Anlage

Betrifft: Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdaten für die Verhinderung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (**Richtlinie EU-PNR**)

Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner **204. Sitzung am 28. Februar 2011 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1. Vorgeschichte

Die Europäische Kommission legte am 2.2.2011 den **Vorschlag für eine Richtlinie über die Verwendung von Fluggastdatensätzen** (PNR) durch die Strafverfolgungsbehörden vor. Dieser Vorschlag geht zurück auf frühere Initiativen, darunter zuletzt der vor In-Kraft-Treten des Vertrags von Lissabon von der Kommission eingebrachte Vorschlag für einen Rahmenbeschluss zur Einführung eines EU-PNR-Systems (KOM (2007) 654).

Zu diesem Vorschlag für einen Rahmenbeschluss hat sich der Datenschutzrat bereits in seiner 180. Sitzung (vom 5.3.2008) und seiner 184. Sitzung (vom 19.11.2008) **kritisch und ablehnend geäußert**. Er hat den beteiligten Bundesministerien (darunter dem als ressortzuständig federführenden BMI) empfohlen, auf europäischer Ebene gegen die genannte Initiative einzutreten.

2. Wesentlicher Regelungsinhalt

Der nunmehrige Richtlinien-Vorschlag sieht – im Wesentlichen ähnlich wie der oben genannte Rahmenbeschluss – kurz gefasst Folgendes vor:

1. Flugunternehmen speichern Passagierdaten von Fluggästen auf **internationalen Flügen**, die im Hoheitsgebiet der Mitgliedstaaten ankommen und von dort abgehen (Vorschlag GB: Ausweitung auf EU-interne Flüge).

2. Verpflichtende Übermittlung dieser Passagierdaten **24 Std vor Abflug und unmittelbar bei Abfertigung** des Fluges von den Fluggesellschaften an eine auf Mitgliedstaatsebene jeweils national einzurichtende PNR-Stelle (oder gemeinsame PNR-Stelle mehrerer Mitgliedstaaten).

3. Speicherung dieser Passagierdaten bei der nationalen PNR-Stelle (oder gemeinsamen PNR-Stelle) für **30 Tage vollinhaltlich** und danach **5 Jahre in „maskierter" Form** (dh verschlüsselt, wobei der Schlüssel zur Entschlüsselung bei der nationalen PNR-Stelle verbleibt).

4. Verwendung der Daten ausschließlich zur Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von **terroristischen Straftaten und schwerer Kriminalität** (Vorschlag von mehreren Mitgliedstaaten: Ausdehnung auf weitere Verwendungszwecke).

5. Auf die Passagierdaten soll zum einen **zeitnah vor, während oder nach dem Flug zugegriffen** werden dürfen, um gesuchte Personen ausfindig zu machen; zu jedem späteren Zeitpunkt innerhalb der 5 Jahre, um die Daten zu strafrechtlichen Zwecken zu durchsuchen, allenfalls auf Anfrage einer anderen Behörde bzw. von Behörden eines anderen Staates (Art. 4 Abs. 2 lit. d, Art. 9 Abs. 2 des Entwurfs).

6. Weiters sollen die zunächst nur „maskiert" (dh mit verschlüsseltem Personenbezug) gespeicherten Daten für Auswertungen verwendet werden, um in der Folge bestimmte **Verhaltensmuster** von typischerweise verdächtigen Personen oder Personengruppen zu analysieren, und um Kriterien zu entwickeln, mit deren Hilfe Personen, die ein vergleichbares Verhalten an den Tag legen, einer näheren behördlichen „Überprüfung" unterzogen werden können. Das „impact assessment" der Kommission fasst diese Funktion zusammen wie folgt: *"For example, an analysis of PNR data may give indications on the most usual travel routes for trafficking*

people or drugs which can be made part of assessment criteria. By checking PNR data in real-time against such criteria, crimes may be prevented or detected."

3. Voraussichtlicher Zeitplan

Der Vorschlag wird dem Rat während der Tagung der Justiz- und Innenminister am 24. und 25.2.2011 von der Kommission vorgestellt. Am 3.3.2011 soll der Vorschlag bereits inhaltlich in der Ratsarbeitsgruppe GENVAL behandelt werden.

4. Bisherige österreichische Position

Auf europäischer Ebene wurde von Österreich (BMI) der Standpunkt eingenommen, dass ein dezentrales System (dh jeder Mitgliedstaat oder mehrere Mitgliedstaaten gemeinsam richten PNR-Stelle ein) nicht wünschenswert sei und dass ein EU-weit zentrales PNR-System vorzuziehen sei, weil es einen größeren „Mehrwert" habe (so zusammengefasst die vom BMI zuletzt in der Sitzung des CATS am 10. Und 11.2.2011 vertretene Position).

5. Datenschutzrechtliche Überlegungen zum vorgeschlagenen EU-PNR-System

5.1 Allgemeines

Die Speicherung der persönlichen Daten aller Flugreisenden, unabhängig von jedem Verdacht, ist ein Eingriff in die Privatsphäre, der aus dem Gesichtspunkt des Grundrechts auf Privatleben und auf Datenschutz (Art. 8 EMRK sowie Art. 7 und 8 der Grundrechtecharta) nur zulässig ist, wenn er gesetzlich vorgesehen, im öffentlichen Interesse unbedingt notwendig und verhältnismäßig ist.

5.2. Eignung und Notwendigkeit

Wenn ein Rechtsakt derart schwere Grundrechtseingriffe vorsieht, **muss die Eignung und dringende Notwendigkeit dieser Eingriffe konkret belegt** sein.

Der nunmehrige 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.

Der Informationsgehalt von PNR Daten geht über den Inhalt von API Daten jedoch weit hinaus. Gleichzeitig ist die Zuverlässigkeit von PNR-Daten nicht nachprüfbar, weil es sich dabei nur um jene Angaben handelt, die der Betroffene der Fluggesellschaft bekannt gegeben hat.

Empirische, objektive Daten, die die Notwendigkeit einer EU-weiten Verwendung (einschließlich der 5-jährigen Speicherung) von PNR-Daten zur Erreichung von Zielen im Interesse der öffentlichen Sicherheit oder den Mehrwert zu bereits bestehenden Datensammlungen belegen, wurden bisher nicht konkret vorgebracht (vgl in diesem Zusammenhang auch die Ausführungen des EDSB vom 20. Dezember 2007 und der Artikel 29-Gruppe vom 5. Dezember 2007 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp145_de.pdf, zuletzt auch die Stellungnahme der Artikel 29-Gruppe zur Mitteilung der Europäischen Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen an Drittländer, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp178_de.pdf.

Die Artikel 29-Gruppe stellt in ihren Stellungnahmen wiederholt fest, dass auch die von der Kommission erwähnten Pilotstudien keine Rückschlüsse auf die Notwendigkeit, Effizienz und Verhältnismäßigkeit des Einsatzes von PNR-Daten erlauben. Sie geht vielmehr davon aus, dass die verfügbaren Informationen über Anwendungsfälle in erster Linie auf einen Einsatz von API-Daten als von PNR-Daten hindeuten (vgl S. 6 der Stn. der Artikel 29-Gruppe vom 5.12.2007).

Der zuweilen – unsubstantiiert – vorgebrachte „Mehrwert“ der Behörden bei der „Überwachung“, den die Schaffung einer solchen staatlichen Datenbank darstellt, ist für sich allein betrachtet und ohne eine eingehende Verhältnismäßigkeitsprüfung kein hinreichender Grund für die rechtliche Zulässigkeit eines Grundrechtseingriffs.

Bisweilen wird auch auf den Umstand hingewiesen, dass andere Staaten (Großbritannien, Frankreich, USA) bereits PNR-Systeme nutzen. Auch dieser Hinweis kann mangels näherer Angaben zu diesen Systemen aber weder den Nachweis erbringen, dass die Maßnahme für die gesamte Europäische Union geeignet bzw. zwingend erforderlich ist, noch kann er belegen, dass diese Systeme der Speicherung und Datenverarbeitung mit der Grundrechtsordnung (EMRK, Grundrechte-Charta) vereinbar sind.

Auch ist zu bezweifeln, ob die Auswertung von Daten, die ausschließlich auf eigenen Angaben der Betroffenen beruhen, geeignet ist, Kriminelle ausfindig zu machen.

Zusammenfassend ist somit festzuhalten, dass die äußerst kurz gehaltenen **Ausführungen der Europäischen Kommission** im vorliegenden Vorschlag zur Eignung bzw. Effizienz und Notwendigkeit eines derartigen EU-PNR Systems **weder die grundsätzliche Eignung des Systems noch die Notwendigkeit** der mit dem Vorschlag verbundenen massiven Eingriffe in das Grundrecht auf Datenschutz unzähliger (unschuldiger) Personen überzeugend **nachweisen können.**

5.3 Zur Verhältnismäßigkeit

5.3.1 Vorhersehbarkeit des Grundrechtseingriffs

Ebenso wie die grundsätzliche Speicherung ist jede **weitere Verarbeitung** (Abgleich, Suchanfrage, Verknüpfungen, etc) aber auch jede Weitergabe dieser in einer Datenbank gespeicherten Daten eine weitere, schwerwiegend in die Privatsphäre der (auch der unschuldigen) Betroffenen eingreifende Maßnahme. Sie bietet dem Staat die Möglichkeit, ohne dem Wissen der Betroffenen durch Kategorisierung oder Verknüpfung den privaten Lebenswandel der Personen zu untersuchen. Auch diese einzelnen Verarbeitungsschritte wären grund- und menschenrechtlich unzulässig, wenn sie nicht im Einzelfall notwendig und verhältnismäßig sind.

Hinsichtlich der **Funktionsweise des Europäischen PNR-Systems ergibt sich** aus dem Entwurf **nicht, welche Daten** (in Echtzeit) mit welchen europäischen oder

nationalen Datenbanken (und auf Basis welcher vordefinierter „Kriterien“ bzw. Risikoanalysen) **abgeglichen** werden sollen (Art. 4 Abs. 2). Ein Abgleich sämtlicher Passagierdaten im Rahmen von Risikoanalysen von unbescholtenen Bürgern stellt einen massiven Eingriff in die Privatsphäre des Einzelnen dar. Ein solch umfassender und im Vorfeld nicht festgelegter Abgleich wäre unverhältnismäßig und aus datenschutzrechtlicher Sicht abzulehnen. Darüber hinaus muss ein Abgleich von Daten **nach bestimmten „Kriterien“ gesetzlich vorgesehen** sein.

Das Grundrecht auf Achtung der Privatsphäre verlangt, dass ein Eingriff in die Privatsphäre durch den Staat "gesetzlich vorgesehen" sein muss. Das bedeutet, dass der Betroffene bereits auf Grund der gesetzlichen Regelung in der Lage sein muss, im Vorhinein abzuschätzen, welche Verarbeitungsschritte der Staat mit seinen Daten unternimmt. Dies wäre daher in der Richtlinie konkret zu regeln, damit Bürger erkennen können, in welcher Form und in welchem Umfang diese Daten verwendet werden. **Diesen Erfordernissen genügt die Richtlinie in der vorliegenden vorgeschlagenen Fassung jedoch nicht.**

5.3.2 Speicherung durch staatliche Stelle

Ein Grundrechtseingriff wiegt **umso schwerer, als** die Speicherung a.) nicht beim Flugunternehmen selbst, sondern durch den Staat erfolgt, b.) für eine Dauer von 5 Jahren (vgl. die kürzere Dauer in der Richtlinie zur Vorratsdatenspeicherung), und c.) nicht auf den Zweck der Terrorismusbekämpfung beschränkt ist, sondern auch für weitere Zwecke wie die Bekämpfung „schwerer“ Kriminalität eingesetzt werden soll (vgl. Art. 2 lit. h und i des Richtlinienentwurfs).

Damit **übersteigt** die Schwere des Eingriffs im vorliegenden Fall wesentlich jenen **Grad der Intensität**, der bei der Vorratsdatenspeicherungs-Richtlinie (RL 2006/24/EG) festzustellen ist, die ihrerseits bereits an die Grenzen des datenschutzrechtlich Zulässigen stößt: Das Urteil des deutschen Bundesverfassungsgerichts zur Vorratsdatenspeicherung wies ausdrücklich auf den Umstand hin, dass die Vorratsdatenspeicherung nur deshalb nicht verfassungswidrig war, weil die Datensammlung nicht beim Staat sondern nur bei den einzelnen

Unternehmen erfolgt, weil keine Inhaltsdaten erfasst und nur eine Speicherdauer von 6 Monaten vorsieht (BVerfG 2.3.2010, 1 BvR 256/08 ua.).

Vor diesem Hintergrund erscheint die **Zulässigkeit einer staatlichen Sammlung aller Fluggastdaten im Hinblick auf grundrechtliche Schranken zweifelhaft**. Es ist darauf hinzuweisen, dass die Vorratsdatenspeicherungsrichtlinie nicht zuletzt vor dem Hintergrund grundrechtlicher Bedenken derzeit von der Europäischen Kommission evaluiert wird.

5.3.3. Länge der Speicherfristen

Die Speicherung der Passagierdaten bei der nationalen PNR-Stelle (oder gemeinsamen PNR-Stelle) erfolgt gemäß dem vorliegenden Vorschlag für 30 Tage vollinhaltlich und danach 5 Jahre in „maskierter“ Form (dh verschlüsselt, wobei der Schlüssel zur Entschlüsselung bei der nationalen PNR-Stelle verwahrt bleibt).

Die in Art. 9 vorgesehene Maskierung soll – zumindest vorerst – den Personenbezug in den Datensätzen beseitigen. Die in Ziffer 2 dieser Bestimmung dazu vorgesehenen zu schwärzenden Datenkategorien erscheinen aber zu wenig weitreichend, zumal offenbar Datenarten nach Ziffer 6 oder 8 des Annex bestehen bleiben würden und damit die Beseitigung des Personenbezugs nicht sichergestellt wäre.

Im Lichte der obigen Bezugnahmen zur Vorratsdatenspeicherungs-Richtlinie erscheint eine **derart lange Speicherfrist** mangels des Nachweises der Notwendigkeit derartiger Fristen im Richtlinienvorschlag als **unverhältnismäßig**.

5.3.4 Präventive und unabhängige Kontrolle

Eine Regelung, die eine 5-Jährige Speicherung und Zugriffsmaßnahmen vorsieht, ist nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte jedenfalls unzulässig, wenn sie Bestimmungen vermissen lässt, die sicherstellen,

dass in jedem Einzelfall eine angemessene und **wirksame Kontrolle** gegen Missbrauch vorgesehen ist (EGMR Fall *Rotaru* gg. Rumänien, 28341/95, § 59 mwN). Das Prinzip der Rechtsstaatlichkeit verlangt unter anderem, dass der jeweilige Eingriff durch Behörden in das Recht der Betroffenen (Datei-Abfrage, Verknüpfung, etc.) **einem wirksamen Kontrollmechanismus unterstellt wird**, der im Regelfall von **den Gerichten oder einer unabhängigen Stelle** wahrzunehmen ist (so der 8 EGMR im Fall *Rotaru* gg. Rumänien, 28341/95, § 59, und im Fall *Klass* gg. Deutschland 6.9.1978, § 55).

Gegen die Einrichtung derartiger Mechanismen lässt sich auch nicht ins Treffen führen, dass es aus kriminaltaktischen oder praktischen Gründen nicht möglich ist, die Betroffenen vom Eingriff zu informieren: Die Rechtsordnungen der Mitgliedstaaten bieten vielfach Beispiele für derartige Kontrollmechanismen, die speziell auf solche Durchsuchungsmaßnahmen abzielen, die dem Betroffenen zunächst nicht bekannt gegeben werden können. Zu nennen sind etwa die richterliche Vorabkontrolle von Abhörmaßnahmen oder von Maßnahmen der Rasterfahndung sowie Einrichtungen wie jene eines unabhängigen Rechtsschutzbeauftragten, der die Abfrage vorab genehmigen und Rechtsmittel zum Schutz der Betroffenen ergreifen kann.

Im Lichte des Grundrechts auf Achtung der Privatsphäre (Art. 8 EMRK) ist eine solche unabhängige Kontrolle im Einzelfall **unabdingbar**.

Die Zwischenschaltung eines wirksamen und unabhängigen Kontrollmechanismus wäre somit sowohl im Zusammenhang mit Zugriffsfragen von innerstaatlichen Behörden erforderlich (Art. 4 Abs. 2 lit. c iVm Art. 9 Abs. 2 des Vorschlags) als auch im Zusammenhang mit Zugriffen aufgrund von Anfragen von oder Übermittlungen an andere(n) Staaten nach Art. 7 des Vorschlags (z.B. durch einen unabhängigen Rechtsschutzbeauftragten oder eine unabhängige Kontrollbehörde).

Zusammenfassend ist festzuhalten, dass der vorliegende Richtlinienentwurf **keine Grundlage für eine unabhängige Vorabkontrolle** der Grundrechtseingriffe schafft. Die Verhältnismäßigkeit des im Richtlinienentwurf vorgesehenen

Grundrechtseingriffs ist daher auch deswegen nicht gegeben, weil die im Entwurf enthaltenen **Kontroll- und Rechtsschutzmechanismen nicht unabhängig und nicht wirksam** erscheinen.

6. Schlussfolgerungen

Das Vorhaben der Einführung eines EU-PNR-Systems iSd vorliegenden Kommissionsvorschlags ist aus datenschutzrechtlicher Sicht **kritisch zu beurteilen**. Da es den Mitgliedstaaten bisher unionsrechtlich freistand, nationale PNR-Systeme zu unterhalten, ist nicht ersichtlich, woraus sich die Notwendigkeit für eine verpflichtende Einführung derartiger Systeme verbunden mit gravierenden Grundrechtseingriffen im Wege einer Richtlinie für alle Mitgliedstaaten ergeben soll (Subsidiarität).

In den Verhandlungen auf Europäischer Ebenen wäre durch das **federführend zuständige Ressort sicherzustellen**, dass umfassende **Darlegungen zur Eignung und Notwendigkeit** des EU-PNR-Systems nachgereicht werden. Ebenfalls wäre darauf hinzuwirken, dass hinsichtlich der Vorhersehbarkeit des Grundrechtseingriffs, dem Faktum der auf staatlicher Ebene erfolgenden Speicherung der Daten und hinsichtlich der Länge der Speicherfristen **verhältnismäßige Lösungen gefunden** werden. Der Vorschlag muss um **Kontrollmechanismen**, die eine unabhängige und wirksame Kontrolle des behördlichen Vorgehens gewährleisten, ergänzt werden.

Sollten diese Ergänzungen zur Darlegung der Eignung und Notwendigkeit sowie die Sicherstellung der Gewährleistung der Verhältnismäßigkeit **nicht erreichbar und die Kostenfrage nicht geklärt sein**, wird dem federführend zuständigen Ressort neuerlich (vgl. schon die Stellungnahmen des Datenschutzrates vom 11.3.2008, GZ BKA-817.324/0002-DSR/2008, sowie vom 28.11.2008, GZ 817.324/0005-DSR/2008) empfohlen, auf europäischer Ebene **gegen die genannte Initiative einzutreten**.