II

(Nicht veröffentlichungsbedürftige Rechtsakte)

KOMMISSION

ENTSCHEIDUNG DER KOMMISSION

vom 14. Mai 2004

über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Passenger Name Records enthalten sind, welche dem United States Bureau of Customs and Border Protection übermittelt werden

(Bekannt gegeben unter Aktenzeichen K(2004) 1914)

(Text von Bedeutung für den EWR)

(2004/535/EG)

DIE KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft,

gestützt 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 Datenverkehr [1], insbesondere auf Artikel 25 Absatz 6,

in Erwägung nachstehender Gründe:

(1) Nach Richtlinie 95/46/EG müssen die Mitgliedstaaten dafür sorgen, dass die Übermittlung personenbezogener Daten in ein Drittland nur dann erfolgt, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet und die Rechtsvorschriften der Mitgliedstaaten zur Umsetzung anderer Bestimmungen der Richtlinie erfüllt sind, bevor die Übermittlung erfolgt.

(2) Die Kommission ist berechtigt, festzustellen, dass ein Drittland einen angemessenen Datenschutz gewährleistet. In diesem Fall können die Mitgliedstaaten personenbezogene Daten übermitteln, ohne dass zusätzliche Garantien erforderlich sind.

(3) Nach der Richtlinie 95/46/EG sind bei der Bewertung des Datenschutzniveaus alle Umstände zu berücksichtigen, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen, sowie insbesondere eine Reihe sonstiger bei der Datenübermittlung wichtiger und in Artikel 25 Absatz 2 der Richtlinie aufgeführter Merkmale.

(4) Der „Passenger Name Record" (PNR) (Fluggastdatensatz) im Luftverkehr ist ein Datensatz mit Reiseangaben für den einzelnen Passagier; er enthält alle Informationen, die für die Bearbeitung und Kontrolle für die bei der Buchung beteiligten und für die sonstigen beteiligten Fluggesellschaften erforderlich sind. Zum Zweck dieser Entscheidung umfassen die Begriffe „Passagier" und „Passagiere" die Mitglieder der Besatzung. „An der Buchung beteiligte Fluggesellschaften" bedeutet eine Fluggesellschaft, bei der der Passagier ursprüngliche Reservierungen vornahm, oder zusätzliche, nach dem Antritt der Reise. „Beteiligte Fluggesellschaft" ist jede Fluggesellschaft, an die die buchende Fluggesellschaft für einen oder mehrere Flüge eine Reservierungsanfrage für einen Passagier gerichtet hat.

(5) Das United States Bureau of Customs and Border Protection (CBP — Zoll- und Grenzschutzbehörde der Vereinigten Staaten) des Departments of Homeland Security (DHS) fordert von allen Fluggesellschaften, die Passagierflüge aus dem Ausland in die Vereinigten Staaten oder von den Vereinigten Staaten ins Ausland anbieten, dass sie ihm elektronischen Zugriff auf den PNR gewähren, soweit dieser PNR in den automatischen Buchungs-/Abfertigungssystemen der Fluggesellschaften erfasst und gespeichert wird.

(6) Rechtsgrundlagen für die geforderte Übermittlung personenbezogener Daten aus dem PNR an das CBP sind ein im November 2001 in den USA erlassenes Gesetz [2] sowie Durchführungsvorschriften [3], die das CBP aufgrund dieses Gesetzes erlassen hat.

[1] ABl. L 281 vom 23.11.1995, S. 31. Richtlinie zuletzt geändert durch die Verordnung (EG) Nr. 1882/2003 (ABl. L 284 vom 31.10.2003, S. 1).

[2] Title 49, United States Code, section 44909(c)(3).

[3] Title 19, Code of Federal Regulations, section 122.49b.

(7) Diese Rechtsvorschriften betreffen die Verbesserung der Sicherheitslage in den USA sowie die Voraussetzungen, unter denen Personen dort ein- und ausreisen dürfen, Angelegenheiten, die die USA in Ausübung ihrer staatlichen Souveränität regeln dürfen. Darüber hinaus stehen die Auflagen in keinerlei Widerspruch zu internationalen Verpflichtungen, die die Vereinigten Staaten eingegangen sind. Die Vereinigten Staaten sind ein demokratischer Rechtsstaat, in dem die bürgerlichen Freiheiten traditionell einen hohen Stellenwert haben. Die Legitimität des Gesetzgebungsverfahrens sowie die Stärke und Unabhängigkeit der Justiz in den USA stehen außer Frage. Darüber hinaus ist die Pressefreiheit ein starker Garant gegen Verletzungen der Grundrechte.

(8) Die Gemeinschaft unterstützt die USA uneingeschränkt im Kampf gegen den Terrorismus innerhalb der Bestimmungen des Gemeinschaftsrechts. Das Gemeinschaftsrecht sieht eine notwendige Ausgewogenheit zwischen Sicherheitsbedenken und Fragen des Datenschutzes vor. Beispielsweise ermöglicht Artikel 13 der Richtlinie 95/46/EG den Mitgliedstaaten, Rechtsvorschriften zu erlassen, die bestimmte Erfordernisse der genannten Richtlinie einschränken, sofern eine solche Einschränkung für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit oder die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten erforderlich ist.

(9) Die Datenübermittlungen betreffen bestimmte für die Datenverarbeitung Verantwortliche, nämlich Fluggesellschaften, die Flüge zwischen der Gemeinschaft und den USA durchführen, sowie einen einzigen Empfänger in den USA, nämlich das CBP.

(10) Jede Vereinbarung zur Schaffung einer Rechtsgrundlage für die Übermittlung von PNR in die USA, insbesondere die vorliegende Entscheidung, sollte befristet sein. Es ist eine Laufzeit von dreieinhalb Jahren vereinbart worden. Während dieses Zeitraums können sich die Rahmenbedingungen wesentlich verändern. Die Gemeinschaft und die USA sind sich darin einig, dass eine Überprüfung der Vereinbarungen erforderlich sein wird.

(11) Die Verarbeitung personenbezogener Daten aus den dem CBP übermittelten PNR durch das CBP unterliegt den Bedingungen, die in der „Verpflichtungserklärung des Department of Homeland Security, Bureau of Customs and Border Protection (CBP)"(nachstehend „Verpflichtungserklärung" genannt) vom 11. Mai 2004 festgelegt sind, sowie den Rechtsvorschriften der Vereinigten Staaten, die in dieser Verpflichtungserklärung aufgeführt sind.

(12) Was das innerstaatliche Recht der Vereinigten Staaten angeht, so ist das Informationsfreiheitsgesetz (Freedom of Information Act — FOIA) in diesem Zusammenhang insofern von Bedeutung, als es die Bedingungen regelt, unter denen sich das CBP einem Offenlegungsantrag widersetzen und die PNR geheim halten darf. Darüber hinaus regelt das Gesetz die Offenlegung von PNR gegenüber den betroffenen Personen, die eng verknüpft ist mit dem Auskunftsrecht des Betroffenen. Es gilt unterschiedslos für Staatsangehörige der USA und Ausländer.

(13) Was die Verpflichtungserklärung angeht, so werden — oder wurden bereits — gemäß deren Absatz 44 einzelne Verpflichtungen in Gesetze, Verordnungen, Richtlinien oder sonstige Anweisungen in den USA aufgenommen und haben damit bereits bzw. werden ein unterschiedliches Maß an Rechtswirkungen erhalten. Die Verpflichtungserklärung wird unter der Zuständigkeit des DHS in vollem Wortlaut im Federal Register veröffentlicht. Sie stellt eine ernsthafte und reiflich überlegte politische Verpflichtung des DHS dar, außerdem wird ihre Einhaltung einer gemeinsamen Überprüfung durch die Vereinigten Staaten und die Gemeinschaft unterzogen. Gegen eine Nichteinhaltung der Verpflichtungen könnte je nach Bedarf auf rechtlichem, administrativem und politischem Wege vorgegangen werden, wobei eine anhaltende Missachtung letztlich zur Aussetzung der Wirkung der vorliegenden Entscheidung führen würde.

(14) Die Vorschriften, nach denen das CBP aufgrund der Gesetze der Vereinigten Staaten und der Verpflichtungserklärung die Passagierdaten aus den PNR verarbeiten werden, erfüllen die Grundanforderungen für ein angemessenes Schutzniveau für natürliche Personen.

(15) Was den Grundsatz der Zweckbindung angeht, so werden die personenbezogenen Daten von Passagieren, die in den dem CBP übermittelten PNR enthalten sind, für einen festgelegten Zweck verwendet und anschließend nur weiterverwendet oder weiterübermittelt, soweit dies mit dem Zweck der ursprünglichen Übermittlung vereinbar ist. PNR-Daten werden ausschließlich verwendet für Zwecke der Verhütung und Bekämpfung des Terrorismus und damit verknüpfter Straftaten, anderer schwerer, ihrem Wesen nach länderübergreifender Straftaten, einschließlich der internationalen organisierten Kriminalität, und der Flucht vor Haftbefehlen bzw. vor Gewahrsamnahme im Zusammenhang mit jenen Straftaten.

(16) Was die Grundsätze der Datenqualität und der Verhältnismäßigkeit angeht, die vor dem Hintergrund des wichtigen öffentlichen Interesses zu betrachten sind, aufgrund dessen die Übermittlung der PNR-Daten erfolgt, so werden die PNR-Daten, die an das U.S. CBP übermittelt werden, von dieser Behörde nicht im nachhinein geändert. Es werden maximal 34 PNR-Kategorien übermittelt, und die US-Behörden werden weitere Anforderungen nur nach Rücksprache mit der Kommission festlegen. Zusätzliche personenbezogene Daten, die unmittelbar aufgrund bestimmter PNR-Daten benötigt werden, werden von nichtstaatlichen Stellen nur auf rechtlich zulässige Weise eingeholt. Generell werden PNR nach spätestens 3 Jahren und 6 Monaten gelöscht; hiervon ausgenommen sind Daten, auf die für bestimmte Ermittlungen zugegriffen worden ist oder auf die anderweitig manuell zugegriffen wurde.

(17) Was den Transparenzgrundsatz angeht, so wird das CBP die Reisenden über den Zweck der Datenübermittlung und der Datenverarbeitung informieren und ihnen Angaben über den für die Verarbeitung Verantwortlichen im Drittland sowie weitere Informationen zur Verfügung stellen.

(18) Was den Grundsatz der Sicherheit betrifft, so wird das CBP technische und organisatorische Sicherheitsmaßnahmen ergreifen, die den mit der Verarbeitung verbundenen Risiken angemessen sind.

(19) Die Rechte auf Auskunft und Berichtigung werden anerkannt: Die betroffene Person kann eine Kopie der PNR-Daten anfordern sowie die Berichtigung unrichtiger Daten verlangen. Die vorgesehenen Ausnahmen sind im Großen und Ganzen mit den Einschränkungen vergleichbar, die Artikel 13 der Richtlinie 95/46/EG den Mitgliedstaaten ermöglicht.

(20) Eine Weiterübermittlung erfolgt nur von Fall zu Fall an andere — auch ausländische — staatliche Behörden mit Terrorismusbekämpfungs- oder Vollzugsaufgaben zu Zwecken, die der zugesagten Zweckbeschränkung gerecht werden. Eine Weiterübermittlung kann auch dann erfolgen wenn die Offenlegung zum Schutz lebenswichtiger Interessen des Betroffenen oder anderer Personen, insbesondere im Falle erheblicher Gesundheitsrisiken, erforderlich ist, ferner im Zusammenhang mit Strafprozessen oder aufgrund anderer gesetzlicher Erfordernisse. Behörden, welche derartige Daten empfangen, dürfen diese Daten aufgrund der ausdrücklichen Offenlegungsbestimmungen nur zu jenen Zwecken verwenden, außerdem dürfen sie die Daten nicht ohne Zustimmung des CBP weiterübermitteln. Keine andere ausländische, zentralstaatliche, bundesstaatliche oder örtliche Behörde hat direkten elektronischen Zugriff auf PNR-Daten, die in Datenbanken der CBP gespeichert sind. Das CBP wird die Offenlegung von PNR gegenüber der Allgemeinheit unter Berufung auf die Ausnahmeregelungen in den betreffenden Bestimmungen des FOIA ablehnen.

(21) Das CBP verwendet keine sensiblen Daten im Sinne des Artikels 8 der Richtlinie 95/46/EG und verpflichtet sich, Instrumente zur Löschung solcher Daten einzuführen und die Daten in der Zwischenzeit nicht zu verwenden, bis ein Filtersystem in Betrieb genommen ist, das sie aus den an die Vereinigten Staaten übermittelten PNR herausfiltert.

(22) Was die Durchsetzungsmechanismen angeht, die die Befolgung dieser Grundsätze durch das CBP sicherstellen sollen, so erhalten die Mitarbeiter des CBP entsprechende Schulung und Informationen, ferner ist die Möglichkeit von Sanktionen gegen einzelne Mitarbeiter vorgesehen. Im Allgemeinen wird der Chief Privacy Officer (Datenschutzbeauftragte) des DHS, bei dem es sich zwar um einen Beamten des DHS handelt, der aber organisatorisch weitgehend autonom ist und jährlich dem Kongress Bericht erstatten muss, darüber wachen, dass das CBP den Datenschutz einhält. Personen, deren PNR-Daten übermittelt worden sind, können sich mit Beschwerden entweder direkt oder über die Datenschutzbehörden in den Mitgliedstaaten an das CBP wenden oder, falls keine Lösung gefunden wird, an den Chief Privacy Officer des DHS. Das DHS Privacy Office wird sich umgehend mit den Beschwerden befassen, die die Datenschutzbehörden der Mitgliedstaaten im Auftrag in der Gemeinschaft ansässiger Betroffener an das Office richten, falls die Betroffenen zu der Auffassung gelangt sind, dass ihre Datenschutzbeschwerden nicht zufrieden stellend vom CBP oder vom DHS Privacy Office behandelt wurden. Die Einhaltung der Verpflichtungserklärung wird jährlich gemeinsam vom CBP in Zusammenarbeit mit dem DHS sowie einem von der Kommission geleiteten Team überprüft.

(23) Im Interesse der Transparenz und um sicherzustellen, dass die zuständigen Behörden der Mitgliedstaaten in der Lage sind, den Schutz von Personen bei der Verarbeitung ihrer personenbezogenen Daten zu gewährleisten, sind — unbeschadet der Feststellung eines angemessenen Schutzniveaus — die besonderen Umstände aufzuführen, unter denen die Aussetzung bestimmter Datenströme gerechtfertigt ist.

(24) Die Gruppe für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, die nach Artikel 29 der Richtlinie 95/46/EG eingesetzt wurde, hat Stellungnahmen über das von den US-Behörden für Passagierdaten gewährleistete Schutzniveau abgegeben, welche der Kommission während der Verhandlungen mit der DHS als Anleitung gedient haben. Die Kommission hat diese Stellungnahmen bei der Erarbeitung dieser Entscheidung zur Kenntnis genommen [1].

(25) Die in dieser Entscheidung vorgesehenen Maßnahmen stehen im Einklang mit der Stellungnahme des Ausschusses, der gemäß Artikel 31 Absatz 1 der Richtlinie 95/46/EG eingesetzt wurde —

HAT FOLGENDE ENTSCHEIDUNG ERLASSEN:

Artikel 1

Im Hinblick auf Artikel 25 Absatz 2 der Richtlinie 95/46/EG wird festgestellt, dass das United States Bureau of Customs and Border Protection (CBP) auf der Grundlage der als Anhang angefügten Verpflichtungserklärung einen angemessenen Schutz bietet für PNR-Daten über Flüge in die oder aus den Vereinigten Staaten, die aus der Gemeinschaft übermittelt werden.

Artikel 2

Diese Entscheidung betrifft die Angemessenheit des Schutzes, den das CBP im Hinblick auf die Anforderungen des Artikels 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet; andere zur Umsetzung sonstiger Vorschriften der Richtlinie festgelegte Bestimmungen und Einschränkungen hinsichtlich der Verarbeitung personenbezogener Daten in den Mitgliedstaaten bleiben davon unberührt.

[1] Stellungnahme 6/2002 zur Übermittlung von Informationen aus Passagierlisten und anderen Daten von Fluggesellschaften an die Vereinigten Staaten, angenommen von der Datenschutzgruppe am 24. Oktober 2002, abrufbar unter http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp66_de.pdf
Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, angenommen von der Datenschutzgruppe am 13. Juni 2003, abrufbar unter http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf
Stellungnahme 2/2004 zur Angemessenheit des Schutzes der personenbezogenen Daten, die in den Fluggastdatensätzen (Passenger Name Records — PNR) enthalten sind, welche dem United States Bureau of Customs and Border Protection (US CBP — Zoll- und Grenzschutzbehörde der Vereinigten Staaten) übermittelt werden sollen, angenommen von der Datenschutzgruppe am 29. Januar 2004, abrufbar unter: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_de.pdf

Artikel 3

1. Unbeschadet ihres Rechts, Maßnahmen zur Durchsetzung einzelstaatlicher Vorschriften zu ergreifen, die gemäß anderen Bestimmungen als denen des Artikels 25 der Richtlinie 95/46/EG angenommen wurden, können die zuständigen Behörden in den Mitgliedstaaten von ihrem Recht Gebrauch machen, zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten die Datenübermittlung an das CBP auszusetzen,

a) wenn eine zuständige US-Behörde feststellt, dass das CBP die geltenden Datenschutzvorschriften nicht einhält, oder

b) wenn eine hohe Wahrscheinlichkeit besteht, dass die im Anhang enthaltenen Schutzvorschriften verletzt werden, Grund zur Annahme besteht, dass das CBP nicht rechtzeitig angemessene Maßnahmen ergreift bzw. ergreifen wird, um den betreffenden Fall zu lösen, die Fortsetzung der Datenübermittlung den betroffenen Personen einen unmittelbar bevorstehenden schweren Schaden zuzufügen droht und die zuständigen Behörden in den Mitgliedstaaten sich unter den gegebenen Umständen in angemessener Weise bemüht haben, das CBP zu benachrichtigen, und ihm Gelegenheit zur Stellungnahme gegeben haben.

2. Die Aussetzung wird beendet, sobald sichergestellt ist, dass die Datenschutzvorschriften befolgt werden und die zuständigen Behörden in den jeweiligen Mitgliedstaaten davon in Kenntnis gesetzt sind.

Artikel 4

1. Die Mitgliedstaaten informieren die Kommission unverzüglich, wenn Maßnahmen gemäß Artikel 3 ergriffen wurden.

2. Die Mitgliedstaaten und die Kommission benachrichtigen einander auch über jedwede Änderung der Datenschutzvorschriften sowie über Fälle, in denen die Maßnahmen der für die Einhaltung der Vorschriften gemäß dem Anhang durch das CBP verantwortlichen Einrichtungen nicht ausreichen, um die Einhaltung zu gewährleisten.

3. Ergeben die gemäß Artikel 3 und gemäß den Absätzen 1 und 2 des vorliegenden Artikels gewonnenen Erkenntnisse, dass die Grundanforderungen für ein angemessenes Schutzniveau für natürliche Personen nicht mehr gewährleistet sind, oder dass eine für die Einhaltung der Vorschriften gemäß dem Anhang durch das CBP verantwortliche Einrichtung ihre Aufgabe nicht wirksam erfüllt, so wird das CBP hiervon benachrichtigt und erforderlichenfalls das in Artikel 31 Absatz 2 der Richtlinie 95/46/EG genannte Verfahren zwecks Aufhebung oder Aussetzung der vorliegenden Entscheidung angewandt.

Artikel 5

Die Anwendung der vorliegenden Entscheidung wird überwacht, und relevante Erkenntnisse werden dem nach Artikel 31 der Richtlinie 95/46/EG eingesetzten Ausschuss mitgeteilt; dazu zählen auch Erkenntnisse, die sich auf die Beurteilung in Artikel 1 dieser Entscheidung auswirken könnten, wonach ein angemessenes Schutzniveau im Sinne des Artikels 25 der Richtlinie 95/46/EG gewährleistet ist für PNR von Fluggästen, die an das CBP übermittelt werden.

Artikel 6

Die Mitgliedstaaten ergreifen binnen vier Monaten nach der Bekanntmachung dieser Entscheidung alle für ihre Umsetzung erforderlichen Maßnahmen.

Artikel 7

Diese Entscheidung läuft 3 Jahre und 6 Monate nach dem Datum ihrer Bekanntmachung aus, es sei denn, sie wird nach dem Verfahren von Artikel 31 Absatz 2 der Richtlinie 95/46/EG verlängert.

Artikel 8

Diese Entscheidung ist an alle Mitgliedstaaten gerichtet.

Brüssel, den 14. Mai 2004

Für die Kommission

Frederik BOLKESTEIN

Mitglied der Kommission

ANHANG

VERPFLICHTUNGSERKLÄRUNG DES *DEPARTMENT OF HOMELAND SECURITY, BUREAU OF CUSTOMS AND BORDER PROTECTION* (CBP)

Zur Unterstützung der Absicht der Europäischen Kommission (im Folgenden „die Kommission" genannt), die ihr durch Artikel 25 Absatz 6 der Richtlinie 95/46/EG („die Richtlinie") verliehenen Befugnisse auszuüben und eine Entscheidung zu verabschieden, mit der dem Bureau of Customs and Border Protection (CBP) des Department of Homeland Security ein angemessenes Datenschutzniveau bescheinigt und den Fluggesellschaften damit die Übermittlung von Passagierdaten [1] (Passenger Name Record data — PNR) ermöglicht wird, die unter Umständen in den Geltungsbereich der Richtlinie fallen, sichert das CBP Folgendes zu:

Rechtsgrundlage für den Zugriff auf PNR

1. Aufgrund der gesetzlichen Bestimmungen (title 49, United States Code, section 44909(c)(3)) und der entsprechenden (vorläufigen) Durchführungsbestimmungen (title 19, Code of Federal Regulations, section 122.49b) muss jede Fluggesellschaft, die Auslands-Passagierflüge aus den oder in die Vereinigten Staaten durchführt, dem CBP (vormals U.S. Customs Service) elektronischen Zugriff auf PNR-Daten gewähren, soweit sie mit den computergestützten Reservierungs-/Abfertigungssystemen („Reservierungssysteme") der Fluggesellschaft erhoben und darin gespeichert werden.

Nutzung von PNR-Daten durch das CBP

2. Die meisten PNR-Datenelemente kann das CBP durch Prüfung des Flugscheins und anderer Reisedokumente der betreffenden Personen im Rahmen seiner normalen Grenzkontrollbefugnisse erlangen. Wenn es diese Daten indessen in elektronischer Form erlangen kann, werden sich die Möglichkeiten des CBP zur Erleichterung des Reisens gutgläubiger Passagiere und zur Durchführung wirksamer Vorabkontrollen der Passagiere zum Zwecke der Risikobewertung beträchtlich verbessern.

3. Das CBP verwendet PNR-Daten ausschließlich zum Zwecke der Verhütung und Bekämpfung 1. des Terrorismus und damit verknüpfter Straftaten, 2. anderer schwerer länderübergreifenden Straftaten, einschließlich internationaler organisierter Kriminalität, und 3. der Flucht vor Haftbefehlen bzw. vor Ingewahrsamnahme im Zusammenhang mit den oben genannten Straftaten. Durch die Nutzung von PNR-Daten für diese Zwecke kann das CBP seine Ressourcen auf Hochrisikobereiche konzentrieren und damit das Reisen gutgläubiger Passagiere erleichtern und gewährleisten.

Verlangte Daten

4. Die Datenelemente, die das CBP verlangt, sind in Anhang „A" aufgeführt. (Diese Elemente werden für die Zwecke dieser Verpflichtungserklärung als „PNR-Daten" bezeichnet.) Das CBP verlangt zwar Zugriff auf alle vierunddreißig (34) in Anhang „A" aufgeführten Datenelemente, geht aber davon aus, dass ein individueller PNR-Datensatz nur selten alle diese Daten enthält. In den Fällen, in denen ein PNR-Datensatz nicht alle aufgeführten Datenelemente enthält, wird das CBP nicht versuchen, über das Buchungssystem der Fluggesellschaft direkten Zugriff auf andere PNR-Daten zu erlangen, die nicht in Anhang „A" aufgeführt sind.

5. Was die „OSI"- und „SSI/SSR"-Datenelemente angeht (die normalerweise als Felder für allgemeine Anmerkungen oder als offene Datenfelder bezeichnet werden), so wird das automatische System des CBP diese Felder nach allen anderen in Anhang „A" aufgeführten Datenelementen durchsuchen. Die Mitarbeiter des CBP werden nicht befugt sein, die vollständigen OSI- und SSI/SSR-Felder manuell zu durchsuchen, es sei denn, das CBP hat die Person, auf die sich der PNR-Datensatz bezieht, als besonders risikoträchtig („high risk") in Bezug auf einen oder mehrere der in Absatz 3 aufgeführten Sachverhalte eingestuft.

6. Zusätzliche personenbezogene Daten, die unmittelbar aufgrund bestimmter PNR-Daten angefordert werden, werden von nichtstaatlichen Stellen nur auf legalem Weg, bei Bedarf z. B. im Rahmen der gegenseitigen Rechtshilfe, und nur für die in Absatz 3 genannten Zwecke eingeholt. Enthält ein PNR-Datensatz beispielsweise Kreditkarteninformationen, können Daten über diesbezügliche Kontenbewegungen eingeholt werden, sofern die entsprechenden gesetzlichen Voraussetzungen erfüllt sind, beispielsweise wenn eine Vorladung vor eine „Grand Jury" oder eine gerichtliche Verfügung vorliegt, oder andere rechtliche Voraussetzungen vorliegen. Der Zugriff auf Daten über E-Mail-Konten, die sich aus einem PNR-Datensatz ergeben, ist ebenfalls an die in den USA geltenden gesetzlichen Voraussetzungen geknüpft, d. h., je nach Art der gewünschten Daten, an gerichtliche Vorladungen, Verfügungen, Haftbefehle oder andere gesetzlichen Verfahren.

7. Das CBP wird sich mit der Europäischen Kommission zur Überarbeitung der Liste der geforderten PNR-Datenelemente (Anhang „A") abstimmen, bevor es eine solche Überarbeitung vornimmt, wenn es feststellt, dass Fluggesellschaften ihren Systemen PNR-Felder hinzugefügt haben, die nach Auffassung des CBP dessen Möglichkeiten zur Risikobewertung erheblich verbessern, oder wenn die Umstände darauf hinweisen, dass ein bis dahin nicht gefordertes PNR-Feld benötigt wird für die begrenzten Zwecke, die unter Absatz 3 dieser Verpflichtungserklärung beschrieben werden.

[1] Für den Zweck dieser Verpflichtungserklärung beinhalten die Worte „Passagier" und „Passagiere" Besatzungsmitglieder.

8. Das CBP kann Daten en bloc an die Transportation Security Administration (TSA) weitergeben, damit die TSA ihr computergestütztes Verfahren zur Vorabkontrolle CAPPS II (Computer Assisted Passenger Prescreening System II) erproben kann. Eine solche Weitergabe erfolgt erst, nachdem PNR-Daten von US-Inlandsflügen zur Erprobung freigegeben wurden. Gemäß dieser Bestimmung weitergegebene PNR-Daten werden weder von der TSA noch von einer anderen, direkt an der Erprobung beteiligten Partei länger als dafür notwendig aufbewahrt, sie werden auch nicht an Dritte weitergegeben [2]. Der Verarbeitungszweck beschränkt sich streng auf die Erprobung des CAPPS-II-Systems und seiner Schnittstellen; er soll außer in Notfällen, in denen ein bekannter Terrorist oder eine Person mit nachgewiesenen Verbindungen zum terroristischen Umfeld identifiziert wurde, keine praktischen Auswirkungen haben. Gemäß der Bestimmung in Absatz 10 über ein automatisches Filterverfahren wird das CBP „sensible" Daten herausfiltern und löschen, bevor es PNR-Daten gemäß dieses Absatzes en bloc an die TSA weitergibt.

Behandlung „sensibler" Daten

9. Das CBP wird keine „sensiblen" Daten (d. h. personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, die politische Meinung, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftsmitgliedschaft hervorgeht, sowie Daten über Gesundheit oder Sexualleben) aus den PNR wie unten beschrieben verwenden.

10. Das CBP wird so rasch wie möglich ein automatisiertes System einführen, das bestimmte „sensible" PNR-Codes und -Bezeichnungen, die das CBP in Absprache mit der Europäischen Kommission festlegt, herausfiltert und löscht.

11. Bis solche automatischen Filter eingesetzt werden können, verpflichtet sich das CBP, keine „sensiblen" PNR-Daten zu verwenden und aus PNR-Daten, die gemäß den Absätzen 28 bis 34 weitergegeben werden dürfen, „sensible" Datenelemente zu löschen [3].

Verfahren für den Zugriff auf PNR-Daten

12. Wenn das CBP PNR-Daten direkt aus dem Reservierungssystem der Fluggesellschaft abruft (oder sie ihm direkt von dort übermittelt werden), um Personen zu ermitteln, die potenziell einer Grenzkontrolle unterzogen werden sollen, werden die Mitarbeiter des CBP nur auf PNR-Daten zugreifen (oder solche entgegennehmen) und benutzen, die Personen betreffen, deren Reiseweg einen Flug in die oder aus den [4] Vereinigten Staaten beinhaltet.

13. Das CBP wird die Passagierdaten aus den Reservierungssystemen der Fluggesellschaften abrufen („pull"), bis die Fluggesellschaften in der Lage sind, ein System für die aktive Übermittlung der Daten („push") an das CBP in Betrieb zu nehmen.

14. Das CBP wird PNR-Daten zu einem bestimmten Flug frühestens 72 Stunden vor Abflug abrufen und das System zwischen dem ersten Abruf, dem Abflug von einem Ort außerhalb und der Ankunft in den Vereinigten Staaten bzw. dem ersten Abruf und dem Abflug aus den Vereinigten Staaten höchstens drei (3) Mal auf etwaige Änderungen der Informationen hin überprüfen. Falls es für die Fluggesellschaften möglich wird, PNR-Daten aktiv zu übermitteln („push"), muss das CBP diese Daten 72 Stunden vor Abflug erhalten; alle Änderungen der PNR-Daten zwischen diesem Zeitpunkt und der Ankunft des Fluges in den Vereinigten Staaten oder seinem Abflug von dort müssen ebenfalls an das CBP übermittelt werden [5]. Falls ausnahmsweise das CBP Vorabinformationen darüber erhält, dass verdächtige Personen mit dem Flugzeug in die USA einreisen, aus den USA ausreisen oder durch die USA reisen könnten, dann kann das CBP früher als 72 Stunden vor dem Abflug PNR-Daten abrufen (oder eine gesonderte Übermittlung verlangen), damit geeignete Strafverfolgungsmaßnahmen sichergestellt werden können, die zwecks Verhütung oder Bekämpfung eines terroristischen Angriffs oder einer schweren Straftat der in Absatz 3 genannten Art unabdingbar sind. Soweit dies praktikabel ist, wird das CBP in den Fällen, in denen früher als 72 Stunden vor Abflug auf PNR-Daten zugegriffen werden muss, die bei der Strafverfolgung üblichen Kanäle benutzen.

---

[2] Für die Zwecke dieser Bestimmung gilt das CBP nicht als direkt an der Erprobung von CAPPS II beteiligte Partei oder als „Dritter".

[3] Bevor das CBP automatische Filter (gemäß Absatz 10) einführt, wird es, wenn PNR, die es gemäß Absatz 35 weitergibt, „sensible" Daten enthalten, sich nach Kräften bemühen, die Offenlegung „sensibler" PNR-Daten unter Beachtung der US-Rechtsvorschriften zu begrenzen.

[4] Dies schließt Transitpassagiere ein, die durch die USA reisen.

[5] Wenn sich Fluggesellschaften bereit erklären, die PNR-Daten aktiv an das CBP zu übermitteln, wird es mit den Fluggesellschaften die Möglichkeit einer regelmäßigen aktiven Übermittlung von PNR-Daten erörtern, dies betrifft den Zeitraum zwischen der erstmaligen Übermittlung 72 Stunden vor dem Abflug von einem Ort außerhalb der Vereinigten Staaten und der Ankunft in den Vereinigten Staaten bzw. vor dem Abflug aus den Vereinigten Staaten. Das CBP versucht ein Verfahren für die aktive Übermittlung der benötigten PNR-Daten einzusetzen, das dem Bedarf der Behörde nach einer wirksamen Risikobewertung gerecht wird und dabei die wirtschaftliche Belastung der Fluggesellschaften so gering wie möglich hält.

Speicherung von PNR-Daten

15. Vorbehaltlich der Zustimmung der National Archives and Records Administration (44 U.S.C. 2101, et seq.) wird das CBP den Online-Zugriff auf PNR-Daten für zugriffsberechtigte CBP-Nutzer ([6]) auf sieben (7) Tage begrenzen; danach wird die Zahl der Bediensteten, die auf die PNR-Daten zugreifen dürfen, noch weiter verringert, und zwar für einen Zeitraum von drei Jahren und sechs Monaten (3,5 Jahre), gerechnet ab dem Zeitpunkt, zu dem auf die Daten im Buchungssystem der Fluggesellschaft zugegriffen wurde (oder sie von dort übermittelt wurden). Nach 3,5 Jahren werden die PNR-Daten, auf die in diesem Zeitraum nicht manuell zugegriffen wurde, vernichtet. PNR-Daten, auf die während der ursprünglichen 3,5-Jahres-Frist manuell zugegriffen wurde, werden vom CBP in eine Datei für gelöschte Datensätze überführt ([7]), wo sie während acht (8) Jahren verbleiben, bevor sie vernichtet werden. Diese Fristen würden indessen nicht für PNR-Daten gelten, die mit einem speziellen Ermittlungsverfahren verknüpft sind (der Zugriff auf solche Daten wäre bis zum Schließen der Akte möglich). Bei PNR, auf die das CBP während der Geltungsdauer dieser Verpflichtungserklärung in den Reservierungssystemen der Fluggesellschaften direkt zugreift (oder die sie direkt von dort übermittelt bekommt), gelten für das CBP die in diesem Absatz festgelegten Speicherfristen, ungeachtet des möglichen Auslaufens dieser Verpflichtungserklärung gemäß Absatz 46.

Sicherheit der Computersysteme des CBP

16. Zugriffsberechtigte Mitarbeiter des CBP erhalten über das geschlossene CBP-Intranet-System, das über eine End-to-End-Verschlüsselung verfügt, Zugang zu PNR; ferner wird die Verbindung vom Datenverarbeitungszentrum der Einwanderungsbehörde kontrolliert. PNR-Daten, die in der CBP-Datenbank gespeichert sind, sind lediglich im Nur-Lese-Modus zugänglich und nur für zugriffsberechtigte Personen, d. h., die Daten als solche können zwar neu formatiert werden, es können aber keinerlei sachliche Änderungen vom CBP daran vorgenommen werden, nachdem sie aus dem Reservierungssystem einer Fluggesellschaft abgerufen wurden.

17. Keine andere ausländische, zentralstaatliche, bundesstaatliche oder lokale Behörde hat direkten elektronischen Zugriff auf PNR-Daten über die CBP-Datenbanken (auch nicht über das Interagency Border Inspection System — IBIS).

18. Einzelheiten über Datenzugriffe in den CBP-Datenbanken (z. B. wer, wo, wann (Tag und Uhrzeit) und etwaige Datenänderungen) werden automatisch erfasst und routinemäßig vom Office of Internal Affairs geprüft, um eine unberechtigte Nutzung des Systems zu verhindern.

19. Nur bestimmte Bedienstete und Angestellte des CBP oder Mitarbeiter von IT-Vertragsunternehmen ([8]) (unter Aufsicht des CBP), die eingehend überprüft wurden, die über ein aktives, passwortgeschütztes Konto im CBP-Computersystem verfügen und die ein nachweisliches dienstliches Interesse an der Einsichtnahme in PNR-Daten haben, dürfen auf PNR-Daten zugreifen.

20. CBP-Bedienstete, CBP-Angestellte und Mitarbeiter von CBP-Vertragsunternehmen müssen in zweijährigem Abstand eine vollständige Sicherheits- und Datenschutzschulung einschließlich einer Prüfung absolvieren. Mit Hilfe der CBP-Systemkontrolle wird überwacht und sichergestellt, dass alle Datenschutz- und Datensicherheitsanforderungen erfüllt werden.

21. Der unbefugte Zugriff von CBP-Mitarbeitern auf die Reservierungssysteme von Fluggesellschaften oder das Computersystem des CBP, in dem PNR gespeichert sind, wird mit strengen Disziplinarmaßnahmen geahndet (bis hin zur Entlassung) und kann strafrechtlich sanktioniert werden (Geldstrafe, Freiheitsstrafe bis zu einem Jahr oder beides) (siehe title 18, United States Code, section 1030).

22. Die CBP-Grundsätze und -Vorschriften sehen außerdem strenge Disziplinarmaßnahmen (bis hin zur Entlassung) gegen jeden CBP-Mitarbeiter vor, der Informationen aus dem CBP-Computersystem ohne offizielle Genehmigung weitergibt (title 19, Code of Federal Regulations, section 103.34).

23. Gegen Bedienstete und Angestellte der Vereinigten Staaten, die PNR-Daten weitergeben, die sie im Rahmen ihrer Beschäftigung erlangt haben, können strafrechtliche Sanktionen (Geldstrafe, Freiheitsstrafe bis zu einem Jahr oder beides) verhängt werden, es sei denn, diese Weitergabe wäre von Rechts wegen zulässig (siehe title 18, United States Code, sections 641, 1030, 1905).

([6]) Bei diesen zugriffsberechtigten Nutzern des CBP würde es sich unter anderem um Mitarbeiter handeln, die den mit Auswertungsaufgaben betrauten Abteilungen in den Außenstellen angehören, sowie um Mitarbeiter des National Targeting Center. Wie bereits erläutert hätten auch Personen, die mit der Wartung, Entwicklung oder Kontrolle der CBP-Datenbank betraut sind, für diese begrenzten Zwecke Zugang zu den Daten.

([7]) Die PNR-Daten werden bei der Überführung in die Datei für gelöschte Datensätze zwar technisch nicht gelöscht, aber als Rohdaten gespeichert (also in einer nicht unmittelbar recherchierbaren Form und damit unbrauchbar für „traditionelle" Ermittlungen der Strafverfolgungsbehörden). Darüber hinaus sind sie — falls unbedingt erforderlich („need to know") — nur zugänglich für zugangsberechtigte Mitarbeiter des Office of Internal Affairs des CBP (und in einigen Fällen, in Zusammenhang mit Kontrollen, für das Office of the Inspector General) sowie für das für die Wartung der Datenbanken zuständige Personal des Office of Information Technology des CBS.

([8]) Jeglicher Zugang von „Vertragsunternehmen" zu PNR-Daten in den Computersystemen des CBP wäre auf Personen beschränkt, die einen Vertrag mit dem CBP über Wartungs- oder Entwicklungsarbeiten an seinem Computersystem geschlossen haben.

Behandlung und Schutz von PNR-Daten durch das CBP

24. Das CBP behandelt PNR-Informationen unabhängig von der Staatsangehörigkeit oder dem Wohnsitzland der betroffenen Person stets als strafverfolgungsrelevante, vertrauliche personenbezogene Informationen des Betroffenen und als vertrauliche Geschäftsinformationen der Luftfahrtgesellschaft und würde solche Daten, außer in den in dieser Verpflichtungserklärung dargestellten Fällen oder aufgrund gesetzlicher Verpflichtungen, nicht offen legen.

25. Die Offenlegung von PNR-Daten gegenüber der Allgemeinheit fällt generell unter den Freedom of Information Act (FOIA) (title 5, United States Code, section 552), der jedermann (unabhängig von Staatsangehörigkeit und Wohnsitz) Zugang zu Unterlagen der US-Bundesbehörden ermöglicht, sofern diese Unterlagen (oder Teile davon) nicht durch eine Ausnahmeregelung des FOIA von der Offenlegung ausgenommen sind. Diese Ausnahmeregelungen des FOIA erlauben einer Behörde, Unterlagen (oder Teile davon) zurückzuhalten, wenn es sich um vertrauliche Geschäftsinformationen handelt, wenn die Offenlegung der Informationen eindeutig eine ungerechtfertigte Verletzung der Privatsphäre des Betroffenen darstellen würde oder wenn die Informationen für Strafverfolgungszwecke erhoben wurden und die Offenlegung nach allgemeinem Ermessen eine ungerechtfertigte Verletzung der Privatsphäre darstellen könnte (title 5, United States Code, sections 552(b)(4), (6), (7)(C)).

26. Die Vorschriften des CBP (title 19, Code of Federal Regulations, section 103.12) für die Bearbeitung von Anträgen auf Datenzugang (zum Beispiel zu PNR-Daten) gemäß FOIA bestimmen ausdrücklich, dass (abgesehen von einigen wenigen Ausnahmen bei Anträgen der betroffenen Personen) die Offenlegungsanforderungen des FOIA nicht anwendbar sind auf CBP-Unterlagen mit 1. vertraulichen Geschäftsinformationen, 2. Informationen, die die Privatsphäre betreffen, wenn die Offenlegung eindeutig eine ungerechtfertigte Verletzung der Privatsphäre darstellen würde, 3. Informationen, die für Strafverfolgungszwecke erhoben wurden und deren Offenlegung nach allgemeinem Ermessen eine ungerechtfertigte Verletzung der Privatsphäre darstellen könnte [9].

27. Bei allen Rechts- oder Verwaltungsverfahren im Zusammenhang mit einem Antrag gemäß FOIA auf Zugang zu PNR-Daten, die von Fluggesellschaften stammen, wird sich das CBP darauf berufen, dass diese Informationen von der Offenlegung gemäß FOIA ausgenommen sind.

Übermittlung von PNR-Daten an andere Behörden

28. Abteilungen des Department of Homeland Security (DHS) werden wie „Drittbehörden" behandelt, die denselben Vorschriften und Bedingungen für die Weitergabe von PNR-Daten unterliegen wie andere Regierungsbehörden außerhalb des DHS; ausgenommen hiervon sind Übermittlungen zwischen dem CBP und der TSA gemäß Absatz 8.

29. Das CBP liefert im Rahmen seines Ermessens nur von Fall zu Fall PNR-Daten an andere Regierungsbehörden, auch solche in Drittländern, die Terrorismusbekämpfungs- oder Strafverfolgungsaufgaben wahrnehmen, und nur zum Zwecke der Verhütung oder Bekämpfung der unter Absatz 3 aufgeführten Straftaten. (Behörden, an die das CBP derartige Daten weitergibt, werden im Folgenden als „designierte Behörden" bezeichnet.)

30. Das CBP wird von seines Ermessens in Bezug auf die Übermittlung von PNR-Daten zu den erklärten Zwecken umsichtig Gebrauch machen. Das CBP wird zunächst prüfen, ob die Offenlegung der PNR-Daten gegenüber einer anderen designierten Behörde dem erklärten Zweck dient (siehe Absatz 29). Wenn dies der Fall ist, wird das CBP prüfen, ob diese designierte Behörde für die Verhütung, Aufklärung oder Verfolgung von Verstößen gegen einschlägige Gesetze oder sonstige Vorschriften oder für die Um- oder Durchsetzung dieser Gesetze oder Vorschriften zuständig ist, sofern das CBP über Anhaltspunkte für eine tatsächliche oder potenzielle Rechtsverletzung verfügt. Die sachliche Begründetheit der Offenlegung muss im Lichte aller dargelegten Umstände gewürdigt werden.

31. Bei der etwaigen Weitergabe von PNR-Daten an andere designierte Behörden gilt das CBP als „Eigentümer" der Daten. Den designierten Stellen obliegen aufgrund der ausdrücklichen Offenlegungsbestimmungen folgende Pflichten: 1. Sie dürfen PNR-Daten nur zu den in Absatz 29 bzw. 34 genannten Zwecken verwenden. 2. Sie müssen sicherstellen, dass die bereitgestellten PNR-Informationen ordnungsgemäß und im Einklang mit den Datenspeicherverfahren der designierten Stelle vernichtet werden. 3. Sie müssen für die Weiterverbreitung die ausdrückliche Genehmigung des CBP einholen. Die Nichtbeachtung der Übermittlungsbedingungen kann Ermittlungen nach sich ziehen, ferner eine Meldung des DHS Chief Privacy Officer; außerdem kann die designierte Stelle vom weiteren Empfang von PNR-Daten des CBP ausgeschlossen werden.

[9] Das CBP würde sich unabhängig von der Staatsangehörigkeit oder dem Wohnsitzland der betroffenen Person unterschiedslos auf diese Ausnahmen berufen.

32. Jede Offenlegung von PNR-Daten durch das CBP wird davon abhängig gemacht, dass die Empfängerbehörde diese Daten als vertrauliche Geschäftsinformationen und als strafverfolgungsrelevante, vertrauliche personenbezogene Daten des Betroffenen gemäß den Absätzen 25 und 26 behandelt, die als von der Offenlegung nach dem Freedom of Information Act (5 U.S.C. 552) ausgenommen behandelt werden sollten. Darüber hinaus wird der Empfängerbehörde mitgeteilt, dass eine Weiterverbreitung derartiger Informationen ohne ausdrückliche vorherige Genehmigung durch das CBP nicht zulässig ist. Das CBP wird eine Weiterübermittlung von PNR-Daten zu Zwecken, die nicht in den Absätzen 29, 34 und 35 aufgeführt sind, nicht genehmigen.

33. Mitarbeiter designierter Behörden, die ohne entsprechende Befugnis PNR-Daten offen legen, können sich strafbar machen (title 18, United States Code, sections 641, 1030, 1905).

34. Keine der hier aufgeführten Bestimmungen darf der Nutzung oder der Weitergabe von PNR-Daten an zuständige Behörden im Wege stehen, wenn die Offenlegung zum Schutz lebenswichtiger Interessen des Betroffenen oder anderer Personen, insbesondere im Falle erheblicher Gesundheitsrisiken, erforderlich ist. In diesen Fällen unterliegt die Offenlegung den in den Absätzen 31 und 32 dargelegten Übermittlungsvoraussetzungen.

35. Keine der hier aufgeführten Bestimmungen darf der Nutzung oder Offenlegung von PNR-Daten im Zusammenhang mit Strafprozessen oder anderen gesetzlichen Erfordernissen im Wege stehen. Das CBP wird die Europäische Kommission über die Verabschiedung aller US-Rechtsvorschriften informieren, die sich substanziell auf die in dieser Verpflichtungserklärung gemachten Zusagen auswirken.

Informations-, Auskunfts- und Widerspruchsrecht der betroffenen Passagiere

36. Das CBP wird Reisende über die Erhebung von PNR-Daten informieren sowie über die Fragen im Zusammenhang mit deren Nutzung (allgemeine Informationen über die Rechtsgrundlage für die Datenerhebung, über den Zweck der Erhebung, den Schutz der Daten, die Weitergabe der Daten, die Identität des zuständigen Bediensteten, die verfügbaren Rechtsbehelfe, Kontaktadressen bei etwaigen Fragen oder Anliegen usw.; diese Informationen sollen über die Web-Site des CB, über Reisebroschüren usw. vermittelt werden).

37. Anträge der Betroffenen (die auch als „unmittelbar betroffene Antragsteller“) bezeichnet werden) auf Überlassung einer Kopie der PNR-Daten, die über sie in den Datenbanken des CBP gespeichert sind, werden gemäß dem Freedom of Information Act (FOIA) behandelt. Anträge dieser Art können entweder per Post an „Freedom of Information Act (FOIA) Request, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229“ gerichtet oder dem „Disclosure Law Officer, U.S. Customs and Border Protection, Headquarters, Washington, D.C.“ ausgehändigt werden. Weitere Informationen über die Verfahren zur Beantragung des Datenzugangs nach dem FOIA enthält der Code of Federal Regulations, Title 19, Section 103.5. Wenn ein unmittelbar Betroffener einen Antrag stellt, wird die Tatsache, dass das CBP die Daten eigentlich als vertrauliche personenbezogene Daten des Betroffenen und als vertrauliche Geschäftsinformationen der Fluggesellschaften ansieht, dem CBP nicht als Vorwand dienen, dem Betroffenen die PNR-Daten unter Berufung auf FOIA vorzuenthalten.

38. In bestimmten Ausnahmefällen kann das CBP seine Befugnisse nach FOIA ausüben und gegenüber dem unmittelbar betroffenen Antragsteller die Offenlegung des ganzen PNR (oder, was wahrscheinlicher ist, eines Teils davon) verweigern bzw. aufschieben, indem es sich auf title 5, United States Code, section 552(b) beruft (falls z. B. die Offenlegung gemäß FOIA nach allgemeinem Ermessen etwaige Strafverfahren beeinträchtigen könnte oder falls damit Techniken und Verfahren der Strafverfolgung in einer Weise preisgegeben würden, die nach allgemeinem Ermessen die Gefahr einer Gesetzesumgehung heraufbeschwören würde). Gemäß FOIA hat jeder Antragsteller das Recht, die Entscheidung des CBP, den Informationszugang zu verweigern, bei der Verwaltung und vor Gericht anzufechten (siehe 5 U.S.C. 552(a)(4)(B); 19 CFR 103.7-103.9).

39. Das CBP verpflichtet sich, Daten auf Antrag von Passagieren, Besatzungsmitgliedern, Fluggesellschaften oder Datenschutzbehörden (wenn diese vom Betroffenen ausdrücklich damit beauftragt wurden) in den Mitgliedstaaten der EU zu berichtigen ([10]), wenn das CBP feststellt, dass derartige Daten in seiner Datenbank gespeichert sind und eine Berichtigung gerechtfertigt und korrekt belegt ist. Das CBP wird jede designierte Behörde, die derartige PNR-Daten erhalten hat, über jede substanzielle Berichtigung dieser PNR-Daten benachrichtigen.

([10]) Was das „Berichtigen“ anbelangt, möchte das CBP klarstellen, dass es nicht befugt sein wird, einzelne Daten in den PNR-Datensätzen der Fluggesellschaften, auf die es zugreift, zu bearbeiten. Es wird vielmehr ein getrennter Datensatz erzeugt, der mit dem PNR-Datensatz verknüpft ist und das für unrichtig befundene Datenelement sowie die entsprechende Berichtigung enthält. Das CBP wird eine Anmerkung in den sekundären Prüfsatz des betreffenden Passagiers einfügen, die besagt, dass bestimmte PNR-Daten unrichtig sind oder sein könnten.

40. Anträge auf Berichtigung von in CBP-Datenbanken gespeicherten PNR-Daten und Beschwerden der Betroffenen über die Behandlung ihrer PNR-Daten durch das CBP können entweder von den Betroffenen selbst oder von der jeweils zuständigen Datenschutzbehörde (sofern sie von dem Betroffenen ausdrücklich damit beauftragt wurde) eingereicht werden, und zwar beim „Assistant Commissioner, Office of Field Operations, U.S. Bureau of Customs and Border Protection, 1300 Penssylvania Avenue, N.W., Washington, D.C. 20229".

41. Falls das CBP einer Beschwerde nicht abhelfen kann, kann die Beschwerde schriftlich an den „Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528" gerichtet werden, der den Sachverhalt untersuchen und sich um Lösung bemühen wird [11].

42. Außerdem wird sich das DHS Privacy Office umgehend mit Beschwerden befassen, die die Datenschutzbehörden der EU-Mitgliedstaaten im Auftrag EU-ansässiger Betroffener an ihn richten, weil die Betroffenen zu der Auffassung gelangt sind, dass ihre Datenschutzbeschwerden bezüglich PNR-Daten nicht zufrieden stellend vom CBP (gemäß den Absätzen 37 bis 41) oder vom DHS Privacy Office behandelt wurden. Das Privacy Office wird seine Schlussfolgerungen mitteilen und die betreffende(n) Datenschutzbehörde(n) über etwaige Maßnahmen informieren. Der DHS Chief Privacy Officer wird in seinem Bericht an den Kongress auch auf die Zahl, den Gegenstand und die Lösung von Beschwerdefällen im Zusammenhang mit der Behandlung personenbezogener Daten vom Typ PNR eingehen [12].

Einhaltung der Verpflichtungen

43. CBP und DHS verpflichten sich, einmal pro Jahr oder häufiger, falls dies von den Parteien vereinbart wird, gemeinsam mit der Europäischen Kommission und erforderlichenfalls Vertretern europäischer Strafverfolgungsbehörden und/oder EU-mitgliedstaatlicher Behörden [13] die Umsetzung dieser Verpflichtungserklärung zu überprüfen.

44. Das CBP wird Vorschriften, Richtlinien und sonstige Anweisungen veröffentlichen, die die hier eingegangenen Verpflichtungen enthalten, um sicherzustellen, dass die Bediensteten, Angestellten und Vertragsunternehmen des CBP sich an diese Verpflichtungserklärungen halten. Wie bereits ausgeführt, werden Verstöße der Bediensteten, Angestellten oder Vertragsunternehmen des CBP gegen die besagten Anweisungen der CBP mit strengen Disziplinarmaßnahmen und gegebenenfalls strafrechtlich geahndet.

Gegenseitigkeit

45. Sollte in der Europäischen Union ein Passagier-Identifikationssystem eingeführt werden, das Fluggesellschaften verpflichtet, Behörden den Zugang zu PNR-Daten von Personen zu gestatten, deren Reiseweg einen Flug in die oder aus der EU einschließt, wird das CBP unter strenger Beachtung des Gegenseitigkeitsgrundsatzes die US-Fluggesellschaften zur Zusammenarbeit anhalten.

Überprüfung und Geltungsdauer der Verpflichtungserklärung

46. Diese Verpflichtungserklärung gilt drei Jahre und sechs Monate (3,5 Jahre), gerechnet ab dem Tag, an dem eine Vereinbarung zwischen den Vereinigten Staaten und der Europäischen Gemeinschaft in Kraft tritt, die die Verarbeitung von PNR-Daten durch Fluggesellschaften zum Zweck ihrer Weiterleitung an das CBP im Einklang mit der Richtlinie erlaubt. Zwei Jahre und sechs Monate (2,5 Jahre) nach Wirksamwerden dieser Verpflichtungserklärung nimmt das CBP, in Absprache mit dem DHS, Gespräche mit der Kommission auf mit dem Ziel, diese Verpflichtungserklärung und alle daran anknüpfenden Vereinbarungen zu beiderseits annehmbaren Bedingungen zu verlängern. Kann vor Ablauf der Geltungsdauer dieser Verpflichtungserklärung keine solche Einigung erzielt werden, verliert die Verpflichtungserklärung ihre Wirkung.

---

[11] Der DHS Chief Privacy Officer ist unabhängig von allen Abteilungen des Department of Homeland Security. Er hat laut Gesetz sicherzustellen, dass personenbezogene Informationen im Einklang mit einschlägigen Gesetzen (siehe Fußnote 13) verwendet werden. Die Entscheidungen des Chief Privacy Officer sind für das DHS verbindlich und können nicht aus politischen Erwägungen übergangen werden.

[12] Gemäß Section 222 des Homeland Security Act aus dem Jahr 2002 (nachstehend „Gesetz" genannt) (Public Law 107-296 vom 25. November 2002) ist der DHS Privacy Officer mit einer „Datenschutz-Folgenabschätzung" beauftragt; zu diesem Zweck hat er die Auswirkungen geplanter Vorschriften des Ministeriums auf den Datenschutz zu untersuchen, einschließlich Art der erhobenen personenbezogenen Daten und Zahl der betroffenen Personen, und dem Kongress jährlich Bericht über die datenschutzrelevanten Tätigkeiten des Ministeriums zu erstatten. Section 222(5) des Gesetzes weist dem DHS Privacy Officer außerdem ausdrücklich die Aufgabe zu, sich mit allen Fällen zu befassen, die die Verletzung der Privatsphäre betreffen, und dem Kongress darüber zu berichten.

[13] Beide Seiten informieren sich gegenseitig vorab über die Zusammensetzung ihrer Delegationen. Sie können auch andere Behörden einbeziehen, die für Datenschutz, Zollkontrollen und anderen Formen der Strafverfolgung, Grenzsicherung und/oder Flugsicherheit zuständig sind. Die Beteiligten müssen die gegebenenfalls erforderlichen Sicherheitsüberprüfungen bestanden haben und sind hinsichtlich der Erörterungen und der ihnen ggf. zugänglich gemachten Unterlagen zur Geheimhaltung verpflichtet. Die Geheimhaltungspflicht verbietet beiden Seiten jedoch nicht, ihren zuständigen Behörden, darunter dem US-Kongress und dem Europäischen Parlament, über die Ergebnisse der gemeinsamen Überprüfung zu berichten. Auf keinen Fall dürfen die teilnehmenden Behörden jedoch personenbezogene Daten von Betroffenen offen legen. Dieses Verbot gilt auch für nichtöffentliche Informationen, die sich aus den ihnen zugänglich gemachten Unterlagen ergeben, sowie für operative oder interne Behördeninformationen, von denen sie bei der gemeinsamen Überprüfung Kenntnis erlangen. Die Modalitäten der gemeinsamen Überprüfung werden von beiden Seiten einvernehmlich festgelegt.

Begründung von Rechten oder Präzedenzfällen

47. Durch diese Verpflichtungserklärung werden keinerlei Rechte oder Vergünstigungen für private oder öffentliche Personen oder Beteiligte begründet oder übertragen.

48. Die Bestimmungen dieser Verpflichtungserklärung stellen keinen Präzedenzfall dar für künftige Diskussionen mit der Europäischen Kommission, der Europäischen Union, mit diesen verbundenen Einrichtungen oder mit Drittstatten über die Übermittlung jedweder Art von Daten.

11. Mai 2004

ANHANG „A“

PNR-Daten, die das CBP von Fluggesellschaften verlangt

1. PNR-Buchungscode (Record Locator)
2. Datum der Reservierung
3. Geplante Abflugdaten
4. Name
5. Andere Namen im PNR
6. Anschrift
7. Zahlungsart
8. Rechnungsanschrift
9. Telefonnummern
10. Gesamter Reiseverlauf für den jeweiligen PNR
11. Vielflieger-Eintrag (beschränkt auf abgeflogene Meilen und Anschrift(en))
12. Reisebüro
13. Bearbeiter
14. Codeshare-Information im PNR
15. Reisestatus des Passagiers
16. Informationen über die Splittung/Teilung einer Buchung
17. E-Mail-Adresse
18. Informationen über Flugscheinausstellung (Ticketing)
19. Allgemeine Bemerkungen
20 Flugscheinnummer
21. Sitzplatznummer
22. Datum der Flugscheinausstellung
23. Historie über nicht angetretene Flüge (no show)
24. Nummern der Gepäckanhänger
25. Fluggäste mit Flugschein aber ohne Reservierung (Go show)
26. Spezielle Service-Anforderungen (OSI — Special Service Requests)
27. Spezielle Service-Anforderungen (SSI/SSR — Special Service Requests)
28. Information über den Auftraggeber (received from)
29. Alle Änderungen der PNR (PNR-History)
30. Zahl der Reisenden im PNR
31. Sitzplatzstatus
32. Flugschein für einfache Strecken (one-way)
33. Etwaige APIS-Informationen
34. ATFQ-Felder (automatische Tarifabfrage)