



622/10/DE
WP 178

**Stellungnahme 7/2010 zur Mitteilung der Europäischen Kommission
über das sektorübergreifende Konzept für die Übermittlung von
Fluggastdatensätzen (PNR) an Drittländer**

angenommen am 12. November 2010

Die Gruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist ein unabhängiges Beratungsgremium der EU für Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 14 der Richtlinie 97/66/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen von der Europäischen Kommission, GD Justiz, Direktion C (Grundrechte und Unionsbürgerschaft), B-1049 Brüssel, Belgien, Büro Nr. MO-59 06/036.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,

eingesetzt nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

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

Artikel 15 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002,

gestützt auf ihre Geschäftsordnung,

hat folgende Stellungnahme angenommen:

1. EINLEITUNG

Die Europäische Kommission hat am 21. September 2010 eine Mitteilung über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer vorgelegt. Darin gelangt die Kommission zu der Auffassung, dass die Nutzung von Fluggastdaten zu Strafverfolgungszwecken zunimmt und immer häufiger als übliches, notwendiges Mittel für die Vereinfachung der Strafverfolgungsarbeit betrachtet wird. Daher hat die Kommission beschlossen, eine Reihe allgemeiner Kriterien festzulegen, die die Grundlage für künftige Verhandlungen über PNR-Abkommen mit Drittländern bilden sollen. Die Mitteilung enthält zudem eine Analyse der gegenwärtigen Verwendung von Fluggastdaten und gibt einen Überblick über die Pläne der Kommission für die in den kommenden Jahren mit Drittländern zu schließenden Abkommen.

Da immer mehr Länder Fluggastdaten anfordern, dürfte sich die Zahl der einschlägigen Abkommen weiter erhöhen. Die Kommission hat daher beschlossen, dass es wünschenswert wäre, einen für alle künftigen PNR-Abkommen maßgeblichen Rahmen festzulegen, um sowohl auf Seiten der Fluggesellschaften als auch bei den Mitgliedstaaten Rechtsunsicherheit zu vermeiden und unnötigen Belastungen vorzubeugen, die durch die Notwendigkeit, den unterschiedlichen Vorschriften verschiedener Drittstaaten nachzukommen, entstehen könnten. Die Artikel-29-Datenschutzgruppe begrüßt das sektorübergreifende Konzept der Kommission für die Bearbeitung von Anfragen auf EU-Ebene und für die Sicherstellung hoher Datenschutzstandards unter vollständiger Wahrung der Grundrechte.

Die Datenschutzgruppe weist darauf hin, dass die Frage des Austausches von Fluggastdaten nicht isoliert betrachtet werden sollte. Das sektorübergreifende Konzept sollte daher auf sämtliche von Drittländern gestellten Anfragen nach Fluggastdaten einschließlich API-Daten, Watchlist-Abgleich und sonstigen Maßnahmen der Vorabkontrolle ausgeweitet werden. Dies heißt auch, dass die Kommission bei Erhalt einer Anfrage nach Fluggastdaten entscheiden sollte, ob bestimmte (bzw. welche) Daten (z.B. API-Daten) ausreichend wären und ein entsprechendes Abkommen schließen sollte.

Was die Fluggastdaten anbelangt, hat die Datenschutzgruppe die Verhandlungen, die zum Abschluss der PNR-Abkommen mit den Vereinigten Staaten, Kanada und Australien geführt haben, eng verfolgt und diesbezüglich mehrere Stellungnahmen abgegeben, in denen auf

verschiedene Datenschutzbelange im Zusammenhang mit PNR-Systemen hingewiesen wurde. Bisher ist zahlreichen Einwänden der Datenschutzgruppe nicht Rechnung getragen worden. Die Mitteilung der Kommission ist gleichwohl ein Schritt in die richtige Richtung – auch wenn einige Bedenken bleiben.

II. NOTWENDIGKEIT DER VERWENDUNG VON FLUGGASTDATEN

Die Datenschutzgruppe unterstützt seit jeher den Kampf gegen den internationalen Terrorismus und schwere grenzüberschreitende Kriminalität. Sie hält diesen Kampf für notwendig und legitim. Sie erkennt an, dass personenbezogene Daten unter bestimmten Umständen wertvoll sein können, ist aber der Auffassung, dass dieses Phänomen durch bloßes Erfassen und Bearbeiten von Fluggastdaten nicht beseitigt werden kann und daher auch alle sonstigen verfügbaren Mittel – vorzugsweise mit weniger in die Privatsphäre unschuldiger Reisende eingreifender Wirkung – genutzt werden sollten, um die Sicherheit zu erhöhen und sichere und effiziente Flugreisen sicherzustellen. Es sei darauf hingewiesen, dass die Fluggesellschaften Fluggastdaten für ihre eigenen geschäftlichen Zwecke erfassen und verwenden. Damit diese Daten auch für andere Zwecke (wie eben Strafverfolgungszwecke) genutzt werden können, bedarf es eines ausgewogenen Konzepts, das dem Schutz der öffentlichen Sicherheit und anderen öffentlichen Interessen gleichermaßen Rechnung trägt wie den Grundrechten des Einzelnen.

Die Kommission merkt in ihrer Mitteilung an, dass Fluggastdaten zunehmend als notwendiges Instrument für die Bekämpfung von Terrorismus und schwerer Kriminalität gelten, untermauert diese Aussage aber nicht. Sie macht dabei keinen Unterschied zwischen dem zunehmenden Rückgriff auf Fluggastdaten und der zunehmenden Akzeptanz dieses Rückgriffs. Es mag durchaus so sein, dass die Strafverfolgungsbehörden immer häufiger auf Fluggastdaten zurückgreifen können, aber dieser bloße Umstand zeugt keineswegs von einer politischen oder öffentlichen Akzeptanz der Erfassung und Verwendung von Fluggastdaten, und rechtfertigen kann er deren Notwendigkeit schon gar nicht.

Die drei in Absatz 2.2 der Mitteilung gewählten Formulierungen scheinen eher den Schluss naheulegen, dass es den Strafverfolgungsbehörden gelegen kommt, dass ihnen Fluggastdaten zur Verfügung stehen, als dass sie Fluggastdaten wirklich benötigen, um gegen Terrorismus und Schwerverbrechen vorgehen zu können. Die Datenschutzgruppe bedauert zudem, dass die Kommission es nicht für nötig erachtet hat, näher auf die Wirksamkeit des Rückgriffs auf Fluggastdaten einzugehen, obschon dieser Aspekt doch von wesentlicher Bedeutung ist, wenn es um die Beurteilung der Notwendigkeit geht.

Die Datenschutzgruppe hat in ihren vorhergehenden Stellungnahmen immer wieder darauf hingewiesen, dass es hier vor allem auf ein ausgewogenes Vorgehen ankommt. Letzteres ist bisher jedoch noch nicht an den Tag gelegt worden. Was vor allem zählt: Es gibt einfach keine objektiven Statistiken oder Nachweise, die den Wert von Fluggastdaten für die internationale Bekämpfung von Terrorismus und schweren grenzüberschreitenden Straftaten deutlich aufzeigen. Somit ist es nicht möglich, die Notwendigkeit oder die Angemessenheit des Rückgriffs auf Fluggastdaten zu Strafverfolgungszwecken eindeutig zu bewerten.

Nach Auffassung der Datenschutzgruppe sollte jedes System zur Auswertung von Fluggastdaten

- nachweisbar notwendig sein, um ein gegebenes Problem zu lösen,
- das Problem mit nachweisbarer Wahrscheinlichkeit lösen,
- in einem angemessenen Verhältnis zum angestrebten Sicherheitsgewinn stehen,
- nachweisbar weniger in die Privatsphäre eingreifen als alternative Verfahren und regelmäßig darauf hin überprüft werden, ob es noch verhältnismäßig ist¹.

Diese Anforderungen werden nachfolgend näher ausgeführt. So ist zum einen die Notwendigkeit festzulegen, dass es die Reisegewohnheiten unter Berücksichtigung des konkreten Reisezwecks zu analysieren gilt. Zur Veranschaulichung sei darauf hingewiesen, dass zur Bekämpfung des Terrorismus nicht zwangsläufig die gleichen Daten erforderlich sind wie beispielsweise zur Bekämpfung des Drogenschmuggels, und dass es dabei auch nicht unbedingt auf eine in gleichem Maße ausgewogene Berücksichtigung von Rechten und Interessen ankommt. Auch sei daran erinnert, dass Fluggastdaten erstmals nach den Ereignissen des 11. September 2001 erfasst wurden, als eine außerordentliche Bedrohung bestand. Inzwischen geht es zunehmend um eine generelle Verarbeitung derartiger Daten zu unterschiedlichen Zwecken, die bisweilen in keinem Zusammenhang mehr mit der ursprünglichen Begründung stehen.

Bevor neue PNR-Abkommen oder –Systeme in Betracht gezogen werden können, sollte eine ausführliche Analyse der Wirksamkeit der schon bestehenden Datenbanken und des bereits erfolgten Informationsaustausches² durchgeführt werden.

Die Datenschutzgruppe weist erneut darauf hin, dass, was die Notwendigkeitsanforderung angeht, API-Daten in vielen Fällen ausreichen können, um einem Ersuchen eines Drittlandes um Übermittlung von Fluggastdaten nachzukommen. Da sich diese Daten nicht auf Reiseabsichten, sondern auf genaue Identifizierungsangaben gründen, wäre es einfacher, die Angemessenheit und die Verhältnismäßigkeit der verarbeiteten Daten zu ermitteln. Ferner sollten nach dem Dafürhalten der Datenschutzgruppe die Zwecke, zu denen Strafverfolgungsbehörden auf API- und PNR-Systeme zurückgreifen dürfen, klar definiert werden, damit die Wirksamkeit dieser Systeme wirklich messbar wird.

Für Ersuchen um bzw. das Anfordern von Fluggastdaten gibt es bereits heute zahlreiche Systeme und Mechanismen, darunter die einschlägigen bilateralen Abkommen zwischen einzelnen Mitgliedstaaten und den USA. Die Kommission sollte, bevor sie etwaige neue Abkommen abschließt, zunächst prüfen, ob von Drittländern gestellten Ersuchen um

¹ Stellungnahme der Datenschutzgruppe vom 5. Dezember 2007 zum Vorschlag für ein europäisches PNR-System. Siehe auch die am 28. September 2007 während der 29. Internationalen Datenschutzkonferenz in Montreal angenommene Entschließung über den dringenden Bedarf an weltweiten Standards zum Schutz von Fluggastdaten, die von Regierungsstellen zu Justizvollzugs- und Grenzschutzzwecken herangezogen werden.

² Beispielsweise bestehen bereits einschlägige multi- oder bilaterale Abkommen zwischen Mitgliedstaaten und Drittländern. Auch sei auf die EU-Vorschriften über das VIS und das SIS sowie, was den Datenaustausch mit Nichtmitgliedstaaten angeht, auf die einschlägigen Abkommen mit Drittländern hingewiesen - insbesondere auf das Rechtshilfeabkommen zwischen der EU und den USA, auf das Abkommen zwischen den USA und Europol vom 6. Dezember 2001 und das Abkommen zwischen Eurojust und den USA vom 6. November 2006.

Übermittlung von Fluggastdaten nicht bereits im Rahmen der bestehenden Systeme und Mechanismen nachgekommen werden könnte.

Ferner gilt es die Verhältnismäßigkeit des Systems unter Berücksichtigung der Auswirkungen der verwendeten Mittel auf die Grundrechte des Einzelnen zu evaluieren, beispielsweise durch eine Analyse der Reisegewohnheiten und durch eine Risikobewertung. Wegen der aus derartigen Beschlüssen resultierenden Eingriffe in die Privatsphäre sollten vor einer etwaigen Einführung eines solchen Systems alternative Optionen gründlich geprüft werden – und zwar weitgehend automatisch, auf der Grundlage der üblichen Muster und im Lichte der Schwierigkeiten des Einzelnen, derartige Beschlüsse anzufechten. Die Datenschutzgruppe würde daher begrüßen, wenn für alle künftigen Legislativvorschläge der Europäischen Kommission, die sich auf die Übermittlung von PNR-Daten beziehen, eine gründliche Abschätzung der Folgen für die Grundrechte des Einzelnen durchzuführen wäre.

Angesichts der vorliegenden wissenschaftlichen Erkenntnisse und der aktuellen Studien muss der Nutzen eines groß angelegten Profiling anhand von Fluggastendaten gründlich hinterfragt werden. Der Datenschutzgruppe sind keine Informationen bekannt, die den Nutzen eines solchen Profiling belegen würden. Aktuelle Studien legen vielmehr den Schluss nahe, dass ein derartiges Profiling besonders bei der Terrorismusbekämpfung kontraproduktiv ist.³

Was schließlich das technische Netz der Fluggesellschaften bzw. der Buchungssysteme angeht, so wirft die vorgesehene Verpflichtung zur Anpassung der Infrastrukturen zwecks einfacherer Erledigung der von den Strafverfolgungsbehörden gestellten Datenanfragen erhebliche datenschutzrechtliche Fragen auf: So sollte in einem Vorstadium keine Neudefinition des Systems zu Zwecken erfolgen, die im Grunde nichts mit den primär gewerblichen Tätigkeiten der Fluggesellschaften zu tun haben. Derartige Infrastrukturen sollten vielmehr ganz auf die Anforderungen der Industrie zugeschnitten werden, nicht auf die der Strafverfolgungsbehörden. Entsprechend den Anforderungen der Industrie sollte das

³ So heißt es beispielsweise in einem in der *Harvard Civil Rights- Civil Liberties Review* erschienenen Artikel von Fred H. Cate mit dem Titel „Government Data Mining, the Need for a Legal Framework“, dass immer mehr darauf hindeutet, dass die Datenerschließung für viele Zwecke, zu denen die US-Regierung diese einsetzen will, kein wirksames Mittel ist. Dies gelte besonders für die Bereiche nationale Sicherheit und Strafverfolgung: So hätten die Regierungsbeamten keine einzige Maßnahme ermitteln können, bei der es anhand von Datenbankenanalysen gelungen sei, terroristische Handlungen aufzudecken oder gar zu verhüten. Zudem stünden einem Gelingen derartiger Anstrengungen erhebliche Hindernisse im Weg, beispielsweise in Form von Problemen mit der Datenqualität, in Form von Schwierigkeiten mit dem Datenabgleich und aufgrund der Grenzen der Datenerschließungswerkzeuge. Dies werde besonders deutlich, wenn man die Datenerschließung auf dem Gebiet der nationalen Sicherheit mit der Datenerschließung für gewerbliche Zwecke vergleiche (Seite 468).

Weiter heißt es in dem Artikel, dass selbst in dem unwahrscheinlichen Fall, dass das Datenerschließungssystem, durch das potenzielle Terroristen vom Zugang zu Flugzeugen abgehalten werden sollen, eine nur einprozentige Quote an falschen Positiven aufweisen würde (was schon weitaus besser wäre als die Quoten der öffentlich gemachten Datenerschließung der Regierung oder der gewerblichen Datenerschließung), noch immer 7,4 Millionen Reisende (ein Prozent von 739 Millionen Fluggästen, die von der US-Verkehrssicherheitsbehörde im Jahr 2005 überprüft wurden) irrtümlicherweise als Terrorverdächtige „ermittelt“ würden (Seite 475).

Siehe auch Jeff Jonas und Jim Harper, „Effective Counterterrorism and the Limited Role of Predictive Data Mining“, Policy Analysis, vom 11. Dezember 2006, S. 8 und 9, wo darauf hingewiesen wird, dass Terrordelikte im Gegensatz zu Konsumgewohnheiten und selbst Finanzdelikten nicht mit genügend großer Häufigkeit erfolgen, um zuverlässige Vorhersagemodelle zu ermöglichen: Ohne durchdachte, sich auf umfangreiche historische Muster gründende Algorithmen sei jede auf die Vorhersage von terroristischen Handlungen abstellende Datenerschließung zum Scheitern verurteilt. Das einzige Ergebnis wäre, dass das nationale Sicherheitssystem mit falschen Positiven überschwemmt würde, d.h. mit Warnungen vor „Verdächtigen“, bei denen es sich in Wirklichkeit um unbescholtene Bürger handele.

System Technologien für einen besseren Schutz der Privatsphäre einschließen, um insbesondere dem Zugriff durch Unbefugte vorzubeugen und die Unversehrtheit der personenbezogenen Daten zu wahren.

III. STANDARDS, INHALTE UND KRITERIEN

Die Datenschutzgruppe begrüßt die in Abschnitt 3.3 der Mitteilung genannten allgemeinen Standards. Diese sollten allerdings nicht als bloße Wunschliste für Verhandlungen gesehen, sondern vielmehr als Kernpunkte aller künftigen PNR-Abkommen betrachtet werden. Viele dieser Standards und Kriterien kommen den Bedenken entgegen, die die Datenschutzgruppe und das Europäische Parlament in der Vergangenheit geäußert haben. Durch ihre Anwendung im Rahmen rechtsverbindlicher Abkommen müsste im Prinzip ein weitaus besserer Schutz der Daten der EU-Bürger ermöglicht und Rechtssicherheit geschaffen werden. Die Datenschutzgruppe sieht jedoch auch hier noch Verbesserungsbedarf und möchte darauf drängen, dass die nachfolgend genannten Aspekte zu den allgemeinen Standards und Kriterien für künftige PNR-Abkommen sowie in künftige Verhandlungsmandate aufgenommen werden.

Einhaltung der EU-Rechtsvorschriften über den Schutz der Privatsphäre und personenbezogener Daten

Jedes künftige PNR-Abkommen sollte selbstredend die Bedingungen, die im geltenden Rechtsrahmen der EU (d.h. in den Rechtsvorschriften sowohl des ehemals ersten als auch des ehemals dritten Pfeilers) für den Schutz der Privatsphäre und personenbezogener Daten festgelegt sind, in vollem Umfang erfüllen. Dies bedeutet unter anderem, dass in allen künftigen PNR-Abkommen zumindest die Rechte der „betroffenen Personen“ im Sinne der Richtlinie 95/46/EG wie auch des Beschlusses 2008/977/JI und der nationalen Durchführungsvorschriften sichergestellt werden müssten. Selbstverständlich sollten die betroffenen Personen in der Praxis von diesen Rechten auch Gebrauch machen können. Auch sollte die Kohärenz sowohl mit dem umfassenden künftigen Datenschutzrahmen der EU als auch mit dem künftigen allgemeinen Abkommen zwischen der EU und den USA über den Austausch von Daten im Rahmen der polizeilichen und strafrechtlichen Zusammenarbeit sichergestellt werden. Durch die Abkommen müsste zudem das Recht auf den Schutz personenbezogener Daten gewahrt werden, das in der seit Inkrafttreten des Vertrags von Lissabon rechtlich bindenden Charta der Grundrechte der Europäischen Union niedergelegt ist.

Die Datenschutzgruppe weist darauf hin, dass in den Drittländern, denen die Daten übermittelt werden, Rechtsvorschriften gelten müssen, die eine zu Strafverfolgungszwecken erfolgende Erfassung und Verarbeitung von Fluggastdaten durch zuständige Behörden ermöglichen. Die einschlägigen nationalen Rechtsvorschriften sollten in allen künftigen PNR-Abkommen aufgeführt werden. Da sämtliche Bedingungen der Abkommen auf bilateraler Ebene vereinbart und von allen Vertragsparteien eingehalten werden müssten, sollten zudem keine Bedingungen einseitig festgelegt, geändert oder ausgelegt werden.

Datenqualität

Die Kommission hat bei ihrer Analyse der internationalen „Trends im Bereich PNR“ festgestellt, dass es sich bei Fluggastdaten zumeist um nicht überprüfte Angaben der Fluggäste oder ihrer Reiseveranstalter handelt, welche zu geschäftlichen Zwecken erfasst werden, nicht jedoch zu Strafverfolgungszwecken. Da es keine (einfache) Möglichkeit gibt, diese Daten auf objektive Weise zu überprüfen, können Fluggastdaten nicht als genaue Informationen angesehen werden. Ihre Erfassung zu Zwecken der Strafverfolgung oder der Einwanderungskontrolle wirft daher Fragen bezüglich der Angemessenheit und Genauigkeit auf. In allen Fällen, in denen ein Austausch von Fluggastdaten nachweislich notwendig ist, müsste dies durch eine Einzelfallbewertung nachgewiesen werden, welche insbesondere eine strenge Notwendigkeits- und Verhältnismäßigkeitsprüfung einschließen müsste.

Dauer der Datenvorhaltung durch Strafverfolgungsbehörden des ersuchenden Drittstaats

Die Kommission fordert in ihrer Mitteilung zu Recht, dass die Vorhaltezeiten nicht länger sein sollten als für die Erreichung des festgelegten Zwecks erforderlich ist. Anders ausgedrückt: Sie sollten angemessen und verhältnismäßig sein. Bei jeder Vorhaltung von Daten nicht unter Verdacht stehender Personen stellt sich die Frage nach der Notwendigkeit, und es könnten Konflikte mit Verfassungsgrundsätzen einiger Mitgliedstaaten entstehen. Der Datenschutzgruppe ist bislang kein Nachweis dafür bekannt, dass die Vorhaltezeiten tatsächlich angemessen und verhältnismäßig sind. Alle betreffenden Daten sollten unmittelbar nach ihrer Analyse gelöscht werden – außer in spezifischen Fällen, in denen sie eine Untersuchung über einen spezifischen Fluggast ausgelöst haben. In derartigen Fällen sollten sie so lange in den betreffenden Akten aufbewahrt werden dürfen, wie es für die laufende Untersuchung erforderlich ist, und dies nach Maßgabe eines geltenden verfahrensrechtlichen Rahmens, der geeignete Garantien für die Sicherheit und die Unversehrtheit der personenbezogenen Daten einschließt. Außerdem sollten sie aus der Originaldatenbank gelöscht werden. Im Hinblick auf die mit den allgemeinen Standards angestrebte Harmonisierung hält es die Datenschutzgruppe für wünschenswert, in allen künftigen PNR-Abkommen ein und dieselbe maximale Vorhaltezeit vorzusehen und in diesem Zusammenhang vorzuschreiben, dass die Vorhaltezeit jedoch nicht länger als nötig sein sollte.

Bedingungen für die Datenübermittlung

Die Datenschutzgruppe begrüßt, dass die Kommission vorschlägt, die Datenübermittlung ausschließlich nach dem „Push“-Verfahren vorzunehmen, bei dem die Daten von den Fluggesellschaften ausgewählt und auf direktem Wege an die Behörden übermittelt werden, und nicht auf ein „Pull“-Verfahren zurückzugreifen. „Pull“-Systeme wären somit passé. Die Datenschutzgruppe ist zwar ebenfalls der Auffassung, dass „Push“-Systeme dem Schutz der Privatsphäre weniger abträglich sind als „Pull“-Systeme, würde aber vorschlagen, für künftige Abkommen auch andere „datenschutzfreundliche“ Übermittlungsverfahren in Betracht zu ziehen. Dabei könnte es sich beispielsweise um ein System handeln, bei dem Daten nur dann gespeichert bzw. vorgehalten werden, wenn sie für eine Warnung oder für eine Untersuchung verwendet werden, so dass tatsächlich nur für notwendig erachtete Daten an Strafverfolgungsbehörden übermittelt würden. Ein solches System müsste natürlich mit den neuesten Sicherheitsvorkehrungen einschließlich Zugriffsprotokollen ausgestattet sein.

Die Datenschutzgruppe hält es ferner für wünschenswert, dass die Fluggesellschaften in ihrer Eigenschaft als für die Verarbeitung Verantwortliche „sensible“ Daten herausfiltern, bevor sie Fluggastdaten an Strafverfolgungsbehörden übermitteln. Falls dies aus technischen Gründen nicht möglich ist, sollte ein Filtermechanismus zwischengeschaltet werden, damit die Strafverfolgungsbehörden nur Zugang zu den gefilterten Daten haben. Zudem bekräftigt die Datenschutzgruppe ihre Einwände gegen jedwede „en bloc“-Übermittlung“ von Fluggastdaten: Aus dem Blickwinkel der Verhältnismäßigkeit wäre eine Übermittlung von Fluggastdaten nämlich nur dann akzeptabel, wenn sie strikt auf der Grundlage konkreter Informationen bzw. Hinweise und auch nur von Fall zu Fall erfolgen würde. Die die Daten anfordernde zuständige Behörde müsste dann jeweils nachweisen, dass die Fluggastdaten in dem betreffenden Einzelfall benötigt werden.

Zugang und Speicherung

Der Zugang zu Daten sollte nach Maßgabe der Verhältnismäßigkeitsprüfung und nur von Fall zu Fall gewährt werden. Die für die Prüfung der Passagierliste verwendeten Kriterien sollten wie ein Treffer/kein-Treffer-Verfahren funktionieren, bei dem Zugang zu identifizierbaren Informationen nur im Fall eines „Treffers“ erteilt wird. Auch müssten Zugangskontrollen vorgesehen werden, damit nur befugte Bedienstete zuständiger Behörden, die von den Daten Kenntnis haben müssen, auf personenbezogene Daten zugreifen können. Wie bereits erwähnt, sollten personenbezogene Daten nur gespeichert werden, wenn sie im Zusammenhang mit einer Untersuchung über einen spezifischen Fluggast stehen.

Weiterleitung

Die Mitteilung der Kommission ist, was die Weiterleitung von Fluggastdaten an andere Regierungsstellen im Empfängerland oder an andere Drittländer anbelangt, nicht besonders klar. Die Datenschutzgruppe ist zwar mit den vorgeschlagenen Kriterien einverstanden, würde aber die Weiterleitungsmöglichkeiten noch enger begrenzen. Vor allem sollte der Grundsatz der Zweckbegrenzung gelten, demzufolge die erfassten Daten von anderen Regierungsstellen im Empfängerland zu keinem anderen Zweck als der Bekämpfung von schweren grenzüberschreitenden Straftaten und terroristischen Handlungen verwendet werden dürfen. Generell sollte darauf hingewiesen werden, dass die Behörde, die die Fluggastdaten ursprünglich angefordert hat, als „für die Verarbeitung Verantwortlicher“ anzusehen ist und auch nach der Weiterleitung der Daten an Dritte für die Daten verantwortlich bleibt. Falls Zweifel bestehen, sollte die betreffende Behörde verpflichtet sein, einer Offenlegung der Daten gegenüber Dritten die Zustimmung zu verweigern. Auch müssten die von der Datenverarbeitung Betroffenen im Fall eines Missbrauchs ihrer Fluggastdaten durch einen solchen Dritten die Möglichkeit haben, den ursprünglichen Empfänger der Daten zur Verantwortung zu ziehen. Die Datenschutzgruppe fordert insbesondere, dass für Datenübermittlungen an andere Regierungsbehörden eine begrenzte Liste eindeutig benannter, zum Erhalt von Fluggastdaten berechtigter Behörden aufzustellen sein sollte und diese jedem künftigen Abkommen als Anhang beigelegt werden sollte. Des Weiteren wird die Kommission ersucht, bei Verhandlungen über etwaige Datenweiterleitungsbestimmungen bestehenden bilateralen Abkommen über den Austausch von Fluggastdaten Rechnung zu

tragen, die das betreffende Drittland möglicherweise eingegangen ist. Die Datenschutzgruppe würde es begrüßen, wenn das EU-Abkommen stets Vorrang vor bilateralen Abkommen hätte.

Gemeinsame Prüfung

Die Datenschutzgruppe ist wie die Kommission der Auffassung, dass es von wesentlicher Bedeutung ist, die PNR-Abkommen regelmäßig zu überwachen und zu überprüfen. An dieser gemeinsamen Überprüfung sollten auch Vertreter der europäischen Datenschutzbehörden teilnehmen. Dabei sollte insbesondere die Möglichkeit bestehen, das Funktionieren des Abkommens einschließlich der Ergebnisse der Ausübung des Rechts auf Datenzugang und anderer Rechte der von der Datenverarbeitung betroffenen Personen sowie der Zusammenarbeit zwischen den Aufsichtsbehörden zu evaluieren. Außerdem hält es die Datenschutzgruppe für wichtig, dass in künftigen Abkommen Sanktionen für den Fall vorgesehen werden, dass eine angesetzte gemeinsame Überprüfung nicht rechtzeitig oder gar nicht durchgeführt wird. Als letzten Schritt müsste dies die Aufkündigung des Abkommens nach sich ziehen.

Verfallsklausel

Es ist erforderlich, die Notwendigkeit eines PNR-Systems in periodischen Abständen erneut zu bewerten und zu evaluieren. Eine derart umfassende und gründliche Bewertung kann nicht im Rahmen der genannten gemeinsamen Überprüfung durchgeführt werden. Daher sollte in jedes künftige Abkommen eine Verfallsklausel aufgenommen werden, welche eine gründliche und unabhängige Bewertung und Evaluierung der Bestimmungen des PNR-Systems vorsieht. Nach dem in der Verfallsklausel genannten Datum dürften dann keine weiteren Daten mehr ausgetauscht werden, sofern die Vertragsparteien das Abkommen nicht verlängern.

IV. FAZIT

Die Datenschutzgruppe stellt mit Zufriedenheit fest, dass die Europäische Kommission die klare Notwendigkeit erkannt hat, dass es dem Thema Datenschutz in künftigen PNR-Abkommen größere Aufmerksamkeit zu schenken gilt, und dass sie rechtsverbindliche Abkommen zu schließen gedenkt, um Rechtssicherheit zu schaffen und eine Gleichbehandlung sicherzustellen. Die Mitteilung vom 21. September 2010 ist ein Schritt in die richtige Richtung. Angesichts der vorliegenden wissenschaftlichen Erkenntnisse und der aktuellen Studien muss der Nutzen eines groß angelegten Profiling anhand von Fluggastdaten jedoch gründlich hinterfragt werden.

Die Datenschutzgruppe betont erneut, dass es eines sektorübergreifenden Konzepts für sämtliche Passagierdaten bedarf, nicht nur für Fluggastdatensätze. Angesichts der aktuellen Entwicklungen wie der Überprüfung des geltenden Rechtsrahmens der EU für den Datenschutz und den angestrebten Verhandlungen mit den Vereinigten Staaten über ein allgemeines Datenschutzabkommen ist Kohärenz gefragt.

Die Datenschutzgruppe weist darauf hin, dass die in der Mitteilung der Kommission genannten allgemeinen Standards und Kriterien als das Mindestmaß des durch künftige PNR-Abkommen zu gewährleistenden Datenschutzes betrachtet werden sollten. Diese Standards könnten und müssten gleichwohl noch in mehreren Punkten weiterentwickelt werden.

Die Datenschutzgruppe ersucht daher die Kommission, das Europäische Parlament und den Rat, diese Stellungnahme bei der Erörterung von Verhandlungsmandaten und Entwürfen für künftige PNR-Abkommen zu berücksichtigen und die Datenschutzgruppe über die betreffenden Folgemaßnahmen auf dem Laufenden zu halten. Selbstverständlich steht die Datenschutzgruppe allen EU-Organen erforderlichenfalls zur Verfügung, um ihren Standpunkt zu präzisieren oder näher auszuführen.

Abschließend möchte die Datenschutzgruppe erneut ihren Wunsch zum Ausdruck bringen, bezüglich der Datenschutzaspekte künftiger Abkommen zu Rate gezogen zu werden, zumal sie das offizielle Datenschutz-Beratungsgremium der EU ist und es sich bei ihren Mitgliedern um Vertreter der nationalen Aufsichtsbehörden handelt, die für die Fluggesellschaften, für die die künftigen Abkommen ja maßgeblich sein werden, zuständig sind. Zudem bittet die Datenschutzgruppe darum, regelmäßig über den aktuellen Stand der Verhandlungen über diese Abkommen informiert zu werden.

Geschehen zu Brüssel am 12. November 2010

*Für die Arbeitsgruppe
Der Vorsitzende
Jacob KOHNSTAMM*