der Richtlinie 2004/82/EG über die Übermittlung von API-Daten die Daten 24 Stunden nach Eingang wieder gelöscht werden und die Richtlinie 2006/24/EG über die Pflichten von Anbietern elektronischer Kommunikationsdienste sieht eine Speicherfrist von maximal zwei Jahren vor.

Der Vergleich mit dem PNR-Akommen EU-USA ist wegen des offensichtlichen Fehlens der nachweislichen Notwendigkeit oder einer hinreichenden Begründung für die in dem Abkommen geforderte 15jährige Speicherfrist kein Argument.

Es sei daran erinnert, dass die Datenschutzgruppe bereits die dreieinhalbjährige Speicherfrist im ersten PNR-Abkommen mit den USA aus dem Jahr 2004 als relativ lang eingestuft hat.

Im PNR-Abkommen mit Kanada ist die Speicherfrist ebenfalls auf dreieinhalb Jahre festgelegt. Eine gemeinsame Überprüfung – die immer noch nicht stattgefunden hat – könnte Erkenntnisse hinsichtlich der Verhältnismäßigkeit dieser Speicherfrist bringen.

8. Datenelemente

Die Liste der im Anhang des Vorschlags aufgeführten Datenelemente ähnelt stark der des im Juli 2007 zwischen der EU und den USA unterzeichneten PNR-Abkommens. Sie enthält alle 19 der dort aufgelisteten Datensätze, wenn auch in leicht abgewandelter Reihenfolge. Wie bereits in der Stellungnahme WP 138 der Datenschutzgruppe zum PNR-Abkommen EU-USA ausgeführt, werden darin bestimmte Datenelemente miteinander kombiniert, die den Umstand zu verschleiern suchen, dass in Wirklichkeit nicht 19, sondern ungefähr 35 einzelne Datenelemente übermittelt werden, vorausgesetzt, diese werden von dem (den) elektronischen Buchungs- und Abfertigungssystem(en) der Fluggesellschaften erfasst.

Die EU-Datenschutzbehörden halten diese Liste der Datensätze für übertrieben, zumal nicht erläutert wird, warum so viele Datenelemente für die Bekämpfung des Terrorismus und der organisierten Kriminalität benötigt werden. Es wird offenbar als gegeben angesehen, dass die Datensätze nützlich sind, da sie von den US-Behörden für nützlich gehalten werden, doch wird ihre Notwendigkeit in dem Vorschlag nicht weiter belegt. Die EU-Datenschutzbehörden machen darauf aufmerksam, dass Datenschürfen („Data mining“) kein erklärtes Ziel des Vorschlags ist.

Zu erwähnen ist ferner, dass das Datenelement „Sprachen“ ein sensibles Datenelement sein könnte, da es die ethnische Zugehörigkeit des Minderjährigen enthüllen könnte, und als solches ohnehin gelöscht werden müsste.

Während einige PNR-Daten von den Fluggesellschaften vor Abflug in die Abfertigungssysteme eingegeben werden (z.B. Gepäckinformationen und Sitzplatznummer), werden andere Angaben vom Fluggast bei Buchung des Fluges gemacht (z.B. Reisroute und Vielfliegerdaten). Anders als API-Daten können nicht in den Abfertigungssystemen gespeicherte PNR-Daten nicht als gesicherte Informationen angesehen werden. Diese Angaben werden von jedem Fluggast bei Buchung eines Fluges freiwillig gemacht. Sie können sogar völlig willkürlich zustande kommen, wie

beispielsweise die Essenswahl. Die Fluggesellschaften sind nicht in der Lage, die Angaben auf ihren Wahrheitsgehalt hin zu überprüfen, und sind im Übrigen auch nicht dazu verpflichtet. Daher können sie auch nicht für die Richtigkeit von PNR-Daten dieser Art zur Rechenschaft gezogen werden. Abgesehen davon, dass in den meisten Fällen die Datensätze für den einzelnen Fluggast sehr begrenzt sind, sind sie ungeprüft, weshalb fraglich ist, ob sie als zuverlässige Informationsquelle zur Risikobewertung herhalten können. Die EU-Datenschutzbehörden sind daher nicht überzeugt davon, dass die Liste der erforderlichen Datenelemente für den erklärten Zweck des Vorschlags erforderlich ist. Sie halten diese Liste für überzogen und fordern daher den Rat auf, sie zu kürzen. In diesem Zusammenhang sei angemerkt, dass das PNR-Abkommen mit Kanada nur 25 Datenelemente vorsieht, die für die Bekämpfung des Terrorismus und der organisierten Kriminalität für ausreichend gehalten werden.

Eine weitere Sorge der EU-Datenschutzbehörden besteht darin, dass die Liste der Datensätze bei Angabe der Kontaktadresse, der Rechnungsanschrift oder von Einzelheiten zu den beteiligten Reisebüros im Herkunfts- und Bestimmungsland Informationen über Dritte enthalten könnte, beispielsweise über den Arbeitgeber, den Lebenspartner oder Verwandte der betroffenen Person. Diese dritte Person weiß meist gar nichts von der Übermittlung der personenbezogenen Daten an die PNR-Zentralstelle und kann daher auch nicht ihre Rechte geltend machen.

9. Herausfiltern sensibler Daten

Artikel 3 und Artikel 6 des Vorschlags sehen ausdrücklich vor, dass sensible Daten, die Aufschluss geben über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Zugehörigkeit zu einer Gewerkschaft, den Gesundheitszustand oder das Sexualleben der betreffenden Person, von der PNR-Zentralstelle oder dem Datenmittler umgehend gelöscht werden müssen. Die Datensätze in Anhang I des Vorschlags enthalten keine solchen sensiblen Daten, doch können sich letztere hinter den Datenfeldern 12 „Allgemeine Hinweise“ und 19 „Historie aller Änderungen in Bezug auf die unter den Nummern 1 bis 18 aufgeführten PNR-Daten“ verbergen. Wie schon gesagt, können auch die von einem Kind gesprochenen Sprachen Auskunft über seine ethnische Zugehörigkeit geben.

Einer der wesentlichen Grundsätze des Datenschutzes ist der, dass derjenige, der die personenbezogenen Daten verarbeitet, hierfür die Verantwortung trägt. Dies ergibt sich aus Artikel 2 Buchstabe d in Verbindung mit Artikel 6 Absatz 2 der Richtlinie 95/46/EG. Ähnliche Bestimmungen finden sich in Artikel 2 Buchstabe d sowie Artikel 5 des Übereinkommens 108. Es sollte daher Aufgabe der Fluggesellschaften sein, sensible Daten herauszufiltern, bevor sie im Wege des „Push“-Systems an einen Datenmittler oder die PNR-Zentralstelle übermittelt werden. Bevor jedoch das Herausfiltern sensibler Daten thematisiert wird, sollten zunächst triftige Gründe genannt werden, weshalb überhaupt sensible Informationen in den Datensätzen erfasst werden müssen. In diesem Zusammenhang sei nochmals darauf verwiesen, dass das PNR-Abkommen mit Kanada keine Datenelemente mit sensiblen Informationen enthält.

Deshalb widerspricht es nach Ansicht der EU-Datenschutzbehörden anerkannten Datenschutzgrundsätzen, wenn in dem Vorschlag die für die Verarbeitung Verantwortlichen, d.h. die Fluggesellschaften, von ihrer Verpflichtung zum Herausfiltern sensibler Daten, die nicht auf der Liste der verlangten Datenelemente stehen, entbunden werden.

Der Vorschlag lässt die Frage unbeantwortet, wie die Datenmittler und die PNR-Zentralstellen zu einem gemeinsamen Verständnis des Begriffs der sensiblen Daten gelangen und in dieser – nicht nur rein technischen – Frage zusammenarbeiten sollen. Überdies können sich Inhalt und Bedeutung sensibler Daten mit der Zeit ändern, weshalb kontinuierlich darauf zu achten ist, ob neue einschlägige sensible Daten auftauchen.

Die EU-Datenschutzbehörden fordern den Rat auf, die Liste der Datenelemente so zu kürzen, dass ein Herausfiltern sensibler Daten nicht mehr nötig ist. Sollte der Rat die Liste dennoch so belassen, wie sie ist, sollte das Herausfiltern sensibler Daten den Fluggesellschaften überlassen bleiben, die sich zu diesem Zweck mit ihren Aufsichtsbehörden und der Kommission ins Benehmen setzen sollten, um festzuhalten, welche Daten zu den sensiblen Daten zu zählen sind, und diese Liste auf dem Laufenden zu halten. Auf diese Weise wird den Datenschutzgrundsätzen Genüge getan und gleichzeitig ein effizientes und einheitliches Vorgehen gewährleistet.

10. Datenschutzbestimmungen

Die Datenschutzvorschriften in Artikel 11 nehmen Bezug auf den Entwurf des Rahmenbeschlusses über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Dieser Beschluss muss noch angenommen werden.

Es ist nicht klar, wie der Rahmenbeschluss über die polizeiliche und justizielle Zusammenarbeit einen geeigneten Schutz liefern soll, da sein Anwendungsbereich auf den Datenaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten beschränkt sein wird. Der vorliegende Vorschlag deckt jedoch einen anderen Bereich - die Übermittlung von Fluggastdaten durch die Fluggesellschaften an die PNR-Zentralstellen – ab. Das Fehlen klarer Datenschutzbestimmungen ist nicht hinnehmbar, so dass in diesem Punkt unbedingt Abhilfe geschaffen werden muss.

Die EU-Datenschutzbehörden halten klare, auf den besonderen Fall zugeschnittene Bestimmungen für unerlässlich, da nicht alle Mitgliedstaaten bei der Umsetzung der Richtlinie 95/46/EG in innerstaatliches Recht Polizei- und Justizbehörden miteinbezogen haben. Sie schlagen daher vor, die Datenschutzbestimmungen in den Vorschlag zu integrieren, anstatt auf ein anderes Rechtsinstrument zu verweisen. Geregelt werden sollte unter anderem, welche Rechte die betroffenen Personen besitzen, etwa das Recht auf Auskunft, Berichtigung der Daten und auf Widerspruch. Dies würde die Transparenz erhöhen und den Schutz der betroffenen Personen erleichtern.

11. Information der betroffenen Personen

Gemäß Artikel 5 Absatz 6 des Vorschlags müssen die Mitgliedstaaten dafür sorgen, dass die Fluggesellschaften die Fluggäste informieren über: die Weitergabe der PNR-Daten an die PNR-Zentralstelle (bzw. gegebenenfalls an den Datenmittler), die Zwecke der Verarbeitung, den Zeitraum ihrer Speicherung, ihre mögliche Verwertung zur Verhütung und Bekämpfung terroristischer Straftaten und der organisierten Kriminalität und die Möglichkeit des Austauschs und der gemeinsamen Nutzung der Daten.

Die EU-Datenschutzbehörden stellen mit Besorgnis fest, dass an keiner Stelle erwähnt wird, an wen sich die betroffene Person wenden kann und wie sie ihre Rechte, insbesondere das Auskunftsrecht, geltend machen kann. Eine derartige Regelung ist jedoch von grundlegender Bedeutung und deshalb empfehlen die EU-Datenschutzbehörden, entsprechende Formulierungen in den Vorschlag aufzunehmen.

Außerdem muss geregelt werden, wie die Aufsichtsbehörden der Mitgliedstaaten das Recht auf Information durchsetzen wollen und welche Sanktionen bei unzureichender Aufklärung der Fluggäste durch Fluggesellschaften, Datenmittler und PNR-Zentralstellen verhängt werden und von wem. Die Datenschutzgruppe möchte nochmals darauf verweisen, dass sie in der Vergangenheit

zwei Stellungnahmen abgegeben hat[5], die den Fluggesellschaften als Orientierung dienen und die Reisenden besser mit diesem Sachverhalt vertraut machen sollten. Wichtig ist nach Ansicht der EU-Datenschutzbehörden auch ein harmonisiertes Vorgehen, das den Bedenken aller Beteiligten Rechnung trägt.

12. Datensicherheit und Verschlüsselungsstandards

Artikel 12 befasst sich mit den Sicherheitsmaßnahmen, die von den PNR-Zentralstellen, den Datenmittlern und den zuständigen Behörden getroffen werden müssen. Der Vollständigkeit halber müsste an dieser Stelle auch ein Verweis auf die nötigen organisatorischen Maßnahmen wie Ausbildung des Personals oder Disziplinarmaßnahmen bei Nichtbeachtung der Sicherheitsvorschriften erfolgen.

Aus den Artikeln 13, 14 und 15 geht hervor, dass der in Artikel 14 genannte Ausschuss Empfehlungen zur Annahme gemeinsamer Protokolle und Verschlüsselungsstandards abgibt. Der Rahmenbeschluss sollte zudem fachliche Beratung durch erfahrene Datenschutzbehörden und IT-Spezialisten vorsehen.

Die Verwendung von Datensicherungstechniken ist von grundlegender Bedeutung und sollte daher nicht auf die lange Bank geschoben werden. Artikel 15 sollte daher auch eine Vorschrift beinhalten, wonach das Hinarbeiten auf eine gemeinsame Methode gefördert und jedwede Verzögerung bei der Sicherung des Übertragungsmodus begründet werden muss.

13. Statistische Daten

Die EU-Datenschutzbehörden begrüßen es, dass der Vorschlag Vorschriften über die Erstellung von Statistiken enthält. Informationen über die Zahl der Strafverfolgungsmaßnahmen aufgrund der Verwertung von PNR-Daten könnten sich als nützlich erweisen (und eventuell Argumente für die Notwendigkeit der Verwendung der PNR-Daten oder Änderungen an der Regelung) liefern. Es ist auch begrüßenswert, dass diese statistischen Daten keine personenbezogenen Daten enthalten dürfen. Voraussetzung hierfür ist eine korrekte und sofortige Anonymisierung. Vor Beginn der Operation sollten daher gemeinsame Regeln für die Anonymisierung erarbeitet werden.

14. Überprüfungs- und Verfallsklausel

Die EU-Datenschutzbehörden begrüßen es, dass die Kommission eine Überprüfung des Rahmenbeschlusses vornehmen wird. Bedenklich ist hingegen, dass unabhängige Aufsichtsbehörden oder externe Experten in diesem Zusammenhang keine Erwähnung finden. Die EU-Datenschutzbehörden halten jedoch eine Beteiligung ihrerseits, sei es direkt oder über Vertreter, an einer ernst zu nehmenden Überprüfung des Abkommen sowohl in der Vorbereitungs- - als auch in der praktischen Durchführungsphase für unerlässlich.
Der Vorschlag sollte klar regeln, wann und wie wird die Überprüfung vorbereitet und ausgeführt wird. Die EU-Datenschutzbehörden empfehlen nachdrücklich, dass der abschließende Bericht auch dem Europäischen Parlament vorgelegt wird.

---

[5] WP 97 „Stellungnahme 8/2004 zur Unterrichtung von Fluggästen anlässlich der Übermittlung persönlicher Daten bei Flügen zwischen der Europäischen Union und denVereinigten Staaten von Amerika“ vom 30. September 2004 und WP 132 „Stellungnahme 2/2007 zur Information von Fluggästen über die Übermittlung von PNR-Daten an amerikanische Behörden“ vom 15. Februar 2007 sowie ein „Kurzes Informationsblatt für Reisen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika“.

Die EU-Datenschutzbehörden gehen davon aus, dass jedes Jahr eine Überprüfung stattfindet und dass Empfehlungen zur Verbesserung des Systems und zu allen den Schutz der Privatsphäre betreffenden Aspekten ausgesprochen werden.

Da der Rahmenbeschluss weit reichende Konsequenzen für alle Reisenden in die und aus der EU haben wird, halten es EU-Datenschutzbehörden für erforderlich, nach Ablauf einer bestimmten Frist die Notwendigkeit dieser Regelung unter Mitwirkung unabhängiger Sachverständiger sorgfältig zu analysieren und zu überprüfen. Eine solch umfassende und ausführliche Prüfung ist im Rahmen der in Artikel 17 vorgesehenen Überprüfung nicht möglich. Die EU-Datenschutzbehörden schlagen daher vor, eine Verfallsklausel einzuführen, wonach vor einer eventuellen Verlängerung der Regelung die Effizienz und Notwendigkeit der Vorschriften des Rahmenbeschlusses sorgfältig analysiert werden müssen. Eine solche Analyse sollte gemeinsam mit unabhängigen Sachverständigen durchgeführt werden.

15. Sonstige Harmonisierungsaspekte

In dieser Stellungnahme haben die EU-Datenschutzbehörden mehrfach zu einem harmonisierten Vorgehen aufgerufen, um eine unterschiedliche Umsetzung des Rahmenbeschlusses durch die Mitgliedstaaten zu vermeiden. Auf einige Punkte wurde bisher noch nicht eingegangen.

Der Vorschlag räumt den Mitgliedstaaten die Möglichkeit ein, bi- oder multilaterale Übereinkünfte oder Abkommen zu schließen, wenn die Ziele des Rahmenbeschlusses dadurch gefördert oder leichter verwirklicht werden können. Diese Bestimmung läuft nach Ansicht der EU-Datenschutzbehörden den Zielen des Rahmenbeschlusses zuwider, der ja gerade eine Harmonisierung auf diesem Gebiet anstrebt.

In der Begründung wird außerdem explizit festgestellt, dass der Rahmenbeschluss den politischen Entscheidungsträgern in den Mitgliedstaaten bei der Umsetzung der Vorschriften größtmöglichen Spielraum lässt. Die Mitgliedstaaten können selbst entscheiden, **wie** und wo sie ihr PNR-System einrichten und wie sie es technisch ausgestalten wollen. Harmonisiert wird nur ein absolutes Mindestmaß an Details. Das ist jedoch möglicherweise nicht genug. Es steht zu befürchten, dass es in einzelnen Mitgliedstaaten zu unterschiedlichen Auslegungen kommt und Fluggesellschaften und Flugreisende mit unterschiedlichen Systemen und Standards konfrontiert sind. In diesem Zusammenhang stellen die EU-Datenschutzbehörden mit Bedauern fest, dass die Richtlinie 2004/82/EG von einigen Mitgliedstaaten noch immer nicht in allen Punkten umgesetzt wurde, obwohl die Umsetzungsfrist seit langem abgelaufen ist. Infolgedessen war es auch noch nicht möglich, die technischen und datenschützerischen Aspekte der nationalen Vorschriften zur Umsetzung der Richtlinie 2004/82/EG zu analysieren. Bisher gibt es noch nicht einmal Erfahrungswerte dazu, wie die Mitgliedstaaten ihren Ermessensspielraum genutzt haben und ob eine weitere Harmonisierung zur Umsetzung der Richtlinie nötig ist. Derartige Erfahrungen wären aber höchst willkommen, um zu sehen, wie viel Ermessensspielraum bei der Umsetzung des vorliegenden Vorschlags erforderlich und wünschenswert ist.

Die EU-Datenschutzbehörden sind der Ansicht, dass eine Situation, in der Fluggesellschaften und betroffene Personen mit unterschiedlichen Systemen und Vorgehensweisen konfrontiert sind, nicht hinnehmbar ist. Um unterschiedliche Risikobewertungen zu verhindern, plädieren sie daher für die Einsetzung eines Forums, auf dem die Mitgliedstaaten ihre Meinungen und bewährten Praktiken austauschen können. Ein solches Forum, an dem auch die Datenschutzbehörden beteiligt werden sollten, wäre der geeignete Ort, um alle sonstigen Fragen im Zusammenhang mit der Umsetzung des Rahmenbeschlusses im Einzelnen zu klären.

III. Fazit

Der Kommissionsvorschlag berührt alle Flugreisenden in die und aus der EU. Er gesellt sich zu der Verpflichtung, bei Beantragung eines Passes oder Visums seine Fingerabdrücke abzugeben, und wird gleichermaßen Auswirkungen auf die Luftfahrtindustrie, die Buchungssysteme und die Strafverfolgungsbehörden haben. Würde der Rahmenbeschluss in seiner jetzigen Form umgesetzt, wäre Europa nicht mehr weit von einer Überwachungsgesellschaft entfernt, in der jeder Reisende als Verdächtiger gilt. Wie schon bei der Vorratsspeicherung von Verbindungsdaten (Richtlinie 2006/24/EG) wird eine große Menge an personenbezogenen Daten von privaten Einrichtungen erfasst und gespeichert, um möglicherweise später von staatlichen Stellen verwertet zu werden, obwohl die Effizienz und Notwendigkeit eines solchen Systems zu keiner Zeit bewiesen wurde. Die Datenerfassung betrifft alle Reisenden, ob verdächtig oder nicht, d.h. in den meisten Fällen unbescholtene Bürger, und ermöglicht die Rekonstruktion ihrer Reisegewohnheiten über viele Jahre hinweg. Es bleiben daher ernsthafte Zweifel, ob der von der EU gewählte Ansatz, bei der Bekämpfung von Terrorismus und organisierter Kriminalität alle Flugreisenden unter Beobachtung und damit unter Generalverdacht zu stellen, der richtige Weg ist, um diesen Phänomenen Herr zu werden, zumal noch überhaupt keine Erfahrungen mit der Verwendung von API-Daten zu Strafverfolgungszwecken vorliegen.

Insgesamt gesehen sind die EU-Datenschutzbehörden der Ansicht, dass der vorliegende Vorschlag einen gemäßigteren Kurs verfolgt als frühere Regelungen zu diesem Thema und insbesondere als das jüngst unterzeichnete PNR-Abkommen EU-USA. Der Zweck des Vorschlags wurde genau umrissen und auf die Verhütung und Bekämpfung von Terrorismus und organisierter Kriminalität beschränkt. Einige der von der Datenschutzgruppe in den Antworten auf den Fragebogen vom Januar 2007 geäußerten Bedenken wurden aufgegriffen. Andere Bedenken sind jedoch noch nicht ausgeräumt, insbesondere was das nach Artikel 8 EMRK erforderliche Kriterium der Notwendigkeit des Vorschlags betrifft, die nur unzulänglich nachgewiesen ist. Anders als API-Daten sind PNR-Daten keine gesicherten Daten und damit nicht zuverlässig. Außerdem versäumt es der Vorschlag, nähere Ausführungen zu den Rechten der Flugreisenden zu machen und entsprechende Schutzvorkehrungen zu treffen. Er enthält lediglich einen Verweis auf den noch nicht verabschiedeten Rahmenbeschluss über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Auch wenn ein europäisches Vorgehen einzelstaatlichen Maßnahmen auf diesem Gebiet vorzuziehen ist, ist festzustellen, dass der Vorschlag den Mitgliedstaaten einen weit reichenden Ermessensspielraum lässt, so dass zu befürchten steht, dass der Rahmenbeschluss unterschiedlich ausgelegt und nicht einheitlich umgesetzt wird. Der Vorschlag äußert sich weder dazu, was unter Risikobewertung zu verstehen ist, noch dazu, wie die Daten zu erkennungsdienstlichen Zwecken verwendet werden sollen. Diese Punkte bedürfen einer weiteren Klärung.

Die Zahl der im Anhang aufgeführten Datenelemente ist überzogen und die Speicherfrist von dreizehn Jahren unverhältnismäßig lang.

Die EU-Datenschutzbehörden begrüßen es, dass für die Übermittlung der Daten der „Push-Methode“ der Vorzug gegeben wurde. Sie sind der Auffassung, dass die „Push-Methode" die einzig anerkannte Art der Übermittlung von Fluggastdaten sein und Fluggesellschaften aus Drittländern diesbezüglich kein Ermessensspielraum eingeräumt werden sollte. Aus datenschützerischer Sicht sollten alle Fluggesellschaften, unabhängig davon, ob sie in Europa oder anderswo niedergelassen sind, gleichbehandelt werden.

Die EU-Datenschutzbehörden vermerken positiv, dass sensible Daten herausgefiltert werden müssen, beharren aber darauf, dass diese Aufgabe den für die Verarbeitung Verantwortlichen und nicht Dritten überlassen werden sollte. Die Datenschutzbehörden müssen allein schon wegen der Erfahrungen, die sie aufgrund ihrer Beteiligung an den Aktivitäten der gemeinsamen

Kontrollinstanzen der „dritten Säule” gesammelt haben, an der Definition sensibler Daten beteiligt werden.

In Anbetracht der aufgezählten Mängel und der Tragweite der Maßnahme, die einschneidende Auswirkungen auf den Datenschutz hat, halten die EU-Datenschutzbehörden eine ernsthafte Debatte unter Einschluss des Europäischen Parlaments, der nationalen Parlamente und aller an der Entwicklung eines solchen Systems beteiligten Akteure, vor allem der Luftfahrtbranche und der Betreiber von Buchungssystemen, für unerlässlich. Eine ausgewogene, datenschutzverträgliche Lösung ist umso wichtiger, als eine künftige europäische PNR-Regelung aufgrund des politischen und ökonomischen Gewichts der EU einen Präzedenzfall für andere Länder in der Welt schaffen würde, die noch über die Einführung einer ähnlichen Regelung nachdenken und dem europäischen Beispiel folgen könnten. Die EU sollte diese Gelegenheit nicht verpassen und deshalb mit hohen Datenschutzstandards aufwarten.

Die EU-Datenschutzbehörden werden weiterhin Input und fachlichen Beistand liefern. In ihrer Eigenschaft als unabhängige Beratungsgremien auf dem Gebiet des Datenschutzes stehen sowohl die Artikel 29-Datenschutzgruppe als auch die Arbeitsgruppe Polizei und Justiz der Kommission und dem Rat jederzeit zur Verfügung. Die Artikel 29-Datenschutzgruppe erwartet, dass sie an der Umsetzung des Rahmenbeschlusses beteiligt wird, da der Beschluss Auswirkungen auf Fluggesellschaften hat, die bereits Pflichten gemäß der Richtlinie 95/46/EG haben.

Brüssel, den
5. und 18. Dezember 2007

Für die Artikel 29-Datenschutzgruppe	*Für die Arbeitsgruppe Polizei und Justiz*
Der Vorsitzende	Der Vorsitzende
Peter SCHAAR	Francesco PIZZETTI