



EUROPÄISCHE KOMMISSION

Brüssel, den 19.5.2011
KOM(2011) 280 endgültig

2011/0125 (NLE)

Vorschlag für

BESCHLUSS DES RATES

über die Unterzeichnung des Abkommens zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an den Australian Customs and Border Protection Service

BEGRÜNDUNG

Nach den australischen Rechtsvorschriften ist jede Fluggesellschaft, die Passagierflüge nach oder aus Australien durchführt, verpflichtet, dem Australian Customs and Border Protection Service vor Ankunft der Fluggäste in Australien beziehungsweise vor ihrer Abreise aus Australien elektronischen Zugriff auf Fluggastdatensätze (Passenger Name Records – PNR) zu gewähren. Als Rechtsgrundlage dienen den australischen Behörden dabei der Customs Act 1901 of the Commonwealth (Cth), section 64AF, der Customs Administration Act (1985 (Cth), der Migration Act 1958 (Cth), der Crimes Act 1914 (Cth), der Privacy Act 1988 (Cth) und der Freedom of Information Act 1982 (Cth).

Die genannten Rechtsvorschriften ermöglichen den elektronischen Zugriff auf PNR-Daten vor Ankunft eines Flugs und verbessern damit deutlich die Möglichkeiten des Australian Customs and Border Protection Service, wirksame Vorabkontrollen der Passagiere zum Zwecke der Risikobewertung durchzuführen und so die Reisesicherheit und damit auch die Sicherheit Australiens zu erhöhen. Die Europäische Union arbeitet mit Australien bei der Bekämpfung von Terrorismus und sonstiger grenzübergreifender schwerer Kriminalität zusammen und sieht die Übermittlung von Daten an Australien als Mittel zur Förderung der polizeilichen und justiziellen Zusammenarbeit auf internationaler Ebene, die sich in der Übermittlung analytischer, aus PNR-Daten abgeleiteter Informationen durch Australien an die Behörden des zuständigen Mitgliedstaats sowie je nach Zuständigkeit an Europol und Eurojust manifestiert.

PNR-Daten sind die Aufzeichnungen der Reisedaten eines jeden Passagiers, die alle Informationen enthalten, die für die Verarbeitung und Überprüfung von Buchungen durch die Fluggesellschaften erforderlich sind.

Die Fluggesellschaften sind verpflichtet, dem Australian Customs and Border Protection Service Zugriff auf diejenigen PNR-Daten zu gewähren, die mit den computergestützten Buchungs- oder Abfertigungssystemen der Fluggesellschaften erhoben und darin gespeichert werden.

Nach den Datenschutzvorschriften der EU sind europäische und andere Fluggesellschaften, die Passagierflüge aus der EU durchführen, nicht befugt, die PNR-Daten ihrer Passagiere an Drittstaaten zu übermitteln, die weder einen angemessenen Schutz personenbezogener Daten gewährleisten noch den Nachweis angemessener Datenschutzgarantien erbringen. Es bedarf einer Lösung, die der Notwendigkeit und Bedeutung der Verwendung von PNR-Daten im Kampf gegen Terrorismus und sonstige grenzübergreifende schwere Kriminalität Rechnung trägt, die rechtliche Grundlage für die Übermittlung von PNR-Daten aus der EU nach Australien schafft und gleichzeitig Rechtsunsicherheit für die Fluggesellschaften verhindert. Diese Lösung sollte außerdem EU-weit einheitlich angewandt werden, um Rechtssicherheit für die Fluggesellschaften zu schaffen und die Achtung des Rechts des Einzelnen auf den Schutz personenbezogener Daten sowie auf materielle Sicherheit zu gewährleisten.

Die Europäische Union unterzeichnete 2008 mit Australien ein Abkommen über die Übermittlung und Verarbeitung von PNR-Daten, das auf einer Reihe von Verpflichtungszusagen der australischen Zollbehörde im Zusammenhang mit der Anwendung ihres PNR-Programms beruht¹.

¹ ABl. L 213 vom 8.8.2008, S. 47.

Nach dem Inkrafttreten des Vertrags von Lissabon und aufgrund des ausstehenden Abschlusses des Abkommens übermittelte der Rat das EU-Australien-Abkommen von 2008 dem Europäischen Parlament, damit letzteres seine Zustimmung zum Abschluss des Abkommens erteilt. Das Europäische Parlament verabschiedete eine Entschließung², in welcher es beschloss, die Abstimmung über das Ersuchen um Zustimmung zu vertagen und eine Neuverhandlung des Abkommens auf der Grundlage bestimmter Kriterien zu beantragen. Bis zur Aufnahme der Neuverhandlung sollte das Abkommen von 2008 vorläufig anwendbar sein.

Am 21. September 2010 erhielt der Rat von der Kommission die Empfehlung, die Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und Australien über die Übermittlung und Verwendung von PNR-Daten zu Zwecken der Verhütung und Bekämpfung von Terrorismus und sonstiger grenzübergreifender schwerer Kriminalität zu genehmigen.

Am 11. November 2010 verabschiedete das Europäische Parlament eine Entschließung zu der Empfehlung der Kommission an den Rat zur Genehmigung der Aufnahme von Verhandlungen.

Am 2. Dezember 2010 erließ der Rat einen Beschluss mit einer Verhandlungsrichtlinie, in dem die Kommission zur Aufnahme von Verhandlungen im Namen der Europäischen Union ermächtigt wurde. Nach Abschluss der Verhandlungen zwischen den Parteien wurde das Abkommen am 6. Mai 2011 paraphiert.

Das Abkommen trägt den in der Mitteilung der Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer³ und in den Verhandlungsrichtlinien des Rates festgelegten allgemeinen Kriterien Rechnung.

Die Verarbeitung von PNR-Daten hat sich als sehr wichtiges Instrument im Kampf gegen Terrorismus und sonstige grenzübergreifende schwere Kriminalität erwiesen. Das Abkommen enthält mehrere bedeutsame Datenschutzgarantien für die Personen, deren Daten übermittelt und verarbeitet werden. So darf die Verarbeitung von PNR-Daten nur für Zwecke der Vorbeugung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von terroristischen Straftaten und grenzübergreifender schwerer Kriminalität erfolgen. Einzelpersonen wird das Recht auf Auskunft, Berichtigung der Daten, Rechtsbehelfe und Informationen eingeräumt. Die PNR-Daten sind ausschließlich im „Push“-Verfahren zu übermitteln; die Verwendung von sensiblen Daten ist verboten. Die Speicherfrist für PNR-Daten ist begrenzt; die Daten sind nach Ablauf eines bestimmten Zeitraums zu anonymisieren. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle, dem Australian Information Commissioner, überwacht.

Gemäß Artikel 218 Absatz 5 des Vertrags über die Arbeitsweise der Europäischen Union muss der Rat die Unterzeichnung internationaler Übereinkünfte genehmigen.

Die Kommission schlägt dem Rat daher vor, einen Beschluss über die Unterzeichnung des Abkommens zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an den Australian Customs and Border Protection Service zu erlassen.

² P7_TA-(2010)0144, 5.5.2010.

³ KOM(2010) 492.

Vorschlag für

BESCHLUSS DES RATES

über die Unterzeichnung des Abkommens zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an den Australian Customs and Border Protection Service

DER RAT DER EUROPÄISCHEN UNION –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 82 Absatz 1 Buchstabe d und Artikel 87 Absatz 2 Buchstabe a in Verbindung mit Artikel 218 Absatz 5,

auf Vorschlag der Europäischen Kommission,

in Erwägung nachstehender Gründe:

- (1) Am 2. Dezember 2010 erließ der Rat einen Beschluss mit Verhandlungsrichtlinien, in dem er die Kommission zur Aufnahme von Verhandlungen im Namen der Europäischen Union zwischen der Europäischen Union und Australien über die Übermittlung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Verwendung zu Zwecken der Verhütung und Bekämpfung von Terrorismus und sonstiger grenzübergreifender schwerer Kriminalität ermächtigte.
- (2) Die Verhandlungen wurden mit der Paraphierung des Abkommens erfolgreich abgeschlossen.
- (3) Das Abkommen sollte vorbehaltlich seines späteren Abschlusses unterzeichnet werden.
- (4) Das Abkommen wahrt die Grundrechte und Grundsätze, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden, namentlich das Recht auf Achtung des Privat- und Familienlebens gemäß Artikel 7 der Charta, das Recht auf Schutz personenbezogener Daten gemäß Artikel 8 der Charta und das Recht auf einen wirksamen Rechtsbehelf und auf ein faires Verfahren gemäß Artikel 47 der Charta. Das Abkommen sollte unter Wahrung dieser Rechte und Grundsätze angewandt werden.
- (5) [Das Vereinigte Königreich und Irland beteiligen sich gemäß Artikel 3 des Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit der Sicherheit und des Rechts im Anhang zum Vertrag über die Europäische Union und zum Vertrag über die Arbeitsweise der Europäischen Union an der Annahme dieses Beschlusses.]

- (6) Dänemark beteiligt sich gemäß den Artikeln 1 und 2 des Protokolls Nr. 22 über die Position Dänemarks im Anhang zum Vertrag über die Europäische Union und zum Vertrag über die Arbeitsweise der Europäischen Union nicht an der Annahme dieses Beschlusses; das Abkommen ist für Dänemark daher weder bindend noch diesem Staat gegenüber anwendbar –

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Die Unterzeichnung des Abkommens zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records - PNR) und deren Übermittlung durch die Fluggesellschaften an den Australian Customs and Border Protection Service wird vorbehaltlich seines Abschlusses zu einem späteren Zeitpunkt genehmigt.

Der Wortlaut des zu unterzeichnenden Abkommens ist diesem Beschluss beigelegt.

Die Kommission wird ermächtigt, die Personen zu bestellen, die vorbehaltlich des Abschlusses des Abkommens zu seiner Unterzeichnung befugt sind.

Artikel 2

Dieser Beschluss tritt am Tag seiner Annahme in Kraft.

Geschehen zu Brüssel am

*Im Namen des Rates
Der Präsident*

ANHANG

ABKOMMEN

zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records - PNR) und deren Übermittlung durch die Fluggesellschaften an den Australian Customs and Border Protection Service

DIE EUROPÄISCHE UNION

und

AUSTRALIEN

nachstehend „die Parteien“ genannt –

IN DEM BESTREBEN, zum Schutz ihrer demokratischen Gesellschaften und ihrer gemeinsamen Werte Terrorismus und grenzübergreifende schwere Kriminalität wirksam zu verhüten und zu bekämpfen,

IN DEM BEMÜHEN, die Zusammenarbeit zwischen den Parteien im Geiste der Partnerschaft zwischen der EU und Australien auszubauen und weiter voranzubringen,

IN DEM BEWUSSTSEIN, dass der Austausch von Informationen ein grundlegender Faktor bei der Bekämpfung von Terrorismus und grenzübergreifender schwerer Kriminalität ist und dass die Nutzung von PNR-Daten in diesem Zusammenhang ein sehr wichtiges Instrument darstellt,

IN ANERKENNUNG DER BEDEUTUNG der Verhütung und Bekämpfung von Terrorismus und grenzübergreifender schwerer Kriminalität bei gleichzeitiger Achtung der Grundrechte und Grundfreiheiten, insbesondere des Schutzes der Privatsphäre und des Schutzes personenbezogener Daten,

EINGEDENK des Artikels 6 des Vertrags über die Europäische Union zur Achtung der Grundrechte, des Artikels 16 des Vertrags über die Arbeitsweise der Europäischen Union zum Recht auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten und der Grundsätze der Verhältnismäßigkeit und Notwendigkeit hinsichtlich des Rechts auf Achtung des Privat- und Familienlebens, Achtung der Privatsphäre und Schutz personenbezogener Daten gemäß Artikel 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten, dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108 des Europarats und dem dazugehörigen Protokoll Nr. 181), der Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union und Artikel 17 (Schutz der Privatsphäre) des Internationalen Pakts über bürgerliche und politische Rechte,

IN DEM BEWUSSTSEIN, dass Australien und die EU 2008 das Abkommen zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) aus der Europäischen Union und deren Übermittlung durch

die Fluggesellschaften an den Australian Customs Service unterzeichnet haben, das seit dem Zeitpunkt der Unterzeichnung vorläufig angewandt wird, aber nicht in Kraft getreten ist,

ZUR KENNTNIS NEHMEND, dass das Europäische Parlament am 5. Mai 2010 beschloss, die Abstimmung über das Ersuchen um Zustimmung zu dem Abkommen zu vertagen, und in seiner Entschließung vom 11. November 2010 die Empfehlung der Europäischen Kommission an den Rat der Europäischen Union zur Aufnahme von Verhandlungen über ein neues Abkommen begrüßte,

IN WÜRDIGUNG der einschlägigen Vorschriften des Australian *Customs Act 1901* (Cth) (Customs Act), insbesondere Section 64AF, wonach alle internationalen Fluggesellschaften, die Passagierflüge nach, von oder über Australien durchführen, verpflichtet sind, auf Anfrage dem Australian Customs and Border Protection Service die PNR-Daten, die mit den computergestützten Buchungs- oder Abfertigungssystemen der Fluggesellschaften erhoben und darin gespeichert werden, nach bestimmten Modalitäten und in einer bestimmten Form zur Verfügung zu stellen,

IN ANERKENNUNG DESSEN, dass der *Customs Administration Act 1985* (Cth), der *Migration Act 1958* (Cth), der *Crimes Act 1914* (Cth), der *Privacy Act 1988* (Cth), der *Freedom of Information Act 1982* (Cth), der *Auditor-General Act 1997* (Cth), der *Ombudsman Act 1976* (Cth) und der *Public Service Act 1999* (Cth) Datenschutzbestimmungen, ein Auskunfts- und Widerspruchsrecht, das Recht auf Berichtigung und Erläuterung der Daten, Rechtsmittel sowie Strafen bei missbräuchlicher Nutzung personenbezogener Daten vorsehen,

UNTER HINWEIS AUF die Verpflichtung Australiens sicherzustellen, dass der Australian Customs and Border Protection Service PNR-Daten nur für Zwecke der Vorbeugung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von terroristischen Straftaten und grenzübergreifender schwerer Kriminalität unter strikter Einhaltung der in dem Abkommen enthaltenen Garantien für den Schutz der Privatsphäre und den Schutz personenbezogener Daten verarbeitet,

IN ANBETRACHT der Bedeutung, die der Weiterleitung der aus PNR-Daten abgeleiteten analytischen Daten durch Australien an die Polizei- und Justizbehörden der Mitgliedstaaten sowie an Europol und Eurojust als einem Mittel zur Förderung der polizeilichen und justiziellen Zusammenarbeit auf internationaler Ebene zukommt,

IN BEKRÄFTIGUNG DESSEN, dass dieses Abkommen kein Muster für künftige Vereinbarungen zwischen Australien und der Europäischen Union oder zwischen einer der beiden Parteien und einem anderen Staat über die Verarbeitung und Übermittlung von PNR-Daten oder anderweitigen Daten darstellt, und unter Hinweis darauf, dass die Notwendigkeit und Durchführbarkeit ähnlicher Vereinbarungen für Seeverkehrspassagiere geprüft werden kann –

SIND WIE FOLGT ÜBEREINGEKOMMEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand des Abkommens

Um die Sicherheit der Allgemeinheit zu gewährleisten, sieht das Abkommen die Übermittlung von PNR-Daten aus der Europäischen Union an den vor. In dem Abkommen ist festgelegt, unter welchen Bedingungen PNR-Daten übermittelt und verwendet werden dürfen, sowie die Art und Weise, in der die Daten zu schützen sind.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieses Abkommens bezeichnet der Begriff

- (a) „Abkommen“ das vorliegende Abkommen, seine Anhänge sowie etwaige Änderungen hierzu;
- (b) ‚personenbezogene Daten‘ alle Informationen über eine bestimmte oder bestimmbare natürliche Person; als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;
- (c) ‚Verarbeitung‘ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit PNR-Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Nutzung, die Weitergabe durch Übermittlung oder Transfer, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten;
- (d) „Fluggesellschaften“ Luftverkehrsunternehmen, die über Buchungssysteme im Hoheitsgebiet der Mitgliedstaaten der Europäischen Union und/oder dort verarbeitete PNR-Daten verfügen und Passagierflüge im Rahmen der internationalen Luftfahrt nach, von oder über Australien durchführen;
- (e) „Buchungssysteme“ das Buchungssystem, das Abfertigungssystem oder gleichwertige Systeme einer Fluggesellschaft, die die gleichen Funktionen bieten;
- (f) „Fluggastdatensätze“ oder „PNR-Daten“ die in der EU von Fluggesellschaften verarbeiteten Informationen zu den in Anhang 1 aufgeführten Reisedaten eines jeden Fluggastes, die für die Verarbeitung und Überprüfung der Buchungen durch die beteiligten Fluggesellschaften erforderlich sind;

- (g) „Fluggast“ einen Passagier oder ein Mitglied der Besatzung, einschließlich des Flugkapitäns;
- (h) „sensible Daten“ alle personenbezogenen Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben;

Artikel 3

Anwendungsbereich

1. Australien stellt sicher, dass der die auf der Grundlage dieses Abkommens erhaltenen PNR-Daten nur für Zwecke der Vorbeugung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von terroristischen Straftaten und grenzübergreifender schwerer Kriminalität verarbeitet.
2. Terroristische Straftaten umfassen Folgendes:
 - (a) Handlungen von Personen, die mit Gewalt verbunden sind oder in anderer Weise Menschenleben, Vermögenswerte oder Infrastruktur gefährden und die dem Wesen und dem Kontext nach zu der Annahme berechtigen, dass sie mit dem Ziel begangen wurden,
 - i) die Bevölkerung einzuschüchtern oder zu nötigen,
 - ii) eine Regierung oder internationale Organisation durch Einschüchterung, Ausübung von Zwang oder Nötigung zu einer Handlung oder Unterlassung zu veranlassen,
 - iii) die grundlegenden politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Strukturen eines Landes oder einer internationalen Organisation ernsthaft zu destabilisieren oder zu zerstören,
 - (b) Unterstützung, Begünstigung oder Bereitstellung finanzieller, materieller oder technischer Hilfe oder finanzieller und anderer Dienstleistungen zur Durchführung der unter Buchstabe a beschriebenen Handlungen oder zu deren Unterstützung,
 - (c) direkte oder indirekte Bereitstellung oder Beschaffung von Finanzmitteln in der Absicht oder mit dem Wissen, dass diese Mittel ganz oder teilweise zur Begehung von Handlungen im Sinne der Buchstaben a oder b verwendet werden oder verwendet werden sollen,
 - (d) Beihilfe zur Begehung der unter den Buchstaben a, b oder c beschriebenen Handlungen, Anstiftung zur Begehung oder Versuch der Begehung solcher Handlungen.
3. Als „grenzübergreifende schwere Kriminalität“ gilt jede Straftat, die nach australischem Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens vier Jahren oder mit einer

schwereren Strafe geahndet wird, wenn die Straftat grenzübergreifenden Charakter hat. Eine Straftat hat grenzübergreifenden Charakter, wenn sie

- (a) in mehr als einem Staat verübt wird,
 - (b) in einem Staat begangen wird, aber ein Großteil ihrer Vorbereitung, Planung, Lenkung oder Überwachung in einem anderen Staat stattfindet,
 - (c) in einem Staat im Rahmen einer organisierten kriminellen Vereinigung begangen wird, die ihren kriminellen Machenschaften in mehr als einem Staat nachgeht, oder
 - (d) in einem Staat verübt wird, aber beträchtliche Auswirkungen in einem anderen Staat hat.
4. In Ausnahmefällen kann Australien PNR-Daten zum Schutz lebenswichtiger Interessen von Einzelpersonen verarbeiten, insbesondere wenn Gefahr für Leib und Leben besteht oder deren Gesundheit bedroht ist.
 5. Darüber hinaus können PNR-Daten fallweise verarbeitet werden, wenn diese Verarbeitung nach australischem Recht ausdrücklich zum Zwecke der Überwachung und Rechenschaftspflicht der öffentlichen Verwaltung sowie zur Erleichterung der Einlegung eines Rechtsbehelfs und zur Verhängung von Strafen bei missbräuchlicher Datennutzung erforderlich ist.

Artikel 4

Bereitstellung von PNR-Daten

1. Die Fluggesellschaften stellen die in ihren Buchungssystemen enthaltenen PNR-Daten dem Australian Customs and Border Protection Service zur Verfügung. Sie dürfen nicht durch die Rechtsvorschriften einer der Parteien daran gehindert werden, den einschlägigen australischen Rechtsvorschriften, nach denen sie zur Bereitstellung der Daten verpflichtet sind, nachzukommen.
2. Australien verlangt von den Fluggesellschaften keine PNR-Datenelemente, die nicht bereits mit ihren Buchungssystemen erhoben wurden und darin gespeichert sind.
3. Sollten die von Fluggesellschaften übermittelten Flugdatensätze Daten enthalten, die nicht in Anhang 1 aufgeführt sind, werden diese Daten vom Australian Customs and Border Protection Service gelöscht.

Artikel 5

Angemessenheit

Die Einhaltung dieses Abkommens durch den Australian Customs and Border Protection Service stellt im Sinne der einschlägigen Datenschutzvorschriften der EU einen angemessenen Schutz der PNR-Daten dar, die für die Zwecke dieses Abkommens dem Australian Customs and Border Protection Service übermittelt werden.

Artikel 6

Polizeiliche und justizielle Zusammenarbeit

1. Der Australian Customs and Border Protection Service stellt den Polizei- und Justizbehörden des betreffenden Mitgliedstaats oder Europol und Eurojust im Rahmen ihres jeweiligen Mandats zum frühestmöglichen Zeitpunkt sachdienliche analytische Informationen, die aus PNR-Daten abgeleitet wurden, im Einklang mit den Abkommen oder Vereinbarungen zwischen Australien und Mitgliedstaaten der Europäischen Union sowie gegebenenfalls Europol oder Eurojust auf dem Gebiet der Strafverfolgung oder des Informationsaustauschs, zur Verfügung.
2. Die Polizei- oder Justizbehörde eines Mitgliedstaats der Europäischen Union kann ebenso wie Europol oder Eurojust im Rahmen ihres jeweiligen Mandats den Zugriff auf PNR-Daten oder sachdienliche Informationen, die aus PNR-Daten abgeleitet wurden, beantragen, wenn diese in einem bestimmten Fall für Zwecke der Vorbeugung, Aufdeckung, Untersuchung oder strafrechtlichen Verfolgung einer terroristischen Straftat oder von grenzübergreifender schwerer Kriminalität erforderlich sind. Der Australian Customs and Border Protection Service stellt derartige Informationen im Einklang mit den in Punkt 1 genannten Abkommen oder Vereinbarungen zur Verfügung.

KAPITEL II

GARANTIEN FÜR DIE VERARBEITUNG VON PNR-DATEN

Artikel 7

Datenschutz und Nichtdiskriminierung

1. PNR-Daten unterliegen dem *Privacy Act 1988* (Cth) (Privacy Act), der die Erhebung, Verwendung, Speicherung und Weitergabe sowie die Sicherheit und die Zugriffsbedingungen sowie die Abänderung von personenbezogenen Daten durch die meisten Behörden und Institutionen der australischen Regierung regelt.
2. Australien stellt sicher, dass die Garantien für die Verarbeitung von PNR-Daten nach diesem Abkommen und den einschlägigen nationalen Rechtsvorschriften für alle Fluggäste ungeachtet ihrer Staatsangehörigkeit, ihres Herkunftslandes oder ihrer physischen Anwesenheit in Australien gelten.

Artikel 8

Sensible Daten

Jegliche Verarbeitung sensibler PNR-Daten durch den Australian Customs and Border Protection Service ist untersagt. Enthalten die PNR-Daten eines Fluggastes, die dem Australian Customs and Border Protection Service übermittelt werden, sensible Daten, werden sie vom Australian Customs and Border Protection Service gelöscht.

Artikel 9

Datensicherheit und Datenintegrität

1. Um den Schutz der Daten gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unerlaubte Veränderung, die unbefugte Weitergabe, den unbefugten Zugriff oder jede unrechtmäßige Form der Verarbeitung zu gewährleisten, gilt Folgendes:
 - (a) Die PNR-Datenverarbeitungsanlagen werden in einer gesicherten physischen Umgebung aufbewahrt und durch leistungsfähige Systeme und technische Schutzvorkehrungen gesichert.
 - (b) PNR-Daten werden getrennt von anderen Daten aufbewahrt. Für die Zwecke eines Datenabgleichs können Daten in das PNR-System aufgenommen werden, nicht aber vom PNR-System in andere Datenbanken übernommen werden. Der Zugriff auf das PNR-System wird auf einige wenige Beamte des Australian Customs and Border Protection Service begrenzt, die vom Chief Executive Officer ausdrücklich mit der Verarbeitung von PNR-Daten für die Zwecke dieses Abkommens beauftragt wurden. Der Zugriff auf das PNR-System durch diese Beamten erfolgt in einer sicheren Arbeitsumgebung, zu der unbefugte Einzelpersonen keinen Zugang haben.
 - (c) Der Zugriff auf das PNR-System durch die in Punkt b genannten Beamten wird durch Zugangskontrollsysteme mit einer Nutzer-ID und einem Kennwort kontrolliert.
 - (d) Der Zugriff auf das Netzwerk des Australian Customs and Border Protection Service sowie auf im PNR-System enthaltene Daten wird kontrolliert. Der automatisch erstellte Kontrollbericht enthält den Benutzernamen, die Angabe des Arbeitsplatzes des Benutzers, Datum und Uhrzeit der Abfrage, Inhalt der Abfrage sowie Anzahl der erhaltenen Datensätze.
 - (e) Alle PNR-Daten werden vom Australian Customs and Border Protection Service sicher an andere Behörden weitergeleitet.
 - (f) Das PNR-System gewährleistet die Meldung von Funktionsstörungen und die Erstellung von Fehlerprotokollen.
 - (g) PNR-Daten werden vor Manipulationen, Veränderungen, Ergänzungen oder Verfälschungen durch Fehlfunktionen des Systems geschützt.
 - (h) Von den in der PNR-Datenbank enthaltenen Daten dürfen keine Kopien angefertigt werden, mit Ausnahme von Backup-Kopien für den Fall eines Systemausfalls.
2. Jeder Verstoß gegen die Datensicherheit, insbesondere solche Verstöße, die die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unerlaubte Veränderung, die unbefugte Weitergabe, den unbefugten Zugriff oder jede unrechtmäßige Form der Verarbeitung zur Folge haben, wird mit wirksamen und abschreckenden Strafen geahndet.

3. Der Australian Customs and Border Protection Service meldet jeden Verstoß gegen die Datensicherheit dem Office of the Australian Information Commissioner und setzt die Europäische Kommission von der Meldung eines derartigen Verstoßes in Kenntnis.

Artikel 10

Aufsicht und Rechenschaftspflicht

1. Die Einhaltung der Datenschutzbestimmungen durch die Regierungsbehörden, die PNR-Daten verarbeiten, wird vom Australian Information Commissioner überwacht, der nach Maßgabe der Bestimmungen des Privacy Act befugt ist, die Einhaltung des Privacy Act durch die Behörden zu überprüfen, und der darüber wacht, inwieweit sich der Australian Customs and Border Protection Service an die Bestimmungen des Privacy Act hält.
2. Der Australian Customs and Border Protection Service hat auf der Grundlage des Privacy Act mit dem Australian Information Commissioner vereinbart, dass dieser sämtliche Aspekte der Nutzung und Verarbeitung von PNR-Daten aus der Europäischen Union durch den Australian Customs and Border Protection Service sowie die Maßnahmen und Verfahren zur Regelung des Zugriffs auf PNR-Daten in regelmäßigen Abständen einer förmlichen Überprüfung unterzieht.
3. Der Australian Information Commissioner wird insbesondere Beschwerden von Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Herkunftslandes entgegennehmen, gegen deren Rechte und Freiheiten durch die Verarbeitung ihrer personenbezogenen Daten verstoßen wurde. Die betroffene Person wird darüber informiert, wie mit der Eingabe verfahren wurde. Darüber hinaus wird der Australian Information Commissioner die betreffenden Personen bei der Wahrnehmung ihrer Rechte nach Maßgabe dieses Abkommens, insbesondere des Rechts auf Auskunft, Berichtigung und Rechtsmittel, unterstützen.
4. Jede Person hat darüber hinaus das Recht, beim Commonwealth Ombudsman Beschwerde gegen die Behandlung durch den Australian Customs and Border Protection Service einzulegen.

Artikel 11

Transparenz

1. Australien verlangt von den Fluggesellschaften, dass sie die Fluggäste anhand klarer und aussagekräftiger Informationen über die Erhebung, Verarbeitung und den mit der Nutzung der PNR-Daten verfolgten Zweck aufklären. Diese Informationen sollten vorzugsweise zum Zeitpunkt der Buchung gegeben werden.
2. Australien stellt auf den Websites der zuständigen Regierungsbehörden Informationen für die Öffentlichkeit über den Zweck der Erhebung und Nutzung von PNR-Daten durch den Australian Customs and Border Protection Service zur Verfügung. Dazu gehören auch Informationen zu den Verfahren, wie die Daten eingesehen und berichtigt werden können und welche Rechtsbehelfe es gibt.

Artikel 12

Recht auf Auskunft

1. Jede Person hat das Recht, ungehindert und ohne unzumutbare Verzögerung auf ihre PNR-Daten zuzugreifen, nachdem sie einen entsprechenden Antrag beim Australian Customs and Border Protection Service gestellt hat. Dieses Recht wird auf der Grundlage des *Freedom of Information Act 1982 (Cth)* (Freedom of Information Act) und des *Privacy Act* gewährt. Das Zugriffsrecht beinhaltet auch die Möglichkeit, Zugang zu Dokumenten des Australian Customs and Border Protection Service zu beantragen und zu erhalten, aus denen hervorgeht, ob personenbezogene Daten übermittelt oder verfügbar gemacht wurden, und die Angaben zu den Empfängern oder Empfängergruppen, an die die Daten weitergegeben wurden, enthalten.
2. Die Offenlegung von Informationen gemäß Absatz 1 kann nach Maßgabe des australischen Rechts für Zwecke der Vorbeugung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten und zum Schutz der öffentlichen oder nationalen Sicherheit angemessenen rechtlichen Beschränkungen unter gebührender Beachtung des berechtigten Interesses der betroffenen Person unterworfen werden.
3. Wird die Auskunft verweigert oder eingeschränkt, ist dies der betroffenen Person innerhalb von dreißig (30) Tagen oder einer anderen gesetzlich vorgeschriebenen längeren Frist schriftlich mitzuteilen. Dabei sind die tatsächlichen oder rechtlichen Gründe, auf die die Entscheidung gestützt wird, der betroffenen Person ebenfalls mitzuteilen. Eine derartige Mitteilung kann unterbleiben, sofern ein Grund nach Absatz 2 vorliegt. In jedem der genannten Fälle ist die betroffene Person über ihr Recht aufzuklären, Beschwerde gegen die Entscheidung des Australian Customs and Border Protection Service einzulegen. Diese Beschwerde ist beim Australian Information Commissioner einzulegen. Darüber hinaus wird die betroffene Person über die Möglichkeiten in Kenntnis gesetzt, nach Maßgabe der australischen Rechtsvorschriften einen administrativen und gerichtlichen Rechtsbehelf einzulegen.
4. Legt eine Person beim Australian Information Commissioner Beschwerde nach Absatz 3 ein, wird sie förmlich über den Ausgang des Prüfverfahrens in Kenntnis

gesetzt. Die betreffende Person erhält zumindest eine Mitteilung, ob ihre Datenschutzrechte im Einklang mit diesem Abkommen beachtet wurden.

5. Der Australian Customs and Border Protection Service legt PNR-Daten nicht gegenüber der Allgemeinheit offen, sondern nur gegenüber Personen, deren PNR-Daten verarbeitet wurden, oder gegenüber Vertretern dieser Personen.

Artikel 13

Recht auf Berichtigung und Löschung der Daten

1. Jede Person hat das Recht, die Berichtigung ihrer vom Australian Customs and Border Protection Service verarbeiteten PNR-Daten zu verlangen, wenn die Daten fehlerhaft sind. Die Berichtigung kann die Löschung der Daten erfordern.
2. Anträge auf Berichtigung der vom Australian Customs and Border Protection Service gespeicherten PNR-Daten können nach Maßgabe des Freedom of Information Act oder des Privacy Act direkt beim Australian Customs and Border Protection Service gestellt werden.
3. Der Australian Customs and Border Protection Service nimmt auf diesen Antrag hin alle notwendigen Überprüfungen vor und teilt der betreffenden Person möglichst umgehend mit, ob ihre PNR-Daten berichtigt oder gelöscht worden sind. Die Mitteilung an die betreffende Person erfolgt schriftlich innerhalb von dreißig (30) Tagen oder einer anderen gesetzlich vorgeschriebenen längeren Frist und enthält Informationen über die Möglichkeit, beim Australian Information Commissioner Beschwerde gegen die Entscheidung des Australian Customs and Border Protection Service einzulegen, sowie über die Möglichkeiten, nach Maßgabe der australischen Rechtsvorschriften einen administrativen und gerichtlichen Rechtsbehelf einzulegen.
4. Legt eine Person beim Australian Information Commissioner Beschwerde nach Absatz 3 ein, wird sie förmlich darüber in Kenntnis gesetzt, wie mit der Eingabe verfahren wurde.

Artikel 14

Rechtsbehelfe

1. Jede Person, gegen deren Rechte nach diesem Abkommen verstoßen wurde, hat das Recht, einen wirksamen administrativen und gerichtlichen Rechtsbehelf einzulegen.
2. Jede Person, der wegen einer unrechtmäßigen Verarbeitung oder einer anderen mit den Rechten nach diesem Abkommen nicht zu vereinbarenden Handlung ein Schaden entsteht, hat Anspruch auf Wiedergutmachung, wozu auch Schadenersatzzahlungen von Australien gehören können.
3. Die Rechte nach den Absätzen 1 und 2 werden allen Personen ungeachtet ihrer Nationalität, ihres Herkunftslands, ihres Wohnorts oder ihrer physischen Präsenz in Australien gewährt.

Artikel 15

Automatisierte Verarbeitung von PNR-Daten

1. Der Australian Customs and Border Protection Service oder die anderen, in Anhang 2 aufgeführten staatlichen Stellen treffen Entscheidungen, die eine nachteilige Rechtsfolge für einen Fluggast haben oder ihn erheblich beeinträchtigen, nicht allein auf der Grundlage der automatisierten Verarbeitung von PNR-Daten.
2. Der Australian Customs and Border Protection Service nimmt keine automatisierte Datenverarbeitung auf der Grundlage von sensiblen Daten vor.

Artikel 16

Speicherung der Daten

1. Die PNR-Daten werden höchstens fünfzehn Jahre ab dem Tag, an dem der Australian Customs and Border Protection Service sie erstmals erhalten hat, gespeichert. Während dieses Zeitraums werden die PNR-Daten nur für Zwecke der Vorbeugung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von terroristischen Straftaten und grenzübergreifender schwerer Kriminalität in folgender Weise in dem PNR-System gespeichert:
 - (a) Vom erstmaligen Erhalt der PNR-Daten an sind diese drei Jahre lang einer beschränkten Anzahl von Bediensteten des Australian Customs and Border Protection Service zugänglich, die vom Chief Executive Officer des Australian Customs and Border Protection Service eigens ermächtigt wurden, Fluggäste zu ermitteln, die möglicherweise von Interesse sein könnten.
 - (b) Nach Ablauf der ersten drei Jahre nach dem erstmaligen Erhalt der PNR-Daten werden diese bis zum Ende des Zeitraums von fünfzehn Jahren in dem PNR-System gespeichert, wobei jedoch alle Datenelemente, die die Identifizierung des Fluggastes ermöglichen könnten, auf den sich die PNR-Daten beziehen, unkenntlich gemacht werden müssen. Derartige anonymisierte PNR-Daten sind nur einer beschränkten Anzahl von Bediensteten des Australian Customs and Border Protection Service zugänglich, die vom Chief Executive Officer des Australian Customs and Border Protection Service eigens ermächtigt wurden, Analysen im Zusammenhang mit terroristischen Straftaten und grenzübergreifender schwerer Kriminalität durchzuführen. Der unbeschränkte Zugang zu den PNR-Daten wird durch ein Mitglied des Senior Executive Service des Australian Customs and Border Protection Service nur gestattet, wenn dies für Zwecke der Vorbeugung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von terroristischen Straftaten und grenzübergreifender schwerer Kriminalität notwendig ist.
2. Zur Anonymisierung der PNR-Daten sind folgende Datenelemente unkenntlich zu machen:
 - (a) Name(n),

- (b) andere Namen in dem PNR-Datensatz sowie Anzahl der in dem Datensatz erfassten Reisenden;
 - (c) sämtliche verfügbaren Kontaktinformationen, einschließlich Informationen zur Kundenidentifizierung;
 - (d) allgemeine Eintragungen, u.a. Other Supplementary Information (OSI), Special Service Information (SSI) und Special Service Request (SSR) Information, sofern sie Angaben enthalten, anhand deren eine natürliche Person identifiziert werden kann;
 - (e) etwaige Daten zum Advance Passenger Processing (APP) oder zur Advance Passenger Information (API), sofern sie Angaben enthalten, anhand deren eine natürliche Person identifiziert werden kann.
3. Unbeschadet des Absatzes 1 dürfen PNR-Daten, die für die Untersuchung, die strafrechtliche Verfolgung oder die Vollstreckung von Strafen in spezifischen Fällen terroristischer Straftaten oder grenzübergreifender schwerer Kriminalität erforderlich sind, für die Zwecke der Untersuchung, der strafrechtlichen Verfolgung oder der Vollstreckung von Strafen in diesen Fällen verarbeitet werden. Die PNR-Daten dürfen gespeichert werden, bis in den betreffenden Fällen die Untersuchung oder die strafrechtliche Verfolgung abgeschlossen oder die Strafe vollstreckt ist.
4. Sobald die in den Absätzen 1 und 3 genannte Speicherfrist abgelaufen ist, sind die PNR-Daten endgültig zu löschen.

Artikel 17

Protokollierung und Dokumentierung der Verarbeitung von PNR-Daten

1. Jegliche Verarbeitung von PNR-Daten, einschließlich des Zugangs zu diesen Daten und deren Abfrage oder Weitergabe sowie der – auch abschlägig beschiedenen – Anforderung von PNR-Daten durch die australischen Behörden oder Behörden von Drittstaaten, ist vom Australian Customs and Border Protection Service für Zwecke der Überwachung der Rechtmäßigkeit der Datenverarbeitung, der Selbstüberwachung und der Gewährleistung einer angemessenen Datenintegrität und Sicherheit der Datenverarbeitung zu protokollieren und zu dokumentieren.
2. Die gemäß Absatz 1 erstellten Protokolle und Dokumentationen dürfen nur für Aufsichts- und Prüfungszwecke, einschließlich Untersuchung und Aufklärung von Fällen unbefugten Zugangs zu den Daten, herangezogen werden.
3. Die gemäß Absatz 1 erstellten Protokolle und Dokumentationen sind dem Australian Information Commissioner auf dessen Anforderung hin zu übermitteln. Der Australian Information Commissioner darf diese Informationen nur zur Aufsicht für Datenschutzzwecke und zur Sicherstellung der ordnungsgemäßen Verarbeitung sowie der Integrität und Sicherheit der Daten verwenden.

Artikel 18

Nutzung von PNR-Daten durch andere australische staatliche Stellen

1. Der Australian Customs and Border Protection Service darf eine Nutzung der PNR-Daten ausschließlich durch die in Anhang 2 aufgeführten australischen staatlichen Stellen nur zulassen, wenn Folgendes gewährleistet ist:
 - (a) Die Empfänger wenden auf die PNR-Daten die in diesem Abkommen festgelegten Garantien an.
 - (b) Die Daten werden nur für die in Artikel 3 genannten Zwecke genutzt.
 - (c) Die Daten werden nur fallweise genutzt, es sei denn, sie wurden anonymisiert.
 - (d) Vor der Nutzung durch die anderen Stellen nimmt der Australian Customs and Border Protection Service eine sorgfältige Bewertung der Relevanz der Daten vor, die genutzt werden sollen. Es werden nur diejenigen Elemente der PNR-Daten zur Nutzung freigegeben, bei denen eindeutig aufgezeigt wird, dass sie unter den betreffenden Umständen notwendig sind. In jedem Fall werden die Daten nur im geringstmöglichen Umfang zur Nutzung freigegeben.
 - (e) Die Empfänger der Daten stellen sicher, dass diese nicht ohne Genehmigung des Australian Customs and Border Protection Service weitergegeben werden; diese Genehmigung wird nur für die in Artikel 3 des Abkommens genannten Zwecke erteilt.
2. Das Verzeichnis der Stellen in Anhang 2 kann im Wege eines diplomatischen Notenwechsels zwischen den Parteien dahingehend geändert werden, dass es folgende Stellen umfasst:
 - (a) jegliche Nachfolgeeinrichtung oder -agentur der in Anhang 2 bereits aufgeführten Einrichtungen und Agenturen;
 - (b) jegliche neue Einrichtung oder Agentur, die nach Inkrafttreten dieses Abkommens gegründet wird und deren Funktionen einen direkten Zusammenhang mit der Verhütung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von Terrorismus und grenzübergreifender schwerer Kriminalität aufweisen;
 - (c) jegliche bereits bestehende Einrichtung oder Agentur, deren Funktionen einen direkten Zusammenhang mit der Verhütung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von Terrorismus und grenzübergreifender schwerer Kriminalität bekommen.
3. Werden analytische Informationen übertragen, die im Rahmen dieses Abkommens erlangte PNR-Daten enthalten, sind die in diesem Artikel festgelegten Garantien für diese Daten zu beachten.
4. Dieser Artikel steht einer gegebenenfalls erforderlichen Weitergabe von PNR-Daten für Zwecke von Artikel 3 Absätze 4 und 5 und von Artikel 10 nicht entgegen.

Weitergabe von PNR-Daten an Behörden von Drittstaaten

1. Der Australian Customs and Border Protection Service darf PNR-Daten nur dann an einzelne Behörden von Drittstaaten weitergeben, wenn Folgendes gewährleistet ist:
 - (a) Der Australian Customs and Border Protection Service hat von der empfangenden Drittstaatsbehörde die Zusicherung erhalten, dass auf die weitergegebenen Daten die gleichen Garantien angewandt werden wie die in diesem Abkommen festgelegten.
 - (b) PNR-Daten dürfen nur an Drittstaatsbehörden weitergegeben werden, deren Funktionen einen direkten Zusammenhang mit der Verhütung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von Terrorismus und grenzübergreifender schwerer Kriminalität aufweisen.
 - (c) Die Daten dürfen ausschließlich für Zwecke der Verhütung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von terroristischen Straftaten und grenzübergreifender schwerer Kriminalität gemäß Artikel 3 weitergegeben werden.
 - (d) Die Daten dürfen nur fallweise weitergegeben werden.
 - (e) Vor der Weitergabe nimmt der Australian Customs and Border Protection Service eine sorgfältige Bewertung der Relevanz der Daten vor, die weitergegeben werden sollen. Es werden nur diejenigen Elemente der PNR-Daten weitergegeben, bei denen eindeutig aufgezeigt wird, dass sie unter den betreffenden Umständen notwendig sind. In jedem Fall werden Daten nur im geringstmöglichen Umfang weitergegeben.
 - (f) Ist dem Australian Customs and Border Protection Service bekannt, dass Daten eines Bürgers eines Mitgliedstaates oder einer in einem Mitgliedstaat ansässigen Person weitergegeben werden, sind die zuständigen Behörden des betreffenden Mitgliedstaates zum frühestmöglichen Zeitpunkt entsprechend zu unterrichten.
 - (g) Der Australian Customs and Border Protection Service hat von der empfangenden Drittstaatsbehörde die Zusicherung erhalten, dass die weitergegebenen Daten nur solange gespeichert werden, bis die Untersuchung oder die strafrechtliche Verfolgung in den betreffenden Fällen abgeschlossen oder die Strafe vollstreckt ist oder bis sie nicht mehr für die in Artikel 3 Absatz 4 genannten Zwecke benötigt werden und in jedem Falle nicht länger als notwendig.
 - (h) Der Australian Customs and Border Protection Service hat von der empfangenden Drittstaatsbehörde die Zusicherung erhalten, dass sie die PNR-Daten ihrerseits nicht weitergibt.
 - (i) Der Australian Customs and Border Protection Service stellt gegebenenfalls sicher, dass der Fluggast über die Weitergabe der ihn betreffenden PNR-Daten unterrichtet wird.

2. Werden analytische Informationen übertragen, die im Rahmen dieses Abkommens erlangte PNR-Daten enthalten, sind die in diesem Artikel festgelegten Garantien für diese Daten zu beachten.
3. Dieser Artikel steht einer gegebenenfalls notwendigen Weitergabe von PNR-Daten für Zwecke von Artikel 3 Absatz 4 nicht entgegen.

KAPITEL III

EINZELHEITEN DER DATENÜBERMITTLUNG

Artikel 20

Übermittlungsmethode

Für die Zwecke dieses Abkommens stellen die Parteien sicher, dass die Fluggesellschaften dem Australian Customs and Border Protection Service die PNR-Daten ausschließlich im „Push“-Verfahren und unter Beachtung folgender Verfahrensbedingungen übermitteln:

- (a) Die Fluggesellschaften übermitteln die PNR-Daten auf elektronischem Wege entsprechend den technischen Erfordernissen des Australian Customs and Border Protection Service oder im Falle technischer Störungen auf jede sonstige geeignete Weise, die ein angemessenes Datensicherheitsniveau gewährleistet.
- (b) Die Fluggesellschaften übermitteln die PNR-Daten unter Verwendung eines vereinbarten Übermittlungsformats.
- (c) Die Fluggesellschaften übermitteln die PNR-Daten in sicherer Weise unter Verwendung der vom Australian Customs and Border Protection Service geforderten gemeinsamen Protokolle.

Artikel 21

Häufigkeit der Datenübermittlung

1. Die Parteien stellen sicher, dass die Fluggesellschaften alle angeforderten PNR-Daten in der in Artikel 20 beschriebenen Weise an den Australian Customs and Border Protection Service übermitteln; je Flug werden die Daten zu höchstens fünf planmäßigen Zeitpunkten übermittelt, wobei die erste Übermittlung bis zu 72 Stunden vor dem planmäßigen Abflug erfolgen kann. Der Australian Customs and Border Protection Service teilt den Fluggesellschaften die Übermittlungszeitpunkte mit.
2. In Fällen, in denen Hinweise darauf vorliegen, dass ein frühzeitiger Zugang zu den Daten notwendig ist, um auf eine bestimmte Gefahr im Zusammenhang mit terroristischen Straftaten oder grenzübergreifender schwerer Kriminalität zu reagieren, kann der Australian Customs and Border Protection Service die PNR-Daten bereits vor der ersten planmäßigen Übermittlung von einer Fluggesellschaft verlangen. Der Australian Customs and Border Protection Service nutzt diesen

Ermessensspielraum mit aller Umsicht und unter Wahrung der Verhältnismäßigkeit sowie ausschließlich unter Einsatz des „Push“-Verfahrens.

3. In Fällen, in denen Hinweise darauf vorliegen, dass ein Zugang zu den Daten notwendig ist, um auf eine bestimmte Gefahr im Zusammenhang mit terroristischen Straftaten oder grenzübergreifender schwerer Kriminalität zu reagieren, kann der Australian Customs and Border Protection Service die PNR-Daten auch zwischen oder nach den in Absatz 1 genannten planmäßigen Übermittlungen von einer Fluggesellschaft verlangen. Der Australian Customs and Border Protection Service nutzt diesen Ermessensspielraum mit aller Umsicht und unter Wahrung der Verhältnismäßigkeit sowie ausschließlich unter Einsatz des „Push“-Verfahrens.

KAPITEL IV

DURCHFÜHRUNGS- UND SCHLUSSBESTIMMUNGEN

Artikel 22

Ausnahmeverbot und Zusammenhang mit anderen Instrumenten

1. Durch dieses Abkommen werden keinerlei Rechte oder Vergünstigungen für Personen oder Einrichtungen privater oder öffentlicher Art begründet oder auf diese übertragen. Jede Partei sorgt dafür, dass dieses Abkommen ordnungsgemäß durchgeführt wird.
2. Durch dieses Abkommen werden keine im australischen Recht verankerten Rechte oder Garantien eingeschränkt.
3. Dieses Abkommen weicht in keinem Punkt von bestehenden Pflichten aus bilateralen Rechtshilfeinstrumenten ab, die zwischen Australien und Mitgliedstaaten der Europäischen Union vereinbart wurden, um auf Antrag Daten zu erhalten, die in strafrechtlichen Verfahren in Fällen von Terrorismus oder grenzübergreifender schwerer Kriminalität als Beweismittel verwendet werden.

Artikel 23

Streitbeilegung und Aussetzung des Abkommens

1. Bei Streitigkeiten über die Auslegung, Anwendung oder Durchführung dieses Abkommens sowie allen damit zusammenhängenden Fragen konsultieren die Parteien einander, um eine einvernehmliche Lösung zu erzielen, die es beiden Parteien ermöglicht, die getroffene Vereinbarung innerhalb eines angemessenen Zeitraums zu erfüllen.
2. Falls die Konsultationen keine Beilegung des Streits bewirken, kann jede Partei durch schriftliche Notifizierung auf diplomatischem Wege die Anwendung dieses Abkommens aussetzen; sofern nichts anderes vereinbart wurde, wird eine solche Aussetzung 120 Tage nach dem Datum ihrer Notifizierung wirksam.

3. Jegliche Aussetzung endet, sobald der Streit zur Zufriedenheit Australiens und der EU beigelegt ist.
4. Unbeschadet der Aussetzung dieses Abkommens werden alle Daten, über die der Australian Customs and Border Protection Service aufgrund dieses Abkommens verfügt, weiter im Einklang mit den Garantien dieses Abkommens einschließlich der Bestimmungen über die Aufbewahrung und Löschung von Daten verarbeitet.

Artikel 24

Konsultation und Überprüfung

1. Die Parteien notifizieren einander, gegebenenfalls vor der Annahme des Abkommens, jegliche Änderung ihrer Rechts- und Verwaltungsvorschriften, die die Durchführung dieses Abkommens wesentlich beeinträchtigen könnte. Jegliche Bezugnahme in diesem Abkommen auf australische Rechtsvorschriften erstreckt sich auch auf etwaige Folgevorschriften.
2. Die Parteien überprüfen gemeinsam ein Jahr nach Inkrafttreten dieses Abkommens und dann regelmäßig während dessen weiterer Laufzeit und zusätzlich auf Ersuchen einer Partei die Durchführung dieses Abkommens und jegliche damit zusammenhängende Angelegenheit. Die Parteien vereinbaren, dass sich die Überprüfung insbesondere auf das Verfahren zur Unkenntlichmachung von Daten gemäß Artikel 16 Absatz 1 Buchstabe b, etwaige Schwierigkeiten im Zusammenhang mit der operativen Effizienz und der Kosteneffizienz des Verfahrens sowie die im Rahmen anderer bewährter PNR-Regelungen einschließlich der EU-Regelung gewonnenen Erfahrungen mit ähnlichen Verfahren erstreckt. Sollte kein operativ effizientes und kosteneffizientes Verfahren verfügbar sein, wird der Zugang zu den Daten durch Archivierung beschränkt und ist nur noch in der für anonymisierte Daten geltenden Weise gemäß Artikel 16 möglich.
3. Die Parteien vereinbaren vor einer gemeinsamen Überprüfung deren Einzelheiten und unterrichten einander über die Zusammensetzung ihrer jeweiligen Überprüfungsteams. Für die Zwecke der gemeinsamen Überprüfung wird die Europäische Union durch die Europäische Kommission und Australien durch den Australian Customs and Border Protection Service vertreten. Die Überprüfungsteams können auch Fachleute für Datenschutz und die Durchsetzung von Rechtsvorschriften umfassen. Vorbehaltlich geltender Rechtsvorschriften müssen die an der gemeinsamen Überprüfung Beteiligten die Vertraulichkeit der Beratungen wahren und angemessene Sicherheitsüberprüfungen bestanden haben. Für die Zwecke der gemeinsamen Überprüfung stellt der Australian Customs and Border Protection Service den Zugang zu den einschlägigen Unterlagen und Systemen sowie zu dem betreffenden Personal sicher.
4. Die Parteien evaluieren das Abkommen und insbesondere dessen operative Effizienz spätestens vier Jahre nach seinem Inkrafttreten.
5. Im Anschluss an eine gemeinsame Überprüfung unterbreitet die Europäische Kommission dem Europäischen Parlament und dem Rat der Europäischen Union

einen Bericht. Australien wird Gelegenheit zur schriftlichen Stellungnahme gegeben, die dem Bericht beigelegt wird.

6. Da sich die Rahmenbedingungen dieses Abkommens durch die Einführung eines EU-eigenen PNR-Systems ändern könnten, konsultieren die Parteien einander im Hinblick auf die Notwendigkeit einer entsprechenden Anpassung des Abkommens, falls ein solches System beschlossen wird.

Artikel 25

Kündigung

1. Dieses Abkommen kann von jeder Partei durch schriftliche Notifizierung auf diplomatischem Wege jederzeit gekündigt werden. Die Kündigung wird 120 Tage nach dem Tag ihres Eingangs oder nach Vereinbarung wirksam.
2. Unbeschadet einer Kündigung dieses Abkommens werden alle Daten, über die der Australian Customs and Border Protection Service aufgrund dieses Abkommens verfügt, weiter im Einklang mit den Garantien dieses Abkommens einschließlich der Bestimmungen über die Aufbewahrung und Löschung von Daten verarbeitet.

Artikel 26

Laufzeit

1. Vorbehaltlich Artikel 25 wird dieses Abkommen für einen Zeitraum von fünf Jahren ab dem Zeitpunkt seines Inkrafttretens geschlossen.
2. Bei Ablauf des in Absatz 1 genannten Zeitraums sowie jedes Verlängerungszeitraums gemäß diesem Absatz wird das Abkommen für einen Folgezeitraum von sieben Jahren verlängert, sofern nicht eine Partei der anderen mindestens zwölf Monate zuvor auf diplomatischem Wege schriftlich ihre Absicht notifiziert, das Abkommen nicht zu verlängern.
3. Unbeschadet des Auslaufens dieses Abkommens werden alle Daten, über die der Australian Customs and Border Protection Service aufgrund dieses Abkommens verfügt, weiter im Einklang mit den Garantien dieses Abkommens einschließlich der Bestimmungen über die Aufbewahrung und Löschung von Daten verarbeitet.

Artikel 27

Vor Inkrafttreten dieses Abkommens erhaltene PNR-Daten

Australien behandelt jegliche PNR-Daten, die von dem Australian Customs and Border Protection Service zum Zeitpunkt des Inkrafttretens dieses Abkommens gehalten werden, im Einklang mit dessen Bestimmungen. Vor dem 1. Januar 2015 sind jedoch keine Daten unkenntlich zu machen.

Artikel 28

Räumlicher Geltungsbereich

1. Vorbehaltlich der Absätze 2 bis 4 gilt dieses Abkommen für das Gebiet, in dem der Vertrag über die Europäische Union und der Vertrag über die Arbeitsweise der Europäischen Union angewandt werden, und für das Hoheitsgebiet Australiens.
2. Dieses Abkommen gilt nur dann für Dänemark, das Vereinigte Königreich oder Irland, wenn die Europäische Kommission Australien schriftlich notifiziert, dass Dänemark, das Vereinigte Königreich oder Irland beschlossen hat, sich diesem Abkommen zu unterwerfen.
3. Notifiziert die Europäische Kommission Australien vor Inkrafttreten dieses Abkommens, dass es auf Dänemark, das Vereinigte Königreich oder Irland Anwendung findet, gilt dieses Abkommen für das Hoheitsgebiet des betreffenden Staates vom gleichen Tag an wie für die durch dieses Abkommen gebundenen EU-Mitgliedstaaten.
4. Notifiziert die Europäische Kommission Australien nach Inkrafttreten dieses Abkommens, dass es auf Dänemark, das Vereinigte Königreich oder Irland Anwendung findet, gilt dieses Abkommen für das Hoheitsgebiet des betreffenden Staates ab dem ersten Tag nach dem Empfang der Notifizierung durch Australien.

Artikel 29

Schlussbestimmungen

1. Dieses Abkommen tritt am ersten Tag des Monats in Kraft, der auf den Tag folgt, an dem die Parteien einander den Abschluss der einschlägigen internen Verfahren notifizieren.
2. Dieses Abkommen ersetzt das Abkommen zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) aus der Europäischen Union und deren Übermittlung durch die Fluggesellschaften an die australische Zollbehörde vom 30. Juni 2008, welches mit dem Inkrafttreten dieses Abkommens außer Kraft tritt.

Geschehen zu ... am ... in zwei Urschriften in englischer Sprache. Das Abkommen wird ebenfalls in bulgarischer, dänischer, deutscher, estnischer, finnischer, französischer, griechischer, italienischer, lettischer, litauischer, maltesischer, niederländischer, polnischer, portugiesischer, rumänischer, schwedischer, slowakischer, slowenischer, spanischer, tschechischer und ungarischer Sprache abgefasst. Im Falle einer Abweichung zwischen den Sprachfassungen ist die englische Fassung maßgeblich.

FÜR DIE EUROPÄISCHE UNION

+++++

FÜR AUSTRALIEN

+++++

Anhang 1

In Artikel 2 Buchstabe f genannte Elemente der PNR-Daten, die die Luftverkehrsgesellschaften dem Australian Customs and Border Protection Service nur in dem Maße überlassen müssen, als sie bereits erhoben werden:

- (1) PNR-Buchungscode (Record Locator Code)
- (2) Datum der Buchung bzw. der Ausstellung des Flugscheins
- (3) Datum bzw. Daten des geplanten Flugs
- (4) Name(n)
- (5) Verfügbare Vielflieger- und Bonus-Daten (d.h. Gratisflugscheine, Upgrades usw.)
- (6) Andere Namen in dem PNR-Datensatz, einschließlich der Anzahl der in dem Datensatz erfassten Reisenden
- (7) Sämtliche verfügbaren Kontaktinformationen, einschließlich Informationen zur Kundenidentifizierung
- (8) Sämtliche verfügbaren Zahlungs-/Abrechnungsinformationen (ohne weitere Transaktionsdetails für eine Kreditkarte oder ein Konto, die nicht mit der die Reise betreffenden Transaktion verknüpft sind)
- (9) Von dem jeweiligen PNR-Datensatz erfasste Reiseroute
- (10) Reisebüro
- (11) Code-Sharing-Informationen
- (12) Informationen über Buchungssplitting bzw. -teilung
- (13) Reisestatus des Fluggastes (einschließlich Bestätigungen und Eincheckstatus)
- (14) Flugscheininformationen (Ticketing Information), einschließlich Flugscheinnummer, Hinweis auf einen etwaigen einfachen Flug (One Way Ticket) und automatische Tarifanzeige (Automatic Ticket Fare Quote)
- (15) Sämtliche Informationen zum Gepäck
- (16) Sitzplatznummer und sonstige Sitzplatzinformationen
- (17) Allgemeine Eintragungen einschließlich OSI, SSI und SSR-Informationen
- (18) Etwaige APIS-Informationen
- (19) Historie aller Änderungen in Bezug auf die unter den Nummern 1 bis 18 aufgeführten PNR-Daten

Anhang 2

Verzeichnis der anderen australischen staatlichen Stellen, denen der Australian Customs and Border Protection Service die Nutzung von PNR-Daten gestatten darf:

- (1) Australian Crime Commission
- (2) Australian Federal Police
- (3) Australian Security Intelligence Organisation
- (4) Commonwealth Director of Public Prosecutions
- (5) Department of Immigration and Citizenship
- (6) Office of Transport Security, Department of Infrastructure and Transport