ARTIKEL-29-DATENSCHUTZGRUPPE

10019/04/DE
WP 87

Stellungnahme 2/2004 zur Angemessenheit des Schutzes der personenbezogenen Daten, die in den Fluggastdatensätzen (Passenger Name Records - PNR) enthalten sind, welche dem United States Bureau of Customs and Border Protection (US CBP - Zoll- und Grenzschutzbehörde der Vereinigten Staaten) übermittelt werden sollen

angenommen am 29. Januar 2004

Stellungnahme 2/2004 zur Angemessenheit des Schutzes der personenbezogenen Daten, die in den Fluggastdatensätzen (Passenger Name Records - PNR) enthalten sind, welche dem United States Bureau of Customs and Border Protection (US CBP - Zoll- und Grenzschutzbehörde der Vereinigten Staaten) übermittelt werden sollen

DIE GRUPPE FÜR DEN SCHUTZ NATÜRLICHER PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN -

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 sowie Artikel 30 Absatz 1 Buchstabe a und Absatz 3 der Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere auf Artikel 12 und 14 -

hat folgende Stellungnahme angenommen:

EINFÜHRUNG

Nach den Ereignissen des 11. September 2001 erließen die USA eine Reihe von Gesetzen und Verordnungen, die Fluggesellschaften bei Flügen in ihr Hoheitsgebiet dazu verpflichten, den US-Behörden personenbezogene Daten über einreisende oder ausreisende Fluggäste und Besatzungsmitglieder zu übermitteln. Insbesondere müssen die Fluggesellschaften dem US Bureau of Customs and Border Protection (US CBP - Zoll- und Grenzschutzbehörde der Vereinigten Staaten) bei Flügen von den, in die und durch die USA elektronischen Zugang zu den im so genannten Passenger Name Record (PNR) enthaltenen Fluggastdaten gewähren. Fluggesellschaften, die diesen Forderungen nicht nachkommen, müssen mit hohen Geldstrafen oder sogar dem Entzug der Landerechte, ihre Passagiere mit Verspätungen bei der Ankunft in den USA rechnen.

Die Arbeitsgruppe gab im Oktober 2002 eine erste und am 13. Juni 2003 eine zweite Stellungnahme ab. Die Stellungnahme vom 13. Juni berücksichtigte die Verpflichtungserklärung der USA vom 22. Mai 2003 („Verpflichtungserklärung des United States Bureau of Customs and Border Protection und der United States Transportation Security Administration“) und entsprach damit dem letzten Stand des Dialogs hinsichtlich der Zugeständnisse auf amerikanischer Seite in Bezug auf die Bedingungen für die Verarbeitung von PNR-Fluggastdaten durch die US-Behörden

In der Stellungnahme vom 13. Juni wies die Arbeitsgruppe auf mehrere Datenschutzprobleme in Zusammenhang mit der Weitergabe von PNR-Fluggastdaten an die US-Behörden hin. Dabei ging es in erster Linie um den Zweck der Übermittlung; den Grundsatz der Verhältnismäßigkeit in Bezug auf die zu übermittelnden personenbezogenen Daten sowie den Zeitpunkt der Übermittlung und die Dauer der

[1] Amtsblatt L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/internal_market/de/dataprot/law/index.htm

Datenspeicherung; die Verarbeitung sensibler Daten; die Bedeutung eines „Push"-Verfahrens für die Übermittlung; die strenge Kontrolle der Weiterübermittlung an andere Behörden in den Vereinigten Staaten oder in anderen Ländern; die Garantien für die betroffenen Personen und ihre Rechte; den Durchsetzungs- und Streitbeilegungsmechanismus sowie die Verbindlichkeit der Verpflichtungen.

Vor kurzem erhielt die Datenschutzgruppe die Mitteilung der Kommission an den Rat und das Parlament „Übermittlung von Fluggastdatensätzen (PNR): Ein sektorübergreifendes EU-Konzept"[2] sowie eine aktualisierte Fassung der US-Verpflichtungserklärung, datiert vom 12. Januar 2004 (Anhang I).

Wie Datenschutzgruppe in der Stellungnahme 4/2003 erklärt hat, hält sie es für sinnvoll, im Lichte der jüngsten Entwicklungen in Bezug auf die Übermittlung von PNR-Fluggastdaten, und insbesondere angesichts der Ergebnisse der Verhandlungen zwischen der Europäischen Kommission und den US-Behörden, eine neue Stellungnahme abzugeben.

1. BEKÄMPFUNG DES TERRORISMUS UND SCHUTZ VON GRUNDRECHTEN UND GRUNDFREIHEITEN

Wie bereits in den Stellungnahmen 6/2002 und 4/2003 festgestellt wurde, weckt die Übermittlung von Daten an die US-Behörden Besorgnis in der Öffentlichkeit; sie hat neben einer internationalen Dimension weitreichende und heikle politische und institutionelle Implikationen.

Die Terrorismusbekämpfung ist ein notwendiges und nützliches Element einer demokratischen Gesellschaft. Indessen muss beim Kampf gegen den Terrorismus die Achtung der Grundrechte und Grundfreiheiten des Einzelnen, zu denen auch der Schutz der Privatsphäre und der Datenschutz gehören, gewährleistet sein.

Diese Rechte werden insbesondere durch die Richtlinie 95/46/EG, Artikel 8 der Europäischen Menschenrechtskonvention und Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union geschützt. Außerdem wird das Recht auf Datenschutz im Entwurf einer Europäischen Verfassung, die der Konvent für die Zukunft Europas vorgelegt hat, anerkannt und ausgedehnt.

Deshalb sollten Grundrechte und Grundfreiheiten, die sich aus den Datenschutzgrundsätzen ableiten, welche für die Verarbeitung personenbezogener Daten in der Europäischen Union gelten, nur eingeschränkt werden, wenn es in einer demokratischen Gesellschaft aus Gründen des Allgemeininteresses, wie sie abschließend in den betreffenden Rechtstexten aufgeführt sind, notwendig ist.

Hier geht es um private Daten, die für gewerbliche Zwecke erhoben worden und in den Datenbanken und den damit verknüpften Reservierungssystemen von Fluggesellschaften erfasst sind, die Flüge von der EU nach den oder durch die USA anbieten. Dass diese privaten Daten an eine staatliche Behörde weitergegeben werden, indem der Behörde Zugriff auf derartige Systeme ermöglicht wird, ist beispiellos in den Beziehungen

[2] KOM(2003) 826 endg.

zwischen der EU und den USA und stellt eine Abweichung vom Datenschutzgrundsatz der Zweckbindung dar, wenn man den Umfang und die Sensibilität der betroffenen Daten bedenkt und die Zahl der von der US-Forderung betroffenen Passagiere, nämlich mindestens 10 bis 11 Millionen pro Jahr. Das verdeutlicht, wie wichtig es ist, umsichtig vorzugehen und auch die Möglichkeiten im Auge zu behalten, die dies für das Data Mining, insbesondere in Bezug auf in Europa ansässige Personen, eröffnet, sowie die damit verbundene Gefahr einer allgemeinen Überwachung und Kontrolle durch ein Drittland.

Hinzu kommt, dass mehrere andere Drittländer bereits ähnliche Datenübermittlungen von Fluggesellschaften gefordert und/oder vorgeschlagen haben. Das wirft die Frage nach der Gleichbehandlung von Drittländern und der Notwendigkeit eines globalen Ansatzes für die Verwendung von Fluggastdaten für Sicherheitszwecke in einem multilateralen Kontext auf.

Es ist nicht bewiesen, dass sich der Terrorismus wirksamer bekämpfen und die innere Sicherheit besser gewährleisten lässt, wenn die Grundsätze der Verhältnismäßigkeit und der Datensparsamkeit nicht ordnungsgemäß berücksichtigt werden; wohingegen die Beachtung dieser Grundsätze eine wesentliche Garantie für den Schutz der Rechte der Bürger darstellt und auch für die wirtschaftliche Entwicklung vorteilhafter ist.

In diesem Zusammenhang stellt die Datenschutzgruppe fest, dass die Übermittlung von PNR-Fluggastdaten mittlerweile auch für anderer Länder Bedeutung erlangt hat, was einen globalen, weltweit einheitlichen Ansatz verlangt, der eine Harmonisierung der für verschiedene Länder in Betracht gezogenen Lösungen bewirkt.

Die Datenschutzgruppe stellt außerdem fest, dass die in jüngster Zeit in einigen Ländern, beispielsweise Australien, gesammelten Erfahrungen zeigen, dass es möglich ist, die legitimen Ziele der inneren Sicherheit und der Bekämpfung des Terrorismus unter Beachtung des Grundsatzes der Verhältnismäßigkeit mit angemessenen Mitteln zu verfolgen, und zwar mit Systemen, die die Grundanforderungen des Schutzes der Privatsphäre und des Datenschutzes erfüllen.

2. GEPLANTE RECHTSAKTE

Die Datenschutzgruppe schließt aus der Mitteilung der Kommission, dass diese der Auffassung ist, es sollte eine solide Rechtsgrundlage für die Übermittlung und von PNR-Fluggastdaten an die US-Behörden geschaffen werden in Form einer Entscheidung der Kommission nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG in Verbindung mit einem internationalen Abkommen, das es den Fluggesellschaften ermöglicht, die Forderungen der Vereinigten Staaten wie gesetzliche Erfordernisse in der EU zu behandeln, und die USA zur Gegenseitigkeit verpflichtet und dazu, ordnungsgemäße Verfahren für in der EU ansässige Personen zu gewährleisten. Deshalb fasst die Kommission den Abschluss eines „einfachen bilateralen Abkommens“ („light bilateral agreement”) mit den Vereinigten Staaten ins Auge.

Da keine einschlägigen Unterlagen vorliegen, kann die Datenschutzgruppe, auch im Hinblick auf die Zuständigkeit der Mitgliedstaaten für die Anwendung der Artikel 6 und 7 der Richtlinie 95/46, keine Stellungnahme zum Inhalt, zur etwaigen Rechtsgrundlage und zum Wert eines solchen Abkommens abgeben.

Die Datenschutzgruppe legt allerdings Wert auf die Feststellung, dass Entscheidungen der Kommission nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG eigentlich auf die Angemessenheit des Schutzes der in ein Drittland übermittelten personenbezogenen Daten abstellen, und dass die Entscheidungen bisher in der Regel die Übermittlung an privatwirtschaftliche Stellen in Drittländern betraf. Im vorliegenden Fall findet die Übermittlung erstmalig aufgrund gesetzlicher Auflagen eines Drittlands statt, die Wirtschaftsteilnehmer in der EU verpflichten, Daten an eine staatliche Behörde in diesem Drittland zu übermitteln, und zwar in einer Weise, die nicht richtlinienkonform ist.

Um eine tragfähige Rechtsgrundlage für diese Übermittlungen zu schaffen, wird eine Angemessenheitsentscheidung in Verbindung mit einem internationalen Abkommen ins Auge gefasst. Dieses Paket soll eine Reihe von Rechtswirkungen entfalten. Die Datenschutzgruppe stellt fest, dass das internationale Abkommen dazu dienen soll, eine Einschränkung des Rechts auf Privatsphäre oder eine Beschränkung des Zweckbindungsgrundsatzes nach Artikel 6 der Richtlinie zu legitimieren; deshalb vertritt sie die Auffassung, dass sich dieses Abkommen unbedingt innerhalb der Grenzen von Artikel 8 der Europäischen Menschenrechtskonvention sowie von Artikel 13 der Richtlinie bewegen sollte.

3. GELTUNGSUMFANG DER ANGEMESSENHEITSENTSCHEIDUNG UND EINES MÖGLICHEN ABKOMMENS: CAPPS II UND TSA

Die Datenschutzgruppe hat das CAPPS-II-Programm und alle anderen für die Massendatenverarbeitung geeigneten Systeme ausdrücklich vom Geltungsbereich ihrer Stellungnahme 4/2003 ausgenommen.

Diese Systeme weichen nämlich qualitativ von der reinen Übermittlung von PNR-Fluggastdaten ab und werfen weitreichende Fragen auf, die geklärt und von der Datenschutzgruppe gezielt in Angriff genommen werden sollten, da sie sich gravierend auf die Grundrechte der betroffenen Personen auswirken.

CAPPS II wirft einige besondere Fragen auf, die nicht nur eine gezielte Prüfung durch die Datenschutzgruppe erfordern, sondern auch andere, stärkere Garantien. Jede künftige Entscheidung über CAPPS II müsste von der Datenschutzgruppe besonders geprüft werden und sollte sich nicht automatisch aus einer Erweiterung des Geltungsumfangs der ersten Angemessenheitsentscheidung der Kommission zur Übermittlung von PNR-Fluggastdaten an die USA ableiten.

Aus diesem Grund und angesichts der Tatsache, dass die Datenschutzgruppe nicht über den endgültigen CAPPS-II-Rechtsrahmen informiert und nicht dazu gehört worden ist, sollte jegliche Nutzung personenbezogener Daten durch die TSA im Zusammenhang mit dem vorgeschlagenen CAPPS-II-System oder seiner Erprobung jetzt und in Zukunft vom Geltungsbereich der Kommissionsentscheidung ausgenommen sein. Mit anderen Worten, die in dieser Stellungnahme getroffenen Aussagen stützen sich auf die Annahme, dass die Kommissionsentscheidung in Zukunft nicht auf CAPPS II ausgedehnt wird, auch nicht indirekt durch einen Verweis auf innerstaatliche Rechtsvorschriften der USA; andernfalls müssten nämlich schon zum jetzigen Zeitpunkt sehr viel kritischere Anmerkungen gemacht werden.

Die Datenschutzgruppe empfiehlt daher der Kommission, in einer Sonderklausel in der Entscheidung klarzustellen, dass die US-Behörden aus der EU übermittelte PNR-Fluggastdaten weder für den Betrieb noch für die Erprobung des CAPPS-II-Systems verwenden.

Die Datenschutzgruppe ist der Meinung, dass das auch für jegliche weitere Verwendung der von Fluggesellschaften übermittelten Daten europäischer Passagiere im Zusammenhang mit anderen Programmen wie beispielsweise Terrorism Information Awareness and US VISIT oder Programmen, die die Verarbeitung biometrischer Daten umfassen, gelten sollte.

4. VERBINDLICHKEIT DER VERPFLICHTUNGSERKLÄRUNG

Die Datenschutzgruppe erinnert daran, dass sich eine Entscheidung der Kommission nicht nur auf bloße „Verpflichtungserklärungen“ staatlicher Behörden stützen sollte, sondern auf Verpflichtungen, die amtlich bekannt gemacht werden, und zwar mindestens im Federal Register, und die für die US-Seite uneingeschränkt bindend sind. Insbesondere sollte kein Zweifel daran gelassen werden, dass sie Rechte Dritter begründen können.

Was diesen Punkt betrifft, steht außer Zweifel, dass die US-Verpflichtungserklärung die US-amerikanische Seite rechtlich nicht bindet. Der neu hinzugefügte Absatz 47 am Ende der Verpflichtungserklärung schränkt deren rechtliche Durchsetzbarkeit sogar weiter ein, denn dort heißt es ausdrücklich: „Durch diese Verpflichtungserklärung werden keinerlei Rechte oder Vergünstigungen für Dritte begründet oder übertragen”.

Die Datenschutzgruppe betont deshalb, dass nicht davon ausgegangen werden kann, dass die Verpflichtungserklärung der US-Seite in der Frage ihrer Verbindlichkeit die Anforderungen erfüllt, die die Datenschutzgruppe in ihrer Stellungnahme 4/2003 aufgestellt hat; sie vertritt ferner die Auffassung, dass es sich hierbei um eine Grundbedingung handelt, die erfüllt sein muss, bevor eine wie auch immer geartete Vereinbarung förmlich getroffen wird.

5. BESONDERE ASPEKTE

Angesichts des oben beschriebenen globalen Kontextes sollten die Forderungen der Vereinigten Staaten, so wie sie sich in der Verpflichtungserklärung (aktualisierte Fassung vom 12. Januar 2004) darstellen, im Lichte der einschlägigen Stellungnahmen der Datenschutzgruppe, insbesondere der Stellungnahme 4/2003 vom 13. Juni 2003, beurteilt werden.

A. BEFRISTUNG DER ANGEMESSENHEITSENTSCHEIDUNG

Für das Paket, das die Verpflichtungserklärung, die Angemessenheitsentscheidung und das damit verknüpfte internationale Abkommen umfasst, wurde eine Geltungsdauer von dreieinhalb Jahren vorgeschlagen.

Die Datenschutzgruppe begrüßt die Aufnahme einer Verfallsklausel in die Vereinbarung und hofft, dass die in ihrer Stellungnahme 4/2003 vorgeschlagene Frist von drei Jahren in Betracht gezogen wird.

B. ZWECKBINDUNG

Das DHS bzw. das US CBP wird die PNR-Fluggastdaten verwenden für die Verhütung und Bekämpfung

1) des Terrorismus und damit verknüpfter Straftaten;

2) anderer schwerer, ihrem Wesen nach länderübergreifender Straftaten, einschließlich organisierter Kriminalität;

3) der Flucht im Falle eines Haftbefehls oder der Gewahrsamnahme wegen der oben genannten Straftaten.

Die Datenschutzgruppe stellt fest, dass die Beschreibung der Zwecke, für die die PNR verwendet werden, enger eingegrenzt und präziser geworden ist. Kategorie 2 ist indessen nach wie vor vage, insbesondere der Umfang der in der US-Verpflichtungserklärung aufgeführten „anderen schweren Straftaten" („other serious crimes"). Außerdem gehen die Zwecke noch immer weit über eine Fokussierung auf die Bekämpfung des Terrorismus hinaus, wie sie die Datenschutzgruppe in ihrer Stellungnahme 4/2003 gefordert hat.

C. LISTE DER ZU ÜBERMITTELNDEN DATENELEMENTE

Auf Vorschlag des US CBP soll die Liste der zu übermittelnden PNR-Fluggastdaten nun 34 Datenelemente umfassen. Die Kommission hat dem zugestimmt. Aus der 38 PNR-Elemente umfassenden Liste in Anhang B der Verpflichtungserklärung vom 22. Mai 2003[3] wurden vier Datenfelder gestrichen (Kennungen für Gratisflugscheine, Zahl der Gepäckstücke, Zahl der Gepäckstücke auf jedem Segment, Upgrades auf eigene/sonstige Veranlassung).

Die Datenschutzgruppe stellt fest, dass hinsichtlich der Liste der zu übermittelnden Datenelemente nur sehr wenige Fortschritte erzielt worden sind. Die überarbeitete US-Liste umfasst nämlich immer noch alle 20 Elemente, die die Datenschutzgruppe in ihrer Stellungnahme 4/2003 für unangemessen und problematisch erachtete.

Außerdem sei darauf hingewiesen, dass die US-Behörden die Zahl der geforderten Datenelemente lediglich durch die Streichung von vier Elementen, die von der Datenschutzgruppe in ihrer Stellungnahme vom 13. Juni akzeptiert worden waren, von

---

[3] Anhang B der Verpflichtungserklärung vom 22. Mai 2003 enthält zwar 39 Datenelemente, doch kann ein PNR tatsächlich nur 38 Elemente umfassen, da das Feld OSI (Weitere Zusatzinformationen – Other Service Information) gemäß dem IATA-Buchungsdienstehandbuch nur verwendet werden sollte, wenn kein SSR-Code (Special Service Request) verfügbar ist. Quelle: IATA Reservation Services Manual, 20. Auflage, gültig von 1. Juni 2003 bis 31. Mai 2004, Ziff. 10.3, S. 127.

38 auf 34 gesenkt haben. Was die verbleibenden 20 Elemente betrifft, die, obwohl die Datenschutzgruppe sie nicht akzeptiert hat, nach wie vor von den US-Behörden gefordert werden, so wurden keinerlei Belege oder Erklärungen vorgelegt, aus denen sich ableiten ließe, inwiefern ihre Verarbeitung in einer demokratischen Gesellschaft für die Terrorismusbekämpfung als notwendig und verhältnismäßig und nicht über das Erforderliche hinausgehend betrachtet werden kann.

Die Datenschutzgruppe erinnert an die Liste von 19 Datenelementen, die sie in ihrer Stellungnahme vom 13. Juni 2003 akzeptierte; jede Hinzufügung zu dieser Liste ist einer strengen Prüfung unter dem Gesichtspunkt der Verhältnismäßigkeit und der Datensparsamkeit zu unterwerfen.

D. SENSIBLE DATEN

In den Gesprächen wurde Einvernehmen darüber erzielt, dass die US-Behörden „bestimmte“ als sensibel geltende PNR-Codes und -Bezeichnungen nicht „verwenden“, sondern löschen werden. In diesem Zusammenhang ist zu beachten, dass es sich hierbei nach Artikel 8 Absatz 1 der Datenschutzrichtlinie, um personenbezogene Daten handelt, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie um Daten über Gesundheit oder Sexualleben.

Die Liste der demnach auszuschließenden Felder und Codedaten ist noch nicht verfügbar. Die Datenschutzgruppe möchte indessen betonen, dass bestimmte Codes, vor allem solche, die sich auf Ernährungsgewohnheiten und besondere gesundheitliche Anforderungen beziehen, sowie Passagiertypcodes, die Aufschluss über konfessionelle Bindungen geben, etwa 'Pilgrim fare', 'Missionary' oder 'Clergy', eindeutig zu löschen sind, während andere eingehender geprüft werden müssen - insbesondere Freitextfelder wie „Allgemeine Anmerkungen“ („General Remarks“), die als sensibel eingestufte Daten enthalten können. In der US-Verpflichtungserklärung vom 12. Januar heißt es, dass diese gelöscht würden, und zwar mit Hilfe einer Liste von Schlüsselwörtern. Diese Vorgehensweise würde nicht garantieren, dass alle sensiblen Daten in diesen Feldern gelöscht werden. Die einzig sichere Lösung wäre daher der Ausschluss dieser Felder, wie es in der Stellungnahme 4/2003 gefordert wird.

In diesem Zusammenhang erinnert die Datenschutzgruppe an ihre Stellungnahme vom 13. Juni 2003, wonach die Übermittlung sensibler Daten ausgeschlossen werden sollte. Es wäre mithin nicht praktikabel, die Löschung erst vorzunehmen, nachdem sensible Daten an die US-Behörden übermittelt worden sind. Die Datenschutzgruppe fordert die Kommission auf, geeignete technische Lösungen zu finden (beispielsweise Filter), die gewährleisten, dass jegliche Übermittlung sensibler Daten an die US-Behörden vermieden wird.

E. VERWENDUNG VON DATEN, DIE SICH AUS PNR-FLUGGASTDATEN ABLEITEN

Aus einem neu eingefügten Abschnitt der Verpflichtungserklärung geht hervor, inwieweit die US-Behörden eingeschränkt sind, was den Zugriff auf aus PNR-Elementen „abgeleiteten“ Daten angeht, die Einzelheiten aus dem Leben eines Passagiers offen

legen und einen gravierenden Eingriff in das Recht der betroffenen Person auf Achtung des Privat- und Familienlebens im Sinne des Artikels 8 der Europäischen Menschenrechtskonvention darstellen können. Die neue Formulierung lautet wie folgt:

„Zusätzliche personenbezogene Daten, die unmittelbar aufgrund bestimmter PNR-Fluggastdaten angefordert werden, werden nur auf legalem Weg von nichtstaatlichen Stellen und nur für rechtmäßige Zwecke der Terrorismusbekämpfung oder der Strafverfolgung eingeholt. Enthält ein PNR-Fluggastdatensatz beispielsweise Kreditkarteninformationen, können Daten über diesbezügliche Kontenbewegungen eingeholt werden, sofern die entsprechenden gesetzlichen Voraussetzungen erfüllt sind, beispielsweise wenn eine Vorladung vor eine „Grand Jury" oder eine gerichtliche Verfügung vorliegt, oder andere rechtliche Voraussetzungen gelten. Der Zugriff auf Daten über E-Mail-Konten, die sich aus einem PNR-Fluggastdatensatz ergeben, ist ebenfalls an die in den USA geltenden gesetzlichen Voraussetzungen geknüpft, d. h., je nach Art der gewünschten Daten, an gerichtliche Vorladungen, Verfügungen, Haftbefehle oder andere gesetzlichen Verfahren."

Diese Klarstellung wird begrüßt. Sie allein kann jedoch die Bedenken der Datenschutzgruppe nicht vollständig zerstreuen. Insbesondere sollten die Zwecke, für die PNR benutzt werden dürfen, nicht durch unspezifizierte „Zwecke der … Strafverfolgung" („law enforcement purposes") ausgeweitet werden. Ferner sollte der Zugriff auf E-Mail-Konten und andere personenbezogene Informationen, die von PNR abgeleitet sind, nur unter Beachtung der verfahrensrechtlichen Erfordernisse erfolgen, die in internationalen Instrumenten über die Zusammenarbeit auf dem Gebiet der Justiz und der Strafverfolgung festgelegt sind. Außerdem muss klar sein, dass die betroffenen Personen sich im Falle eines Missbrauchs an eine unabhängige Behörde wenden können.

F. DAUER DER DATENSPEICHERUNG

Das US CBP speichert die übermittelten PNR-Fluggastdaten für die vereinbarten Zwecke für einen Zeitraum von dreieinhalb Jahren. PNR-Fluggastdaten, auf die in diesem Zeitraum manuell zugegriffen wurde, werden vom US CBP in eine Datei für gelöschte Datensätze überführt, wo sie weitere 8 Jahre verbleiben.

Die Arbeitsgruppe stellt fest, dass dies einen Fortschritt gegenüber der ursprünglich in der Verpflichtungserklärung vom 22. Mai vorgesehenen Speicherfrist von 7 Jahren darstellt. Dreieinhalb Jahre sind jedoch sehr viel länger als die „Wochen oder Monate", die die Datenschutzgruppe in ihrer Stellungnahme 4/2003 forderte. Die Datenschutzgruppe bezweifelt, dass die undifferenzierte Speicherung aller PNR-Elemente für einen so langen Zeitraum als „in einer demokratischen Gesellschaft notwendig… und verhältnismäßig" eingestuft werden kann.

Darüber hinaus ist eine Zusatzfrist von 8 Jahren allein auf Grund der Tatsache, dass auf die Daten zugegriffen wurde, insofern unverhältnismäßig, als sie nicht mit einem konkreten Ermittlungsverfahren oder Haftbefehl, das/der sich auf die betroffenen Person bezieht, verknüpft ist und es ermöglicht, die Frist von dreieinhalb Jahren de facto zu übergehen.

In diesem Zusammenhang sei darauf hingewiesen, dass auch andere Lösungen denkbar sind, die ebenfalls eine wirksame Kriminalitätsbekämpfung ermöglichen, dabei jedoch den Datenschutzgrundsätzen besser Rechnung tragen. So sieht beispielsweise das in

Australien entwickelte System vor, dass der australische Zoll Passagierdaten nicht aufbewahrt oder speichert, es sei denn, es wurde eine strafbare Handlung des Passagiers ermittelt oder die Informationen werden für Ermittlungen wegen des Verdachts der Begehung einer Straftat benötigt.

G. ÜBERMITTLUNGSVERFAHREN

Was das Verfahren für die Übermittlung angeht, so verweist die Datenschutzgruppe auf ihre Stellungnahme 4/2003, in der sie die Auffassung vertreten hat, dass die einzige Form der Datenübermittlung, die keine größeren Probleme aufwirft, das „Push"-Verfahren ist, d. h. ein Verfahren, bei dem die Fluggesellschaften die Daten auswählen und an die US-Behörden übermitteln, im Gegensatz zu einem „Pull"-Verfahren, bei dem die US-Behörden direkten Zugriff auf die Datenbanken der Fluggesellschaften und der Reservierungssysteme hätten.

Die Datenschutzgruppe ist ernsthaft besorgt, dass die technischen Voraussetzungen für ein direkt von den europäischen Luftfahrtgesellschaften zu betreibendes „Push"-Verfahren noch nicht geschaffen sind, obwohl die US-Behörden bislang keinerlei Einwände gegen diese bereits vor mehreren Monaten vorgeschlagene Lösung erhoben haben. Die Datenschutzgruppe hält es für erforderlich, dass spätestens im April 2004 konkrete Maßnahmen verabschiedet werden, und fordert die Kommission nachdrücklich auf, unverzüglich in diesem Sinne tätig zu werden. Des Weiteren betont die Datenschutzgruppe, dass nicht von einem angemessenen Datenschutzniveau auf US-Seite ausgegangen werden kann, solange kein „Push"-System implementiert wurde.

H. ZEITPUNKT DER DATENÜBERMITTLUNG

In ihrer Stellungnahme 4/2003 hat die Datenschutzgruppe empfohlen, das US CBP solle die Daten für einen bestimmten Flug frühestens 48 Stunden vor Abflug erhalten und danach sollten die Daten nur einmal aktualisiert werden.

In diesem Punkt deckt sich die neueste Fassung der Verpflichtungserklärung mit der vorangegangenen, d. h. sie sieht vor, dass die US-Behörden 72 Stunden vor dem Abflug Datenzugang erhalten und die Daten bis zu dreimal aktualisiert werden.

Die Datenschutzgruppe bedauert, dass bei den Verhandlungen in diesem Punkt keine Verbesserungen erzielt wurden.

I. ÜBERMITTLUNG VON PNR-FLUGGASTDATEN AN ANDERE BEHÖRDEN IN DEN VEREINIGTEN STAATEN ODER IN ANDEREN LÄNDERN

In ihrer Stellungnahme 4/2003 forderte die Datenschutzgruppe eine genaue Festlegung, an welche anderen öffentlichen Stellen die Daten weitergegeben werden dürfen, und stellte fest, dass jede direkte oder indirekte Weiterübermittlung nur von Fall zu Fall erfolgen sollte und nur unter der Voraussetzung, dass eine spezifische „Verpflichtungserklärung" abgegeben wird, die nicht ungünstiger ist als diejenige, die

die US-Behörden gegenüber der Kommission abgegeben haben. Darüber hinaus sollte die Zahl der Behörden eingeschränkt werden, an die Daten übermittelt werden dürfen.

Die Datenschutzgruppe stellt fest, dass bisher keine umfassende Liste der staatlichen Behörden vorgelegt worden ist, an die unter Umständen Daten weitergeleitet werden sollen. Die Datenschutzgruppe hat außerdem nach wie vor Bedenken gegen Bestimmungen, die es dem US CBP erlauben, Daten „im Zusammenhang mit anderen gesetzlichen Erfordernissen" („as otherwise required by law") offen zu legen, insbesondere wenn diese Bestimmungen im Lichte geltender oder vorgeschlagener Rechtsvorschriften und Absichtserklärungen betrachtet werden, die vorsehen, dass die Vereinigten Staaten ihre Daten in bestimmten Fällen an andere Länder weitergeben.

Insbesondere weichen die unter Ziffer 29 und 35 der Verpflichtungserklärung vorgesehenen Mechanismen erheblich vom Zweckbestimmungsgrundsatz laut Feststellung der Datenschutzgruppe ab (d. h. Bekämpfung des Terrorismus und damit verknüpfter Straftaten), ja sogar von der weiter gefassten Zweckbestimmung in Ziffer 1 und Ziffer 3 der Verpflichtungserklärung.

J. GARANTIEN – RECHTE DER BETROFFENEN PERSON

1) KLARE INFORMATION DER BETROFFENEN PERSON

In Stellungnahme 4/2003 wird im Einklang mit Artikel 10 der Richtlinie gefordert, dass die betroffenen Personen über die verfügbaren rechtsbehelfswirksamen Instrumente hinaus klar und eindeutig über die Identität des für die Datenverarbeitung Verantwortlichen und den Zweck der Verarbeitung informiert werden und dass sie weitere Auskünfte erhalten, beispielsweise über das Bestehen von Auskunfts- und Berichtigungsrechten.

Die Datenschutzgruppe nimmt zur Kenntnis, dass das US CBP den Reisenden Informationen zur Verfügung stellt. In diesem Zusammenhang stellt die Datenschutzgruppe fest, dass es möglich sein wird, nach genauerer Festlegung der Rechtsgrundlage umgehend eine Standardmitteilung auszuarbeiten, u. a. in Anlehnung an den Entwurf, der der Datenschutzgruppe vorgelegt wurde. Es wäre indessen zu beachten, dass ein umfassendes Informationsblatt die Erfüllung der gesetzlichen Anforderungen für die Rechtmäßigkeit der Übermittlung von PNR-Fluggastdaten in die USA ergänzen, aber keinesfalls ersetzen kann.

2) AUSKUNFTSRECHT

In ihrer Stellungnahme 4/2003 hat die Datenschutzgruppe hervorgehoben, dass tatsächlich durchsetzbare Garantien hinsichtlich der Vorschriften des Informationsfreiheitsgesetzes (FOIA) erforderlich sind, wenn gewährleistet werden soll, dass dieses Gesetz nicht von Dritten in Anspruch genommen wird, um sich Zugang zu PNR-Fluggastdaten zu verschaffen, die im Besitz der US-Behörden sind, und dass das Auskunftsrecht der Betroffenen über ihre eigenen Daten ausnahmslos und eindeutig durchgesetzt wird.

Was den Zugang Dritter zu den Daten angeht, so begrüßt die Datenschutzgruppe die Klarstellungen des US CBP in der Unterlage „Exemptions Under the Freedom of Information Act (FOIA) Applicable to Passenger Name Record (PNR) Data".

Was den Zugang der Passagiere zu ihren eigenen Daten angeht, so bestehen indessen nach wie vor Bedenken hinsichtlich der Art und Weise, in der Ausnahmeregelungen den Betroffenen entgegengehalten werden können, um ihnen den Zugang zu den Daten zu verweigern.

Darüber hinaus stellt die Datenschutzgruppe fest, dass das Auskunftsrecht der Betroffenen nicht wie in der Stellungnahme 4/2003 gefordert ausdrücklich auf alle zusätzlichen Daten ausgedehnt worden ist, die im Zuge der Verarbeitung der aus Europa übermittelten Daten anfallen können (Risikoprofil, Ausschlussliste usw.).

3) BERICHTIGUNG

In ihrer Stellungnahme 4/2003 hat die Datenschutzgruppe hervorgehoben, wie wichtig es ist, dass den betroffenen Personen ein wirksamer Mechanismus zur Berichtigung ihrer Daten zu Verfügung gestellt wird. Die Datenschutzgruppe stellt fest, dass der „Privacy Act“ aus dem Jahr 1974 nach wie vor nur für Staatsangehörige oder Einwohner der Vereinigten Staaten gilt. Die Frage der Gleichbehandlung von Einwohnern der Vereinigten Staaten und Europas ist mithin noch nicht gelöst, und es muss festgestellt werden, ob die Berichtigungsverfahren, die in der Verpflichtungserklärung vorgesehen sind, als so wirksam und rechtlich bindend betrachtet werden können wie das im FOIA verankerte Recht von Staatsangehörigen und Einwohnern der Vereinigten Staaten auf Berichtigung.

4) RECHTSBEHELF

Der Datenschutzbeauftragte des Ministeriums für Heimatschutz (DHS Privacy Office) ist bereit, Beschwerden beschleunigt zu bearbeiten, die die Datenschutzbehörden der EU-Mitgliedstaaten im Auftrag EU-ansässiger Betroffener an ihn richten, die der Meinung sind, dass ihre Beschwerde vom Ministerium bzw. von seinem Dienst nicht zufrieden stellend behandelt wurden.

Die Datenschutzgruppe begrüßt diese Entwicklung. Es ist wichtig, dass Betroffene im Einzelfall qualifizierte Hilfe erhalten können; die Frage der tatsächlichen Unabhängigkeit des Chief Privacy Officer, die die Datenschutzgruppe in der Stellungnahme 4/2003 aufgeworfen hat, ist jedoch noch nicht gelöst. Die Mitglieder der Datenschutzgruppe sind der Meinung, dass die internen Regelungen, die sie hinsichtlich der Funktionen des in FAQ 5 der Safe-Harbor-Vereinbarung vorgesehenen Gremiums getroffen haben, in diesem Zusammenhang hilfreich sein könnten. Sie werden prüfen, welche Anpassungen für die Anwendung im PNR-Kontext notwendig sein könnten.

Die Datenschutzgruppe bedauert andererseits, dass es keine Garantie dafür gibt, dass die Passagiere sich im Falle von Streitigkeiten mit dem DHS in jedem Fall eine wirklich unabhängige Instanz anrufen können. Außerdem wird jetzt deutlich, dass die Verpflichtungserklärung unter Umständen keine verbindliche Rechtswirkung hat und möglicherweise keine vor Gericht durchsetzbaren Pflichten begründen kann (siehe Ziffer 9). Das ist nach wie vor eine erhebliche Lücke im Vergleich zu den Rechten, die in der EU jede Person, deren Daten dort verarbeitet werden, unabhängig von ihrer Herkunft hat.

K. ÜBERPRÜFUNGEN

Die Verpflichtungserklärung wurde um folgende Formulierung erweitert (vgl. Ziffer 43):

„US CBP und DHS verpflichten sich, einmal pro Jahr oder häufiger, falls dies von den Parteien vereinbart wird, gemeinsam mit der Kommission und erforderlichenfalls Sachverständigen aus den Mitgliedstaaten der Europäischen Union[4] die Umsetzung dieser Verpflichtungserklärung zu überprüfen. Damit wollen beide Seiten einen Beitrag zur wirksamen Anwendung der in dieser Verpflichtungserklärung beschriebenen Verfahren leisten. Gegenstand dieser gemeinsamen Überprüfung können die Ergebnisse des Jahresberichts des DHS Chief Privacy Officer an den Kongress (vgl. Ziffer 42) sein, ferner mit Genehmigung des Chief Privacy Officer alle Audits, die im Berichtszeitraum durchgeführt wurden, oder andere Erkenntnisse, insbesondere solche, die die Datensicherheit, die Weitergabe von PNR an designierte Behörden und den Zugang der Mitarbeiter zu PNR-Informationen in den entsprechenden Datenbanken sowie die Bearbeitung von Beschwerden betreffen. Soweit der DHS Chief Privacy Officer dem zustimmt, kann sich die gemeinsame Überprüfung auch auf die Anwendung der Verpflichtungserklärung erstrecken bzw. auf Fragen, die zu einer wirksameren Nutzung von PNR-Fluggastdaten für die unter Ziffer 3 aufgeführten Zwecke beitragen können."

Auch diese Entwicklung wird von der Datenschutzgruppe begrüßt, und sie erwartet, dass die Überprüfungen mit der für eine echte Wirksamkeit notwendigen Offenheit und Transparenz vorgenommen werden. Die Mitglieder der Datenschutzgruppe erklären sich in jedem Fall bereit, zu kooperieren und die von beiden Parteien vereinbarten Geheimhaltungsregelungen zu beachten, soweit sie um Mitwirkung an einer solchen Überprüfung gebeten werden. Die Datenschutzgruppe behält sich selbstverständlich das Recht vor, unabhängig vom Zeitplan der Überprüfungen, diese Frage erneut zu prüfen, wenn sie es ist für erforderlich hält.

L. DATENABGLEICH

Erfahrungen aus jüngster Zeit haben gezeigt, dass neben den oben angeführten Punkten ein weiterer Faktor berücksichtigt werden muss. Die vom US CBP erhobenen PNR-Fluggastdaten werden in den Vereinigten Staaten mit Fahndungslisten abgeglichen: Das hat dazu geführt, dass mehrere Flüge von der EU in die USA in letzter Minute abgesagt werden mussten. Die Informationen, die im Anschluss daran veröffentlicht wurden, brachten zu Tage, dass es sich um Fehler oder Probleme handelte, die auf Namensgleichheiten mit Terrorismusverdächtigen zurückzuführen waren.

---

[4] Beide Seiten informieren sich gegenseitig vorab über die Zusammensetzung ihrer Delegationen. Sie können auch andere Behörden einbeziehen, die für Datenschutz, Zollkontrollen und anderen Formen der Strafverfolgung, Grenzsicherung und/oder Flugsicherheit zuständig sind. Die Beteiligten sind zur Geheimhaltung verpflichtet und müssen die gegebenenfalls erforderlichen Sicherheitsüberprüfungen bestanden haben. Die Geheimhaltungspflicht verbietet beiden Seiten jedoch nicht, ihren zuständigen Behörden, darunter dem US-Kongress und dem Europäischen Parlament, über die Ergebnisse der gemeinsamen Überprüfung zu berichten. Die Modalitäten der gemeinsamen Überprüfung werden von beiden Seiten einvernehmlich festgelegt.

Diese Probleme berühren den für den Datenschutz geltenden Grundsatz der Datenqualität. Die Datenschutzgruppe ist der Meinung, dass mehr getan werden sollte, um solche Folgen für Passagiere, Besatzung und Fluggesellschaften zu vermeiden.

FAZIT

Die Datenschutzgruppe möchte noch einmal darauf hinweisen, dass das übergeordnete Ziel ihrer Bewertung, wie in ihrer Stellungnahme 4/2003 dargelegt, darin besteht, einen klaren Rechtsrahmen für die Übermittlung von Flugpassagierdaten in die USA zu schaffen, der mit den Grundsätzen des Datenschutzes vereinbar ist. Die Datenschutzgruppe hat die Fortschritte im Dialog zwischen den USA und der EU über PNR-Fluggastdaten zur Kenntnis genommen, insbesondere hinsichtlich der Verpflichtungserklärung vom 12. Januar 2004, die die US-Regierung kürzlich vorgelegt hat, und ist erfreut festzustellen, dass einige Verbesserungen gegenüber der früheren Fassung der Verpflichtungserklärung erzielt worden sind.

Diese Fortschritte erlauben aber nach Auffassung der Datenschutzgruppe noch keine positive Angemessenheitsentscheidung. Nach Auffassung der Datenschutzgruppe sollten unabhängig von der gewählten Lösung mindestens die folgenden Datenschutzgrundsätze beachtet werden:

- **Datenqualität:**
    - Die Zwecke der Datenübermittlung sollten sich auf die Bekämpfung terroristischer Straftaten und spezifischer, zu definierender Straftaten mit Terrorismusbezug beschränken.
    - Die Liste der zu übermitteln Datenelemente sollte dem Grundsatz der Verhältnismäßigkeit entsprechen und nicht über das Notwendige hinausgehen.
    - Beim Abgleich mit Daten von Verdächtigen sollte im Interesse der Ergebnissicherheit ein hoher Qualitätsstandard gewährleistet sein.
    - Die Speicherfristen sollten kurz sein und dem Grundsatz der Verhältnismäßigkeit genügen.
    - Passagierdaten sollten nicht für die Einrichtung und/oder Erprobung von CAPPS II oder ähnlichen Systemen verwendet werden.
- **Sensible Daten** sollten nicht übermittelt werden.
- **Rechte der betroffenen Personen:**
    - Die Passagiere sollten rechtzeitig, klar und umfassend informiert werden.
    - Das Auskunftsrecht und das Recht auf Berichtigung sollten diskriminierungsfrei gewährleistet werden.
    - Es sollten hinreichende Garantien dafür existieren, dass den Passagieren wirklich unabhängige Beschwerdeinstanzen zur Verfügung stehen.

- **Verbindlichkeit der Verpflichtungen der US-Behörden:**

    - Die Verpflichtungserklärung der USA sollte für die US-Seite uneingeschränkt rechtsverbindlich sein.

    - Es sollte klargestellt werden, welchen Geltungsumfang, welche Rechtsgrundlage und welchen Wert ein etwaiges „einfaches internationalen Abkommen“ („light international agreement“) hätte.

- Die **Weiterübermittlung** von PNR-Fluggastdaten an andere Behörden in den Vereinigten Staaten oder in anderen Ländern sollte streng begrenzt werden.

- **Übermittlungsverfahren:** Es sollte ein „Push“-Verfahren benutzt werden, bei dem die Daten direkt von den Fluggesellschaften ausgewählt und an die US-Behörden übermittelt werden.

Brüssel, den 29. Januar 2004

Für die Datenschutzgruppe
Der Vorsitzende
Stefano RODOTA