



**10031/03/DE
WP 85**

**Stellungnahme 1/2004 zu dem in Australien gewährleisteten Schutzniveau bei der
Übermittlung von Fluggastdatensätzen (Passenger Name Record data – PNR-
Daten) von Fluggesellschaften**

Angenommen am 16. Januar 2004

Die Gruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist ein unabhängiges europäisches Beratungsgremium in 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: Europäische Kommission, GD Binnenmarkt, Direktion E (Dienstleistungen, Urheberrecht, Gewerbliches Eigentum und Datenschutz), B-1049 Brüssel, Belgien, Büro C100-6/136.

Website: www.europa.eu.int/comm/privacy

**STELLUNGNAHME 1/2004 DER 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,**

**zu dem in Australien gewährleisteten Schutzniveau bei der Übermittlung von
Fluggastdatensätzen (Passenger Name Record data – PNR-Daten) von
Fluggesellschaften**

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

unter Hinweis auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr¹, insbesondere auf Artikel 29 sowie Artikel 30 Absatz 1 Buchstabe b der Richtlinie,

gestützt auf die Geschäftsordnung der Gruppe², insbesondere auf Artikel 12 und 14,

in der Erwägung, dass

die australische Regierung die Kommission aufgefordert hat³, festzustellen, dass Australien bei der Übermittlung von Fluggastdaten (Passenger Name Record data – nachstehend „PNR-Daten“) von Fluggesellschaften im Sinne von Artikel 25 der Richtlinie einen angemessenen Schutz gewährleistet,

die Europäische Kommission die Gruppe diesbezüglich um Stellungnahme ersucht hat -

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG

Nach den australischen Rechtsvorschriften für den Grenzschutz ist der australische Zoll ermächtigt, Fluggastdaten (Passenger Name Record data – PNR-Daten) internationaler Fluggesellschaften vor Ankunft der Fluggäste in Australien einer Risikobewertung zu unterziehen. Diese Rechtsvorschriften sollen die Sicherheit an der australischen Grenze verbessern, und sie dienen insbesondere der Umsetzung des Wahlprogramms 2001 der Regierung zur Erhöhung der nationalen Sicherheit.

Der Zugang des Zolls zu PNR-Daten, deren Nutzung und Weitergabe an Dritte ist im australischen Recht durch das Zollgesetz (Customs Act) von 1901, das

¹ ABl. L 281 vom 23.11.1995, S. 31, abrufbar unter:

http://europa.eu.int/comm/internal_market/privacy/index_de.htm

² Angenommen von der Arbeitsgruppe auf ihrer dritten Tagung am 11.9.1996.

³ anlässlich des Treffens zwischen dem australischen Außenminister Alexander Downer und EU-Kommissionsmitglied Chris Patten am 26. Januar 2003, sowie erneut anlässlich des Treffens zwischen dem australischen Justizminister Daryl Williams und EU-Kommissionsmitglied Frits Bolkestein am 1. Oktober 2003 und des Ministertreffens der EU-Troika in Rom am 2. Oktober 2003.

Zollverwaltungsgesetz (Customs Administration Act) von 1985, das Datenschutzgesetz (Privacy Act) von 1988 und eine Verpflichtungserklärung des Zolls gegenüber dem Parlament, die PNR-Daten nicht zu speichern, geregelt.

Die Fluggesellschaften müssen dem Zoll Zugang zu bestimmten ihnen vorliegenden PNR-Daten gewähren. Wenn die Fluggesellschaften den australischen Anforderungen entsprechen, so kann dies zu Problemen im Hinblick auf die Richtlinie 95/46/EG über den Datenschutz führen. Daher hat die Kommission Verhandlungen mit Australien aufgenommen, um die Bedingungen festzulegen, die es ihr ermöglichen, ein angemessenes Schutzniveau gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG festzustellen. Die Kommission hat die Arbeitsgruppe über die Verhandlungen auf dem Laufenden gehalten. Insbesondere wurde der Arbeitsgruppe von der Kommission ein Dokument übergeben, das die Verpflichtung des australischen Zolls gegenüber dem australischen (Bundes-) Parlament in Bezug auf den Zugang zu Fluggastdaten, die Zusage, diese Daten nicht zu speichern, sowie die Feststellungen des Senats zu dieser Frage enthält.⁴

Die Arbeitsgruppe stellt fest, dass die Übermittlung von PNR-Daten durch Fluggesellschaften an Behörden außerhalb der Europäischen Union bei der Öffentlichkeit Bedenken hervorruft und international, politisch und juristisch gesehen weitreichende und mit Brisanz verbundene Auswirkungen hat. Um diesen Bedenken Rechnung zu tragen, sollte einer Kommissionsentscheidung im Anhang eine vollständige Darstellung des einschlägigen australischen Regelungsrahmens beigelegt werden. Ferner empfiehlt die Arbeitsgruppe, dass in der Kommissionsentscheidung ein Mechanismus vorgesehen werden sollte, über den die Kommission von jeder Änderung der einschlägigen Rechtsvorschriften in Kenntnis gesetzt wird.

2. DIE AUSTRALISCHEN RECHTSVORSCHRIFTEN ÜBER PNR-DATEN

Die Arbeitsgruppe nimmt die Erklärungen der australischen Regierung zu diesem Thema zur Kenntnis. Diesen Erklärungen zufolge erstrecken sich die australischen Rechtsvorschriften über PNR-Daten auf folgende Situationen:

- ***Das Zollgesetz (Customs Act) von 1901 in seiner geänderten Fassung***

Anhang 7 des Gesetzes zur Änderung der Bestimmungen über die Grenzsicherheit (Terrorismus) (Border Security Legislation Amendment (Terrorism) Act) von 2002, das der Änderung des Zollgesetzes (Customs Act) von 1901 (nachstehend „das Zollgesetz“) diente, wurde am 2. August 2002 in Kraft gesetzt und ermächtigt den Zoll, durch Ersuchen des Leiters der Zollbehörde (Chief Executive Officer of Customs - CEO) Fluggastinformationen zu erlangen. So ist der Betreiber einer internationalen Fluggesellschaft gemäß § 64AF des Zollgesetzes verpflichtet, dem Zoll auf Ersuchen des Leiters der Zollbehörde Zugang zu PNR-Daten zu gewähren. In § 64AF Absatz 1 Buchstabe a ist festgelegt, dass das Ersuchen des Leiters der Zollbehörde an den Betreiber einer Fluggesellschaft in einer bestimmten Art und Form gestellt wird. Das Ersuchen wird nach seiner Ausfertigung durch den Leiter der Zollbehörde zu einem formalen Rechtsdokument, das den Betreiber bei Erhalt zur Übermittlung der Fluggastdaten verpflichtet.

⁴ Antwortschreiben Australiens vom November 2003 zu Fragen, die während einer Videokonferenz zwischen Vertretern der Kommission und der australischen Regierung am 27. Oktober 2003 aufgeworfen wurden.

Die Arbeitsgruppe stellt fest, dass der Verpflichtung zur Gewährung des Zugangs auch dann nachzukommen ist, wenn es sich bei den betreffenden Daten um personenbezogene Daten gemäß dem australischen Datenschutzgesetz (Privacy Act) von 1988 handelt. Nach § 273GAB des Zollgesetzes ist die Weitergabe von Fluggastdaten an den Zoll selbst dann gestattet, wenn es sich um personenbezogene Daten im Sinne des Datenschutzgesetzes handelt und die Weitergabe andernfalls durch das Datenschutzgesetz geregelt würde.

Die Arbeitsgruppe stellt fest, dass die australische Regierung mit der Festlegung einer Strafe für den Fall der Nichteinhaltung ihre Absicht zum Ausdruck gebracht hat, dem Leiter der Zollbehörde die Ausübung seiner Befugnisse gemäß § 64AF verbindlich vorzuschreiben. Es liegt nicht in seinem Ermessen, eine Fluggesellschaft von der Anwendung von § 64AF zu befreien. Dagegen räumt dieser Paragraph dem Leiter der Zollbehörde einen Ermessensspielraum ein, was den Zeitpunkt des Ersuchens und die Festlegung von Art und Form des Zugangs zu den Fluggastdaten des Betreibers betrifft.

Den australischen Behörden zufolge sind Art und Form des Ersuchens in einem rechtsverbindlichen Dokument niedergelegt, das die Einzelheiten betreffend den Systemzugang und die Bereitstellung der Daten vorschreibt.

- ***Das Zollverwaltungsgesetz (Customs Administration Act) von 1985***

§ 16 des Zollverwaltungsgesetzes von 1985 (nachfolgend als „Zollverwaltungsgesetz“ bezeichnet) regelt die Aufzeichnung und Weitergabe *vertraulicher Informationen*. Alle PNR-Daten, auf die der Zoll zugreift, sind vertrauliche Informationen im Sinne dieses Paragraphen, so dass die Aufzeichnung und Weitergabe dieser Informationen in Übereinstimmung mit diesem Paragraphen erfolgen müssen. *Vertrauliche Informationen sind Informationen, von denen eine Person in Ausübung ihres Dienstes direkt oder indirekt Kenntnis erhält bzw. in deren Besitz sie gelangt (unabhängig davon, ob die Informationen etwas mit diesem Dienst zu tun haben oder nicht).*

Das Zollverwaltungsgesetz untersagt die unbefugte Aufzeichnung und Weitergabe bestimmter Informationen, die sich im Besitz des Zolls befinden, sieht Ausnahmen von diesem Verbot vor und enthält spezielle Vorschriften für die autorisierte Weitergabe *personenbezogener Daten*.⁵ Grundsätzlich ist nach dem Zollverwaltungsgesetz die Aufzeichnung bzw. Weitergabe vertraulicher Informationen verboten, sofern sie nicht gemäß § 16 gestattet oder gemäß einem anderen Gesetz bzw. im Rahmen der Ausübung dienstlicher Pflichten vorgeschrieben bzw. gestattet ist.⁶

Das Zollverwaltungsgesetz gilt für den Leiter der Zollbehörde sowie für eine begrenzte Gruppe von Bediensteten gemäß den Festlegungen von Absatz 1AA.

- ***Das Datenschutzgesetz (Privacy Act) von 1988***

Die Commonwealth-Regierung erließ 1988 ein Datenschutzgesetz, das so genannte „Commonwealth Privacy Act 1988“ (nachstehend als „Datenschutzgesetz“ bezeichnet). Der Geltungsbereich dieses Gesetzes erstreckt sich vor allem auf die Tätigkeiten der Ministerien und Behörden der Bundesregierung, denen es bestimmte

⁵ „Personenbezogene Daten“ gemäß der Definition im Datenschutzgesetz (Privacy Act) von 1988, auf die in Absatz 1A des Zollverwaltungsgesetzes Bezug genommen wird.

⁶ § 16 Absatz 2.

Datenschutzgrundsätze (Information Privacy Principles – IPPs) auferlegt, die auf den OECD-Leitlinien von 1980 für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten beruhen und deren Einhaltung von einem Datenschutzbeauftragten („Privacy Commissioner“) überwacht wird.⁷ Als Behörde der Commonwealth-Regierung unterliegt der Zoll den für den öffentlichen Dienst geltenden Bestimmungen des Datenschutzgesetzes (siehe Anhang A, der eine Zusammenfassung des Gesetzes enthält). Die meisten Datenschutzgrundsätze betreffen Datensätze, die personenbezogene Daten enthalten, nicht jedoch die Daten selbst. Die Arbeitsgruppe geht davon aus, dass gemäß der Definition des Begriffs „Datensatz“ zum Beispiel Datenbanken unter das Datenschutzgesetz fallen.

Die Arbeitsgruppe stellt fest, dass es sich bei sämtlichen PNR-Daten, die vom Zoll aufbewahrt werden, ebenfalls um *personenbezogene Daten* im Sinne des Datenschutzgesetzes von 1988 handelt. Daher ist der Zoll verpflichtet, die Daten in Übereinstimmung mit diesem Gesetz zu behandeln, auch im Hinblick auf die Sammlung, Verwendung, Aufbewahrung und Verbreitung der Daten. Nach den Datenschutzgrundsätzen sind die Behörden der Commonwealth-Regierung in folgenden Bereichen zu einem angemessenen Umgang mit personenbezogenen Daten verpflichtet:

- Sammlung und Ersuchen um Übermittlung personenbezogener Daten (Datenschutzgrundsätze 1 bis 3),
- Speicherung und Sicherung (Datenschutzgrundsatz 4),
- Identifizierung der gespeicherten personenbezogenen Daten (Datenschutzgrundsatz 5),
- Zugang von Personen zu den sie betreffenden personenbezogenen Daten (Datenschutzgrundsatz 6),
- Recht auf Berichtigung (Datenschutzgrundsatz 7),
- die Anforderung, dass personenbezogene Daten richtig, aktuell und vollständig sein müssen (Datenschutzgrundsatz 8),
- die Anforderung, dass personenbezogene Daten nur für einen wichtigen Zweck verwendet werden dürfen (Datenschutzgrundsatz 9),
- Beschränkungen für die Verwendung personenbezogener Daten (Datenschutzgrundsatz 10) und
- Beschränkungen für die Weitergabe personenbezogener Daten (Datenschutzgrundsatz 11).

Der australischen Regierung zufolge führt der Datenschutzbeauftragte bei den Behörden der Commonwealth-Regierung Prüfungen durch, um die Einhaltung der Datenschutzgrundsätze sicherzustellen. Die Regierung teilte ferner mit, dass der Zoll förmliche Verfahren zur Prüfung des Zugangs zur Fluggastdaten durch den Datenschutzbeauftragten und die Innenrevision des Zolls eingeführt hat. Derzeit wird der Justizminister mit einem Vorschlag zur Änderung des Datenschutzgesetzes befasst, die es dem Datenschutzbeauftragten ermöglichen soll, eine Prüfung beim Zoll durchzuführen, um zu gewährleisten, dass keine Aufbewahrung identifizierbarer PNR-Daten erfolgt.

⁷ Gemäß § 14 des Gesetzes. Siehe auch <http://www.privacy.gov.au/>.

3. FUNKTIONSWEISE UND MERKMALE DER REGELUNGEN DES ZOLLS FÜR DEN ZUGANG ZU PNR-DATEN

Die Arbeitsgruppe nimmt die von den australischen Behörden übermittelten Erklärungen zu dieser Frage zur Kenntnis. Diesen Erklärungen zufolge zeichnen sich die Regelungen für den Zugang zu PNR-Daten durch folgende Merkmale und durch die nachstehend beschriebene Funktionsweise aus.

- ***Verarbeitung und Aufbewahrung von PNR-Daten***

Der Zugang zu PNR-Daten über das SITA-Netz ist im Anhang zur vorliegenden Stellungnahme beschrieben, der Bestandteil dieser Stellungnahme ist. Die PNR-Daten, auf die zugegriffen wird, umfassen keine historischen Daten, sondern lediglich PNR-Daten für aktuelle Flüge.

Die erste Stufe der Verarbeitung von PNR-Daten durch den Zoll besteht in einer automatischen Risikobewertung mittels eines Software-Abfragesystems. Das heißt, dass bestimmte Daten der PNR von Fluggesellschaften (Buchungs- und Abfertigungsdaten) mit einer automatischen Profilanalysesoftware ausgewertet werden. Die Software sondert durchschnittlich 95 % bis 97 % der Fluggäste eines Flugs aus, weil deren PNR der Auswertung zufolge keinem Risikoprofil entspricht. Die PNR dieser Fluggäste werden vom Zoll nicht gesichtet oder heruntergeladen, und es erfolgen kein weiterer Zugriff und keine weitere Bewertung.

Ein menschlicher Eingriff findet erstmals statt, wenn Bedienstete des Zolls die PNR-Daten der (je Flug durchschnittlich) verbleibenden 3 % bis 5 % der Fluggäste überprüfen, die durch die automatische Profilanalysesoftware ausgewählt wurden. Die PNR dieser Fluggäste werden von einem Bediensteten des Zolls des in Canberra ansässigen Bereichs Fluggastüberprüfung (Passenger Analysis Unit – PAU) visuell auf eine mögliche Bedrohung geprüft. Besteht nach der zusätzlichen Prüfung weiterhin ausreichend Grund zu der Annahme, dass von dem betreffenden Fluggast eine Gefahr ausgeht, so kann veranlasst werden, dass die betreffende Person bei der Ankunft an der australischen Grenze einer genauen Kontrolle unterzogen wird. Dies betrifft 0,05 % bis 0,1 % der Fluggäste eines Fluges. Von den Zollstellen an der Grenze (am Flughafen) wird die abschließende Entscheidung darüber getroffen, ob der betreffende Fluggast eingehender kontrolliert wird.

Zur Aufbewahrung von PNR-Daten ist der Zoll gesetzlich nicht verpflichtet, es ist ihm aber auch gesetzlich nicht verboten, diese Daten zu speichern. Die PNR-Daten der Fluggäste, von denen gemäß der Auswertung durch die automatische Profilanalysesoftware aller Wahrscheinlichkeit nach keine Gefahr ausgeht (95 % bis 97 % der Fluggäste) werden nicht aufbewahrt, und zu diesen PNR-Daten wird kein Datensatz angelegt. Das heißt, beim Zoll gilt grundsätzlich, dass diese Daten nicht aufbewahrt werden.

Die PNR-Daten der 0,05 % bis 0,1 % der Fluggäste, deren weitere Überprüfung beim Zoll veranlasst wird, werden bis zum Abschluss der Grenzkontrolle aufbewahrt, jedoch nicht gespeichert. Anschließend werden diese PNR-Daten vom PC des betreffenden Bediensteten des Bereichs Fluggastüberprüfung (PAU) gelöscht und nicht in australische Datenbanken eingegeben.

Der Zoll bewahrt personenbezogene Daten aus PNR nur dann auf, wenn ein Fluggast gegen ein Grenzschutzgesetz verstoßen hat, für dessen Umsetzung der Zoll zuständig ist. Im Falle eines vermuteten Verstoßes werden die Daten während der Dauer der Ermittlungen vorübergehend aufbewahrt. Führen die Ermittlungen nicht zu einer strafrechtlichen Verfolgung bzw. wird keine Zuwiderhandlung nachgewiesen, so werden die PNR-Daten vernichtet.

Der oben beschriebene Grundsatz der Nichtaufbewahrung von PNR-Daten ist in einer Verpflichtung verankert, die der Zoll gegenüber dem australischen (Bundes-) Parlament eingegangen ist, als der Senatsausschuss für Rechts- und Verfassungsfragen die Gesetzesvorlage von 2002 (Nr. 2) zur Änderung der Gesetzgebung über die Sicherheit (Terrorismus) und damit zusammenhängende Gesetzesvorlagen prüfte.⁸ Um die Zustimmung des australischen Parlaments dafür zu erlangen, dass Fluggesellschaften gesetzlich dazu gezwungen werden können, PNR-Daten weiterzugeben, und in Anerkennung der Bedenken des Bundesdatenschutzbeauftragten (Federal Privacy Commissioner) in Bezug auf die Speicherung personenbezogener Daten versicherte der Zoll gegenüber dem Parlament, dass er keine PNR-Daten speichern werde, und verpflichtete sich, dass *der Zoll Fluggastdaten nur dann aufbewahrt und speichert, wenn einem Fluggast eine rechtswidrige Handlung nachgewiesen wurde bzw. die Informationen für die Ermittlungen zur Aufklärung einer mutmaßlichen Straftat benötigt werden.*⁹ Die Feststellungen des Senatsausschusses und die Erwartungen, die das Parlament im Hinblick auf den Zugang zu PNR-Daten an den Zoll richtet, sind in den Absätzen 4.80 bis 4.87 des Ausschussberichts vom Mai 2002 aufgeführt.

Den Erklärungen der australischen Behörden zufolge ist diese Verpflichtung verbindlich. Auch bei einem Wechsel an der Spitze der Zollbehörde oder des Ministeriums würde die Änderung der Bedingungen einen Verstoß gegen die Verpflichtung darstellen. Dementsprechend ist der Leiter der Zollbehörde an diese Verpflichtung gebunden, da er sich der Missachtung des Parlaments schuldig machen würde, handelte er der Absicht von § 64 AF zuwider. Auf der Grundlage dieser Verpflichtung hat der Zoll strikte Vorgaben in Bezug auf das Vorgehen bei der Verwendung von PNR-Daten ausgearbeitet, die insbesondere die Aufbewahrung von Daten verhindern. Überdies wurde das für die Analyse der PNR eingesetzte EDV-System so konzipiert, dass es nicht möglich ist, Daten aufzubewahren.

Die Arbeitsgruppe geht davon aus, dass das australische System eine allgemeine längerfristige Speicherung von PNR-Daten und ihre anschließende Verarbeitung verhindert, und nimmt die Erklärungen und Zusicherungen der australischen Regierung zur Kenntnis. Wie bereits erwähnt, werden die PNR-Daten eines Fluggastes nur dann aufbewahrt, wenn festgestellt wurde, dass dieser gegen ein Grenzschutzgesetz verstoßen hat, für dessen Einhaltung der Zoll zuständig ist. Im Falle eines mutmaßlichen Verstoßes werden die Daten für die Dauer der Ermittlungen zu dem mutmaßlichen Verstoß vorübergehend aufbewahrt. Wenn die Ermittlungen nicht zu einer strafrechtlichen Verfolgung führen oder keine Zuwiderhandlung nachgewiesen wird, werden die PNR-Daten vernichtet. In allen anderen Fällen werden die PNR-Daten nicht aufgezeichnet. Außerdem hat der Zoll keinen Zugang zu den Daten eines Fluges mehr, sobald dieser aus den Systemen der Fluggesellschaft gelöscht ist, d. h. 24 bis 48 Stunden nach der Landung des Flugzeugs. Daher weist dieses System nach Einschätzung der Arbeitsgruppe mit

⁸ Antwortschreiben Australiens vom November 2003, Seite 2.

⁹ Antwortschreiben Australiens vom Juni 2003, Seite 9-10; Antwortschreiben Australiens vom November 2003, Seite 10.

Blick auf den Datenschutz einen wichtigen und grundlegenden Unterschied gegenüber dem Ansatz der USA auf, wo PNR-Daten aus den Datenbanken der Fluggesellschaften heruntergeladen und zur anschließenden Bearbeitung in einer gesonderten Datenbank gespeichert werden.

Die Arbeitsgruppe stellt ferner fest, dass das australische System die systematische Übermittlung von PNR-Daten von den Fluggesellschaften an die australischen Behörden einschließt. Zugleich betrifft jede Übermittlung von einer Fluggesellschaft nur einen bestimmten Flug, und jeder für einen solchen Flug erstellte PNR ist speziell für diesen Flug bestimmt. Die PNR, auf die zugegriffen wird, beinhalten also keine historischen Daten. Daher stützt die Arbeitsgruppe ihren Standpunkt darauf, dass zwar systematisch PNR-Daten übermittelt werden, diese Daten jedoch nur einen ganz bestimmten Flug betreffen und die australischen Behörden generell den Grundsatz der Nichtaufbewahrung der PRN-Daten anwenden.

- ***Der Zweck des Zugriffs auf PNR-Daten durch den Zoll***

Die Arbeitsgruppe stellt fest, dass den australischen Behörden zufolge der Zoll zu dem Zweck auf PNR-Daten zugreift, *den Beschluss der australischen Regierung umzusetzen, dass alle PNR-Daten von Fluggästen bei Flügen von oder nach Australien ausgewertet werden, um durch die Identifizierung derjenigen Fluggäste, von denen eine Gefahr durch terroristische oder damit zusammenhängende kriminelle Aktivitäten ausgehen kann, den Grenzschutz zu verbessern.*¹⁰ Der Zugriff ist auf diejenigen Flüge beschränkt, die in § 64 AF Absatz 6 des Zollgesetzes als internationale australische Flüge definiert werden, d. h. Flüge nach, durch oder von Australien.¹¹

- ***PNR-Datenelemente, auf die zugegriffen wird***

Bei den PNR-Daten, die zur Verarbeitung durch den Zoll erhoben werden, handelt es sich um Informationen aus den Fluggastdatensätzen von Personen, die sich auf einem Flug nach oder von Australien befinden. Diese Fluggastdatensätze sind in den verschiedenen Bereichen der Reservierungs- und Abfertigungskomponenten der computergestützten Buchungssysteme (Computer Reservation System - CRS) von Fluggesellschaften gespeichert.¹²

Nach Aussage der australischen Behörden ist die erste computergestützte Abfrage von Fluggastdaten auf eine begrenzte Gruppe von PNR-Datenelementen gerichtet, genauer gesagt auf 18 PNR-Datenelemente. Keines dieser Elemente erstreckt sich auf sensible Daten, die mit Zustimmung des Zolls herausgefiltert werden können, oder auf Daten wie Vielflieger-Einträge.

Die Arbeitsgruppe bewertete die 18 PNR-Datenelemente, die von der automatischen Profilanalysesoftware des Zolls verwendet werden, im Vergleich zu den PNR-Datenelementen, die in ihrer Stellungnahme 4/2003 vom 13. Juni 2003 aufgelistet sind.¹³

¹⁰ Antwortschreiben Australiens vom November 2003, Seite 1.

¹¹ Antwortschreiben Australiens vom Mai 2003, Punkt 3, Seite 3 and 4.

¹² Anhang D zum Antwortschreiben Australiens vom November 2003.

¹³ Seite 8 der Stellungnahme.

Die Arbeitsgruppe stellt fest, dass sieben der 18 PNR-Datenelementen¹⁴ nicht zu den Datenelementen gehören, die in ihrer Stellungnahme 4/2003 als nicht über den angestrebten Zweck hinausgehend eingestuft werden. Ferner sind vier PNR-Datenelemente¹⁵ enthalten, die bis dahin noch nicht von der Arbeitsgruppe bewertet wurden.

Wenn ein Fluggast im Ergebnis der automatischen Profilanalyse als möglicherweise risikobehaftet eingestuft wird, können von einem dazu befugten Bediensteten des Zolls weitere PNR-Datenelemente untersucht werden. Fünf dieser Elemente¹⁶ gehören nicht zu den Datenelementen, die in der genannten Stellungnahme als nicht über den angestrebten Zweck hinausgehend eingestuft wurden, zwei der Datenelemente¹⁷ wurden von der Arbeitsgruppe in ihrer Stellungnahme 4/2003 noch nicht bewertet.

Die Arbeitsgruppe stellt fest, dass der Zoll in Fällen, in denen der Verdacht auf ein hohes Risiko besteht, den gesamten PNR einschließlich der sensiblen Daten prüfen darf. Dies kann (je Flug durchschnittlich) 0,05 % bis 0,1 % der Passagiere betreffen, die von der automatischen Profilanalysesoftware als möglicherweise risikobehaftet ausgewählt werden.

- ***Art und Form des Zugriffs auf PNR-Daten***

Der Zugriff der automatischen Risikobewertungssoftware des Zolls auf die genannten PNR-Datenelemente ist insoweit gestattet, als er in einer bestimmten Art und Form erfolgt, auf die in § 64AF Absatz 1 Buchstabe a des Zollgesetzes verwiesen wird und die in einem speziellen Dokument über Art und Form beschrieben ist. Nach Angaben der australischen Behörden ist jede andere Form des Zugriffs nach australischem Recht ungesetzlich. Zusätzlich zu dem Dokument über Art und Form gibt es noch ein Dokument über die Modalitäten des Systemzugriffs, in dem die Verfahren beschrieben sind, die dem Zoll in Übereinstimmung mit dem Zollgesetz, dem Zollverwaltungsgesetz und dem Datenschutzgesetz den Zugriff auf Fluggastdaten ermöglichen.

Die Art des Zugriffs wird als kontinuierlicher elektronischer Echtzeit-Onlinezugriff auf die CRS-Komponenten des Computersystems der Fluggesellschaft oder auf Systeme zur Speicherung von Fluggastdaten beschrieben.

Dabei handelt es sich um einen Nur-Lese-Zugriff (wie in Absatz 2.3 Buchstabe c des Dokuments über die Modalitäten des Systemzugriffs für den Zugang des Zolls zu Fluggastdaten beschrieben), der nur von einer begrenzten Zahl von Bediensteten des Zolls vorgenommen werden kann, die vom Leiter der Zollbehörde dazu ermächtigt wurden. Die Zugriffsrechte werden von der Fluggesellschaft gewährt.

¹⁴ Zahlungsarten (ohne genauere Angaben), Reisebüro, Bearbeiter, Codeshare-Information, Informationen über die Splittung/Teilung einer Buchung, Sonstige Service-Anforderungen (OSI) und Spezielle Service-Anforderungen (SSR).

Die als nicht über den angestrebten Zweck hinausgehend eingestuften PNR-Daten sind Buchungsdaten, Daten über den geplanten Abflug, gesamter Reiseverlauf für den jeweiligen PNR, Auflistung nicht angetretener Flüge (no show), Zahl der Gepäckstücke, Nummern der Gepäckanhänger und Fluggäste mit Flugschein, jedoch ohne Reservierung (Go show).

¹⁵ Stadt, in der der Flugschein ausgefertigt wurde, Nationalität, Geburtsjahr und Datum, an dem der Flugschein gekauft wurde.

¹⁶ Zahl der Reisenden im PNR, Sitzplatzstatus, Telefonnummern, Reisestatus, allgemeine Bemerkungen und etwaige APIS/API-Informationen.

¹⁷ Geburtsdatum und vollständiger Name des Fluggastes.

Die Form des Zugriffs ist durch speziell für diesen Zweck konzipierte Computer-Software des Zolls vorgegeben. Diese Software ist auf einem EDV-System des Zolls installiert, das über ein als SITA bezeichnetes Netz mit dem System der Fluggesellschaft verbunden ist. Das technische Verfahren für den Zugriff auf PNR-Informationen über SITA ist in einem technischen Anhang zu dieser Stellungnahme beschrieben.

- ***Der erste Empfänger der PNR-Daten***

Die Arbeitsgruppe stellt fest, dass der Zoll als einzige Behörde auf die von Fluggesellschaften übermittelten PNR-Daten zugreift. Beim Zoll ist der Zugang auf eine kleine Gruppe von Bediensteten beschränkt, die dem Bereich Fluggastüberprüfung beim Hauptsitz der Zollbehörde in Canberra zugeteilt wurden. Jeder einzelne Bedienstete muss, bevor er Zugriff auf Fluggastdaten erhält, vom Leiter der Zollbehörde durch eine Ermächtigungsurkunde gemäß Absatz 64AF(1) des Zollgesetzes dazu autorisiert werden. In dem betreffenden Absatz ist festgelegt, dass der Betreiber eines internationalen Luftverkehrsunternehmens ein Ersuchen des Leiters der Zollbehörde erhält, dem dazu ermächtigten Bediensteten ständig Zugang zu Fluggastdaten seines Unternehmens zu gewähren. In dem Dokument über Art und Form des Zugangs zu Fluggastdaten heißt es: *„Der Leiter der Zollbehörde wird mehrere Bedienstete in bestimmten Positionen ermächtigen, auf Ihr System zuzugreifen. Die Angaben zu den betreffenden Bediensteten, werden Ihnen mittels eines von Ihnen bereitgestellten Formulars zur Registrierung/Anmeldung für einen Benutzer-Anmeldecode und ein Passwort mitgeteilt.“*

Auf die „ermächtigten Bediensteten“ wird auch in den Modalitäten für den Systemzugriff Bezug genommen, in denen die Einzelheiten für den Zugriff auf die Computersysteme zwischen dem Zoll und den Fluggesellschaften festgelegt sind. Darin heißt es, dass ausschließlich dazu ermächtigte Bedienstete des Zolls auf das System einer Fluggesellschaft zugreifen dürfen (Absatz 2.2). Darüber hinaus wird erwähnt, dass der Zoll der betreffenden Fluggesellschaft mitteilt, wer die dazu ermächtigten Bediensteten sind, und dass der Zugang zu dem Computersystem der Fluggesellschaft auf diese Bediensteten (oder dafür benannte Computeradressen, die für den automatischen Systemzugriff und die Überprüfung der PNR-Daten verwendet werden) begrenzt ist (Absatz 2.3).

- ***Weitergabe***

PNR-Daten, zu denen der Zoll Zugang hat, dürfen nur unter den nachstehend genannten Umständen an bestimmte Dritte weitergegeben werden:

- a) An ein Gericht, wenn der Zoll durch gerichtliche Anordnung zur Weitergabe der Daten aufgefordert wird.
- b) An die australische Bundespolizei (Australian Federal Police, nachstehend als „AFP“ bezeichnet) für weitere Ermittlungen und zur Strafverfolgung nach australischem Recht, wenn eine an der australischen Grenze angekommene Person vom Zoll einer Straftat bezichtigt wird. Der Zoll gibt nicht den gesamten PNR an die AFP weiter, kann jedoch unter bestimmten Umständen konkrete Angaben übermitteln, die zur Festnahme des Fluggastes geführt haben. Zugang zu Einträgen betreffend Kreditkarteninformationen

und Telefonnummern kann nur bei Vorliegen eines Durchsuchungsbefehls gewährt werden.

Im Rahmen von Verwaltungsvereinbarungen zwischen dem Zoll und der AFP übergibt der Zoll alle schweren Straftaten (z. B. Terrorismus, Einfuhr von Drogen, die der Zoll bei der Grenzkontrolle findet) der AFP zur Ermittlung und Strafverfolgung übergeben.

Als Behörde der Commonwealth-Regierung unterliegt die AFP dem Datenschutzgesetz. Nach dem Datenschutzgrundsatz 11 dieses Gesetzes darf eine Behörde, die Informationen vom Zoll erhält, diese nicht für einen anderen Zweck als den, zu dem ihr die Informationen übermittelt wurden, verwenden oder offen legen.

Darüber hinaus sind alle Mitarbeitern der AFP gemäß § 60A des australischen Bundespolizeigesetzes (Australian Federal Police Act) von 1979 zur Geheimhaltung verpflichtet. In diesem Paragraphen ist festgelegt, dass derzeitige und frühere Mitarbeiter der AFP Informationen, die sie bei der Ausübung ihrer Pflichten erhalten haben, weder unmittelbar noch mittelbar aufzeichnen oder offen legen dürfen, sofern sie nicht durch den Paragraphen dazu ermächtigt werden oder dies aufgrund eines anderen Gesetzes bzw. bei der Ausübung ihrer Pflichten als Mitarbeiter der AFP erforderlich ist. Verstöße gegen § 60 werden mit Haftstrafen von bis zu zwei Jahren geahndet.

Im Hinblick auf die Weitergabe von PNR-Daten gilt für den Zoll der Datenschutzgrundsatz 11 nach Maßgabe von § 14 des Datenschutzgesetzes. Nach diesem Datenschutzgrundsatz gelten für die Weitergabe personenbezogener Daten spezifische Beschränkungen. Ein Datensatz-Verantwortlicher (ähnlich dem für die Verarbeitung der Daten Verantwortlichen im Sinne der Richtlinie) darf keine personenbezogenen Daten für einen anderen als den vorgesehenen Zweck offen legen, ausgenommen in einigen genau festgelegten Ausnahmefällen, so zu Beispiel, wenn der Betroffene seine Zustimmung gegeben hat, die Weitergabe gesetzlich vorgeschrieben oder gestattet ist und wenn dies zur Durchsetzung des Strafrechts, eines Gesetzes zur Verhängung einer Geldstrafe oder zum Schutz der öffentlichen Einnahmen erforderlich ist.

Darüber hinaus gelten für Bedienstete des Zolls, die auf Fluggastdaten zugreifen dürfen, die Voraussetzungen von § 16 des Zollverwaltungsgesetzes von 1985, der Bestimmungen über die Aufzeichnung und Weitergabe vertraulicher Informationen wie PNR-Daten enthält.

Nach Aussagen der australischen Behörden gibt es keine weiteren Bestimmungen betreffend die Weitergabe personenbezogener Daten an Dritte.¹⁸

- ***Sicherheit***

Den australischen Behörden zufolge wurden im Hinblick auf den Zugang zu PNR-Daten mehrere Schichten an Sicherheitsvorkehrungen angelegt.

So ist der Zugang auf eine kleine Gruppe zugriffsberechtigter Bedienstete des Zolls begrenzt. Ferner wurden umfangreiche physische und elektronische Sicherheitsmaßnahmen mit Blick auf eine Abgrenzung der Fluggastdaten von den allgemeinen Zollangelegenheiten getroffen. Dabei handelt es sich insbesondere um folgende Maßnahmen: Die Daten von Fluggesellschaften werden über ein eigens dafür

¹⁸ Antwortschreiben Australiens vom Mai 2003, Punkt 1, Seite 2.

eingerrichtetes LAN gesichert, das physisch und elektronisch von allen anderen Zollsystemen getrennt ist. Die Workstations des Bereichs Fluggastüberprüfung des Zolls befinden sich in einem gesicherten Computerraum, zu dem der Zutritt beschränkt ist. Um auf die Daten von Fluggesellschaften zuzugreifen, sind in drei Schritten Anmeldenamen/Passwörter einzugeben, d. h. für den Zugang zum LAN, für den Zugang zur PNR-Analysesoftware und für Zugang zu dem von der Fluggesellschaft bereitgestellten System (z. B. akustische Kennung Fluggesellschaft/Passwort). Vertretern des Betreibers des Netzwerks SITA zufolge ist das australische System nicht mit dem Datenstrom für die Visakontrolle durch Bedienstete des Zolls außerhalb des Bereichs Fluggastüberprüfung verbunden, es bestehe eine völlige Trennung zwischen den zwei Datenströmen. Die australischen Behörden haben bestätigt, dass die APIS-Daten für die Visakontrolle vollkommen getrennt von dem PNR-Datenstrom geführt werden.

- ***Sensible Daten***

Nach Aussagen der australischen Regierung wird allen personenbezogenen Daten vom Zoll ein gleich hohes Schutzniveau eingeräumt, das sich nicht von dem Schutzniveau für sensible Daten (wie rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen oder gesundheitsbezogene Daten)¹⁹ unterscheidet.

- ***Information***

Mit Blick auf eine angemessene Information der Fluggäste weist die Arbeitsgruppe darauf hin, dass diese klare und genaue Angaben zu ihren Rechten erhalten müssen, insbesondere zu ihrem Recht auf Zugang und Berichtigung sowie zu den verfügbaren Rechtsmitteln. Diese Informationen sollten nach Möglichkeit beim Kauf des Tickets zugänglich gemacht werden.

- ***Recht auf Zugang und Berichtigung***

Da der Zoll dem Datenschutzgesetz unterliegt, muss er PNR-Daten gemäß den Datenschutzgrundsätzen 6 und 7 behandeln, die ausdrücklich Zugangs-, Berichtigungs- und Einspruchsrechte vorsehen.

Gemäß dem Datenschutzgrundsatz 6 hat eine Person das Recht auf Zugang zu den sie betreffenden personenbezogenen Daten, es sei denn, dass der Datensatz-Verantwortliche durch ein Gesetz, das seinerseits den Zugang zu Dokumenten regelt, ermächtigt oder verpflichtet ist, den Zugang zu verweigern. Bei diesen Gesetzen handelt es sich um das Gesetz zur Wahrung des Rechts auf Auskunft (Freedom of Information Act) von 1982 und das Archivgesetz (Archives Act) von 1983. Nach dem Gesetz zur Wahrung des Rechts auf Auskunft ist eine Behörde verpflichtet, einem Bürger die von ihm angeforderten Dokumente zugänglich zu machen (unabhängig davon, ob sie personenbezogene Daten enthalten), sofern die betreffenden Dokumente nicht einer Kategorie angehören, für die Ausnahmen gelten. Nach dem Archivgesetz sind mehr als 30 Jahre alte Unterlagen, die im australischen Bundesarchiv aufbewahrt werden, der Öffentlichkeit zugänglich.

Ist der Datensatz-Verantwortliche nicht bereit ist, einen Datensatz zu ändern, so kann nach Datenschutzgrundsatz 7 der Betroffene fordern, dass der Datensatz-

¹⁹ Ebenda, Punkt 10, Seite 7.

Verantwortliche angemessene Maßnahmen trifft, um diesbezüglich eine Erklärung beizufügen.

Die Arbeitsgruppe stellt fest, dass PNR-Daten nur dann gespeichert werden, wenn ein Verstoß gegen das Grenzschutzgesetz begangen wurde, für dessen Umsetzung der Zoll zuständig ist, bzw. während der Ermittlungen wegen eines mutmaßlichen Verstoßes gegen dieses Gesetz. Zusätzlich zu den genannten gesetzlich verankerten Rechten kann jeder, der einer Straftat beschuldigt wird, zum Zwecke der Verteidigung während des gesamten Gerichtsverfahrens um Zugang zu den über sie vorliegenden Daten nachsuchen.

- ***Durchsetzungsmechanismen***

Durch das Datenschutzgesetz wird das unabhängige Amt des Bundesdatenschutzbeauftragten (Office of the Federal Privacy Commissioner) geschaffen. Der Datenschutzbeauftragte²⁰ ist in seiner Eigenschaft als durch dieses Gesetz bestellter Beamter²¹ gesetzlich verpflichtet, Beschwerden von Einzelpersonen über die Verletzung der Privatsphäre gemäß dem Datenschutzgesetz und anderen damit zusammenhängenden Rechtsvorschriften nachzugehen. Der Datenschutzbeauftragte wird für eine befristete Amtszeit eingesetzt. Um seine Unabhängigkeit zu gewährleisten, kann er nur aus sehr schwerwiegenden Gründen wie Verletzung der Amtspflicht oder Unfähigkeit des Amtes enthoben werden.

Die Arbeitsgruppe stellt fest, dass der Datenschutzbeauftragte gemäß § 52 des Datenschutzgesetzes Entscheidungen treffen und erklären kann, dass bestimmte Praktiken die Privatsphäre verletzen und abzustellen sind, dass der Beklagte den Beschwerdeführer für jeglichen ihm entstandenen Schaden entschädigen muss und dass letzterer Anspruch auf eine Entschädigungsleistung in bestimmter Höhe hat. Gemäß §§ 58 bis 60 des Datenschutzgesetzes sind die Behörden verpflichtet, die Vorgaben einer Entscheidung nach § 52 zu erfüllen. Hält sich eine Behörde nicht an eine solche Entscheidung, so kann der Beschwerdeführer oder der Datenschutzbeauftragte ein Verfahren bei einem Bundesgericht anstrengen, um sie durchzusetzen.

Derzeit unterliegt der Datenschutzbeauftragte aufgrund von Absatz 41(4) des Datenschutzgesetzes Beschränkungen, wenn es darum geht, Beschwerden von nichtaustralischen Bürgern oder Gebietsansässigen im Hinblick auf den Datenschutzgrundsatz 7 (Berichtigung) nachzugehen. Dies wird zurzeit geprüft, um eine Aufhebung dieser Beschränkungen zu erwirken. Die Arbeitsgruppe stellt fest, dass der Datenschutzbeauftragte Beschwerden von nichtaustralischen Bürgern oder Gebietsansässigen mit Blick auf alle anderen Datenschutzgrundsätze uneingeschränkt nachgehen kann.

Ferner stellt die Arbeitsgruppe fest, dass gemäß dem Gesetz über den Bürgerbeauftragten (Ombudsman Act) von 1976 alle Fluggäste das Recht haben, sich beim Bürgerbeauftragten des Commonwealth über die Behandlung durch den Zoll bei der Grenzabfertigung zu beschweren.

²⁰ Teil V.

²¹ Teil IV Abschnitt 1.

4. DER GELTUNGSBEREICH DER VORLIEGENDEN STELLUNGNAHME

Der Geltungsbereich der vorliegenden Stellungnahme erstreckt sich auf den Schutz der Grundrechte und -freiheiten im Hinblick auf die Verarbeitung personenbezogener Daten im Zusammenhang mit PNR-Daten, die den australischen Behörden von Fluggesellschaften für Flüge übermittelt werden, welche in § 64 AF Absatz (6) des Zollgesetzes als internationale australische Flüge definiert sind, d. h. Flüge nach, durch oder von Australien.

Die Arbeitsgruppe gibt diese Stellungnahme ab, nachdem sie die Angemessenheit des Schutzniveaus geprüft hat, das Australien für Fluggastdaten von Fluggesellschaften bietet. Dieser Schutz wird durch das australische Zollgesetz von 1901, das australische Zollverwaltungsgesetz von 1985, das Datenschutzgesetz von 1988 und die beschriebene Verpflichtungserklärung des Zolls gegenüber dem Parlament gewährleistet. Somit bezieht sich die vorliegende Stellungnahme auf das Schutzniveau, das von Australien nach der beantragten Übermittlung von personenbezogenen Daten zu Passagieren und Besatzungsmitgliedern auf der Grundlage der oben genannten Gesetze und der Verpflichtungserklärung des Zolls gegenüber dem Parlament geboten wird. Die Arbeitsgruppe hat insbesondere die Erklärungen und Zusicherungen der australischen Behörden im Hinblick auf die Auslegung der Bestimmungen dieser Gesetze und der Verpflichtungserklärung des Zolls gegenüber dem Parlament sowie im Hinblick auf die Situationen, die unter den Geltungsbereich dieser Gesetze und dieser Verpflichtungserklärung fallen, berücksichtigt.

Darüber hinaus stellt die Arbeitsgruppe fest, dass die australischen Modalitäten des Systemzugriffs über SITA am ehesten als auf Abruf beruhende Übermittlungsmethode (Pull) eingestuft werden können. Daher basiert die vorliegende Stellungnahme auf den derzeitigen Erkenntnissen zur Funktionsweise der Modalitäten des Systemzugriffs über SITA, die im Anhang zu dieser Stellungnahme beschrieben sind.

Die vorliegende Stellungnahme wird ferner unter der Bedingung abgegeben, dass die Beschränkung gemäß Absatz 41(4) des Datenschutzgesetzes im Hinblick auf Untersuchungen des Datenschutzbeauftragten aufgrund von Beschwerden nichtaustralischer Bürger oder Gebietsansässiger im Zusammenhang mit dem Datenschutzgrundsatz 7 (Berichtigung) aufgehoben wird.

Die Arbeitsgruppe behält sich außerdem generell das Recht vor, die vorliegende Stellungnahme, wenn sie nicht angemessen berücksichtigt wird oder wenn im Verlauf künftiger Verhandlungen die Rechtsvorschriften erheblich geändert werden, durch eine weitere Stellungnahme zu ergänzen.

Darüber hinaus wird im Falle einer nicht ordnungsgemäßen Umsetzung der von der australischen Verwaltung gegebenen Garantien eine Neubewertung der Situation erforderlich. Aus diesem Grund ist es wichtig, dass die Kommission einen regelmäßigen Bericht über die tatsächliche Verwendung der Daten und die Sicherstellung des Schutzes in Australien vorlegt. Dies dürfte es ermöglichen, die Bedingungen, unter denen Fluggastdaten in Australien verarbeitet werden, zu überprüfen und sicherzustellen, dass die der Entscheidung der Kommission zugrunde liegenden Annahmen nach wie vor zutreffen.

5. DER VORÜBERGEHENDE CHARAKTER DER ANGEMESSENHEITSFESTSTELLUNG

Der Umfang der ausgetauschten Datenströme hängt mit den ernststen Geschehnissen zusammen, die sich in jüngster Zeit auf internationaler Ebene ereignet haben. Die Arbeitsgruppe empfiehlt, die Situation regelmäßig zu prüfen, um festzustellen, ob diese Datenströme nach wie vor erforderlich sind. Bei einer Änderung der internationalen Lage müsste dies überprüft werden. Die Arbeitsgruppe empfiehlt der Kommission, in ihre Entscheidung Klauseln zur Begrenzung der Geltungsdauer aufzunehmen und die Lage auf jeden Fall in drei Jahren erneut zu prüfen.

6. ERGEBNISSE DER BEWERTUNG

Die Arbeitsgruppe weist darauf hin, dass die australische Regierung zur Durchführung dieser Bewertung Informationen über die Auslegung der einschlägigen Bestimmungen des Zollgesetzes von 1901, des Zollverwaltungsgesetzes von 1985, des Datenschutzgesetzes von 1988 und der Verpflichtungserklärung des Zolls gegenüber dem Parlament übermittelt und Zusicherungen gegeben hat, dass die australischen Vorschriften in Bezug auf PNR-Daten im Einklang mit dieser Auslegung umgesetzt werden. Daher hat sich die Arbeitsgruppe bei ihrer Untersuchung auf diese Auskünfte der australischen Regierung gestützt, so dass ihre Stellungnahme davon abhängt, ob die von der australischen Regierung übermittelten Fakten bei der tatsächlichen Umsetzung der Vorschriften über PNR-Daten in Australien bestätigt werden. Was den Geltungsbereich des australischen Gesetzes über PNR-Daten betrifft, so hat die Arbeitsgruppe die Erklärungen und Zusicherungen berücksichtigt, die die australische Regierung im Hinblick auf die Auslegung der einschlägigen Bestimmungen des Zollgesetzes von 1901, des Zollverwaltungsgesetzes von 1985 und der Verpflichtungserklärung des Zolls gegenüber dem Parlament sowie im Hinblick auf die Fälle abgegeben hat, die in den Geltungsbereich des Datenschutzgesetzes von 1988 fallen. Darüber hinaus stützt die Arbeitsgruppe ihren Standpunkt auf das Zusammenspiel zwischen den PNR-Datenelementen, auf die der australische Zoll zugreift, dem Zweck des Zugriffs auf diese Daten und dem allgemeinen Grundsatz der Nichtaufbewahrung dieser Daten. Dieses Zusammenspiel hat nach Auffassung der Arbeitsgruppe zu einem insgesamt ausgewogenen Herangehen durch die australischen Behörden geführt. Die vorliegende Stellungnahme wird ferner vorbehaltlich der Bedingung abgegeben, dass die australischen Behörden Absatz 41(4) des Datenschutzgesetzes überarbeiten, der die Möglichkeiten des Datenschutzbeauftragten einschränkt, Beschwerden von nichtaustralischen Bürgern oder Gebietsansässigen in Bezug auf die Berichtigung nachzugehen, und dass die Beschränkung im Zuge dieser Überarbeitung aufgehoben wird. Die vorliegende Stellungnahme wurde auf der Grundlage dieser Annahmen, Erklärungen und Bedingungen verfasst.

Schlussfolgerung: Die Arbeitsgruppe gelangt auf der Grundlage der genannten Erkenntnisse und vorbehaltlich der Berücksichtigung der in den Absätzen 3, 4 und 5 genannten Fragen zu der Annahme, dass Australien ein angemessenes Schutzniveau im Sinne von Artikel 25 Absatz 6 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung von Fluggastdaten bietet, die den australischen Behörden von Fluggesellschaften für Flüge übermittelt werden, die in § 64 AF Absatz (6) des Zollgesetzes als internationale australische Flüge definiert werden, d. h. Flüge nach, durch oder von Australien.

Geschehen zu Brüssel, am 16. Januar 2004

*Im Namen der Arbeitsgruppe
Der Vorsitzende
Stefano RODOTA*