



**RAT DER
EUROPÄISCHEN UNION**

**Brüssel, den 8. Dezember 2011
(OR. en)**

17434/11

**Interinstitutionelles Dossier:
2011/0382 (NLE)**

**JAI 862
USA 85
RELEX 1234
DATAPROTECT 139**

GESETZGEBUNGSAKTE UND ANDERE RECHTSINSTRUMENTE

Betr.: Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security

ABKOMMEN
ZWISCHEN DEN VEREINIGTEN STAATEN VON AMERIKA
UND DER EUROPÄISCHEN UNION
ÜBER DIE VERWENDUNG VON FLUGGASTDATENSÄTZEN
UND DEREN ÜBERMITTLUNG
AN DAS UNITED STATES DEPARTMENT OF HOMELAND SECURITY

DIE VEREINIGTEN STAATEN VON AMERIKA,

im Folgenden auch "Vereinigte Staaten", und

DIE EUROPÄISCHE UNION

im Folgenden auch "EU",

im folgenden zusammen "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 transatlantischen Partnerschaft auszubauen und weiter voranzubringen;

IN ANERKENNUNG des Rechts der Staaten, die Sicherheit ihrer Bürger zu gewährleisten und ihre Grenzen zu schützen, in Anerkennung ihrer Verantwortung hierfür und eingedenk der Verantwortung aller Nationen für den Schutz von Menschenleben und der öffentlichen Sicherheit, auch im internationalen Verkehr;

IN DER ÜBERZEUGUNG, dass der Austausch von Informationen einen wesentlichen Beitrag zur Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität leistet und dass die Verarbeitung und Verwendung von Fluggastdatensätzen (PNR-Daten) in diesem Zusammenhang notwendig ist und Informationen liefert, die auf andere Weise nicht erlangt werden können;

IN DEM FESTEN WILLEN, terroristische Straftaten und grenzübergreifende Kriminalität unter Achtung der Grundrechte und Grundfreiheiten zu verhüten und zu bekämpfen und eingedenk der Bedeutung des Schutzes der Privatsphäre und personenbezogener Daten und Informationen;

UNTER BERÜCKSICHTIGUNG internationaler Regelungen sowie der Gesetze und Vorschriften der Vereinigten Staaten, wonach von jeder Fluggesellschaft, die Auslands-Passagierflüge in die oder aus den Vereinigten Staaten durchführt, verlangt wird, dem Department of Homeland Security (DHS) PNR-Daten zur Verfügung zu stellen, soweit solche Daten erhoben und in den computer-gestützten Buchungs- bzw. Abfertigungssystemen der Fluggesellschaften gespeichert werden, sowie unter Berücksichtigung vergleichbarer Verpflichtungen, die derzeit oder künftig in der EU angewandt werden;

IN ANBETRACHT DESSEN, dass das DHS PNR-Daten zum Zwecke der Verhütung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung terroristischer Straftaten und grenzübergreifender Kriminalität unter Beachtung der Garantien für den Schutz der Privatsphäre und der personenbezogenen Daten und Informationen gemäß diesem Abkommen verarbeitet und verwendet;

IN ANBETRACHT der Bedeutung, die der Übermittlung von PNR-Daten und einschlägigen analytischen Informationen, die die Vereinigten Staaten von Amerika aus PNR-Daten gewinnen, an die Polizei- und Justizbehörden der Mitgliedstaaten der Europäischen Union, im Folgenden EU-Mitgliedstaaten, sowie an Europol oder Eurojust als Mittel zur Stärkung der internationalen polizeilichen und justiziellen Zusammenarbeit zukommt;

IN BESONDERER ANERKENNUNG der aus ihren Rechtsvorschriften und Gründungsdokumenten ersichtlichen langen Tradition, die beide Parteien hinsichtlich der Achtung des Privatlebens vorweisen können;

EINGEDENK des Artikels 6 des Vertrags über die Europäische Union, in dem sich die EU zur Achtung der Grundrechte verpflichtet, des Artikels 16 des Vertrags über die Arbeitsweise der Europäischen Union über das Recht auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, der Grundsätze der Verhältnismäßigkeit und der Notwendigkeit hinsichtlich des Rechts auf Achtung des Privat- und Familienlebens, der Achtung der Privatsphäre und des Schutzes personenbezogener Daten gemäß Artikel 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten, dem Übereinkommen Nr. 108 des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dessen Zusatzprotokoll Nr. 181 und der Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union;

EINGEDENK der robusten Verfahren zum Schutz der Privatsphäre und Gewährleistung der Datenintegrität, die das DHS derzeit anwendet, unter anderem in den Bereichen Objektschutz, Zugangskontrolle, Datentrennung und -verschlüsselung, Auditkapazitäten und effektive Rechenschaftspflicht;

EINGEDENK der Bedeutung der Datenqualität, -genauigkeit, -integrität und -sicherheit und einer angemessenen Rechenschaftspflicht, die die Einhaltung der Grundsätze garantiert;

ANGESICHTS des Grundsatzes der Transparenz und der Vorkehrungen, die die Vereinigten Staaten treffen, um die betroffenen Fluggäste über die Notwendigkeit der Erfassung von PNR-Daten und deren Verwendung zu den Zwecken, für die sie erfasst werden, zu informieren;

IN ANERKENNUNG dessen, dass das DHS PNR-Daten erfassen und auswerten muss, um seinen Grenzschutzauftrag erfüllen zu können, und dass Vorkehrungen getroffen werden, um sicherzustellen, dass die Erfassung und Verwendung von PNR für die Zwecke, für die sie erfasst werden, weiterhin relevant und erforderlich sind;

IN ANERKENNUNG dessen, dass davon ausgegangen werden kann, dass das DHS im Hinblick auf dieses Abkommen und seine Anwendung die an das DHS übermittelten PNR-Daten bei der Verarbeitung und der Verwendung angemessen schützt;

EINGEDENK dessen, dass die Vereinigten Staaten und die Europäische Union in ihren Bemühungen um die Bekämpfung von Verbrechen und Terrorismus für einen hohen Schutz von personenbezogenen Informationen eintreten und entschlossen sind, unverzüglich eine den beiderseitigen Zielen förderliche Vereinbarung über den umfassenden Schutz der personenbezogenen Daten zu treffen, die im Rahmen der Verbrechen- und Terrorismusbekämpfung ausgetauscht werden;

IN ANERKENNUNG der erfolgreichen Gemeinsamen Überprüfungen der Abkommen zwischen den Parteien von 2004 und 2007 über die Übermittlung von PNR-Daten in den Jahren 2005 beziehungsweise 2010;

IN ANERKENNUNG des Interesses der Parteien und der EU-Mitgliedstaaten an einem Austausch von Informationen über die Methode der Übermittlung von PNR-Daten sowie über die Weiterleitung solcher Daten gemäß den einschlägigen Artikeln dieses Abkommens sowie in Anerkennung des Interesses der EU an der Einbeziehung dieses Aspekts in das in diesem Abkommen vorgesehene Konsultations- und Überprüfungsverfahren;

UNTER BEKRÄFTIGUNG, dass dieses Abkommen keinen Präzedenzfall im Hinblick auf weitere Vereinbarungen zwischen den Parteien oder zwischen ihnen und einer anderen Partei über die Verarbeitung, Verwendung und Übermittlung von PNR-Daten oder anderer Daten oder über den Datenschutz darstellt;

IN ANERKENNUNG dessen, dass dieses Abkommen und seine Anwendung in der Europäischen Union und in den Vereinigten Staaten vom Grundsatz der Verhältnismäßigkeit und den damit verbundenen Relevanz- und Notwendigkeitsprinzipien getragen werden;

EINGEDENK der Tatsache, dass die Parteien die Übermittlung von PNR-Daten für den Seeverkehr weiter erörtern können –

KOMMEN WIE FOLGT ÜBEREIN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

ARTIKEL 1

Zweck

- (1) Zweck des Abkommens ist es, für Sicherheit zu sorgen, Menschenleben zu schützen und die öffentliche Sicherheit zu gewährleisten.
- (2) Zu diesem Zweck legt das Abkommen die Aufgaben der Parteien bei der Übermittlung, Verarbeitung und Verwendung von PNR-Daten und Bedingungen hierfür fest.

ARTIKEL 2

Anwendungsbereich

- (1) PNR-Daten im Sinne der Leitlinien der Internationalen Zivilluftfahrt-Organisation sind Daten, die von Fluggesellschaften oder deren bevollmächtigten Agenturen für jeden von einem oder für einen Fluggast gebuchten Flug erfasst werden und in den Buchungs- und Abfertigungssystemen der Fluggesellschaften oder in gleichwertigen Systemen, die ähnliche Funktionen bieten (in diesem Abkommen kollektiv „Buchungssysteme“ genannt), gespeichert sind. PNR-Daten im Sinne dieses Abkommens sind die im Anhang des Abkommens ("Anhang") beschriebenen Datenarten.

(2) Dieses Abkommen gilt für Fluggesellschaften, die Passagierflüge zwischen der Europäischen Union und den Vereinigten Staaten durchführen.

(3) Dieses Abkommen gilt auch für in der Europäischen Union eingetragene Fluggesellschaften und für Fluggesellschaften, die in der Europäischen Union Daten speichern, wenn sie Passagierflüge in die oder aus den Vereinigten Staaten durchführen.

ARTIKEL 3

Bereitstellung von PNR-Daten

Die Fluggesellschaften stellen dem DHS die in ihren Buchungssystemen enthaltenen PNR-Daten nach den DHS-Anforderungen und nach Maßgabe dieses Abkommens zur Verfügung. Sollten die von Fluggesellschaften übermittelten Fluggastdatensätze Daten enthalten, die nicht im Anhang aufgeführt sind, so löscht das DHS diese Daten bei Erhalt.

ARTIKEL 4

Verwendung von PNR-Daten

(1) Die Vereinigten Staaten erfassen, verwenden und verarbeiten PNR-Daten zum Zwecke der Verhütung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung folgender Straftaten:

a) terroristischer und damit verbundener Straftaten, darunter

- i) Handlungen, die –
 - 1. mit Gewaltanwendung verbunden sind oder Menschenleben, Vermögenswerte oder Infrastruktur gefährden und
 - 2. allem Anschein nach bezwecken,
 - a) die Zivilbevölkerung einzuschüchtern oder zu nötigen,
 - b) die Politik einer Regierung durch Einschüchterung oder Nötigung zu beeinflussen oder
 - c) die Handlungsfähigkeit einer Regierung durch massive Zerstörung von Sachen, Tötung, Entführung oder Geiselnahme zu beeinträchtigen.
- ii) Handlungen, die in geltenden internationalen Übereinkünften zur Terrorismusbekämpfung und in entsprechenden Protokollen eine Straftat darstellen und als solche definiert sind;
- iii) jegliche direkte oder indirekte Bereitstellung oder Beschaffung von Finanzmitteln in der Absicht oder in dem Wissen, dass diese Mittel ganz oder teilweise zur Verübung von Handlungen im Sinne der Ziffern i oder ii verwendet werden oder verwendet werden sollen;
- iv) der Versuch, eine in den Ziffern i, ii oder iii aufgeführte Handlung zu begehen;

- v) Teilnahme an einer Handlung im Sinne der Ziffern i, ii oder iii;
 - vi) Organisation einer in den Ziffern i, ii oder iii aufgeführten Handlung oder Anleitung anderer zur Verübung einer solchen;
 - vii) jeglicher sonstiger Beitrag zu einer Handlung im Sinne der Ziffern i, ii oder iii;
 - viii) Drohung mit einer Handlung nach Ziffer i, wenn die Umstände die Drohung glaubhaft erscheinen lassen;
- b) sonstiger Straftaten, die mit einer Freiheitsstrafe von drei oder mehr Jahren geahndet werden können und grenzübergreifender Art sind.

Eine Straftat gilt als grenzübergreifend, wenn sie

- i) in mehr als einem Land verübt wird,
- ii) in einem Land verübt wird, aber ein Großteil ihrer Vorbereitung, Planung, Lenkung oder Überwachung in einem anderen Staat stattfindet,

- iii) in einem Land im Rahmen einer organisierten kriminellen Vereinigung verübt wird, die kriminelle Handlungen in mehr als einem Land nachgeht,
- iv) in einem Land verübt wird, aber beträchtliche Auswirkungen in einem anderen Land hat oder
- v) in einem Land verübt wird und sich der Straftäter in einem anderen Land aufhält oder dorthin ausreisen will.

(2) PNR-Daten können erforderlichenfalls bei einer erheblichen Bedrohung oder zum Schutz lebenswichtiger Interessen von Einzelpersonen oder auf Anordnung eines Gerichts fallweise verwendet und verarbeitet werden.

(3) PNR-Daten können zur Ermittlung von Personen verwendet und verarbeitet werden, die bei Ankunft in den oder bei Abflug aus den Vereinigten Staaten einer ausführlicheren Befragung oder Kontrolle unterzogen werden oder eingehender kontrolliert werden müssen.

(4) Absätze 1, 2 und 3 gelten unbeschadet der innerstaatlichen Strafverfolgung, justizieller Befugnisse oder Verfahren, wenn bei der Verwendung und Verarbeitung von PNR-Daten andere Gesetzesübertretungen oder Indizien dafür entdeckt werden.

KAPITEL II

GARANTIE FÜR DIE VERWENDUNG VON PNR-DATEN

ARTIKEL 5

Datensicherheit

- (1) Das DHS stellt geeignete technische Maßnahmen und organisatorische Vorkehrungen sicher, um in den PNR-Datensätzen enthaltene personenbezogene Daten und Informationen vor Zerstörung, Verlust, Offenlegung, Änderung, Verarbeitung oder Verwendung zu schützen und den Zugriff darauf zu verhindern, wenn dies versehentlich, unrechtmäßig oder ohne Befugnis geschieht.
- (2) Das DHS verwendet geeignete Technologien zur Gewährleistung des Schutzes, der Sicherheit, Vertraulichkeit und Integrität der Daten. Es gewährleistet insbesondere, dass
- a) von den zuständigen Behörden anerkannte Verschlüsselungs-, Genehmigungs- und Dokumentierungsverfahren angewandt werden. Insbesondere ist der Zugriff auf PNR-Daten zu sichern und auf besonders befugte Bedienstete zu begrenzen;
 - b) PNR-Daten in einer gesicherten physischen Umgebung aufbewahrt und mit physischen Einbruchssicherungssysteme gesichert werden und
 - c) ein Mechanismus vorhanden ist, mit denen sichergestellt wird, dass Abfragen von PNR-Daten nach Maßgabe des Artikels 4 erfolgen.

- (3) Bei einer Verletzung des Datenschutzes (wie unbefugter Zugriff oder unerlaubte Offenlegung) ergreift das DHS angemessene Maßnahmen zur Benachrichtigung der betroffenen Personen und gegebenenfalls zur Minderung des Schadensrisikos infolge einer unerlaubten Offenlegung personenbezogener Daten und Informationen sowie technisch mögliche Abhilfemaßnahmen.
- (4) Im Anwendungsbereich dieses Abkommens informiert das DHS ohne unangemessene Verzögerung die zuständigen europäischen Behörden über ernste Verletzungen des Datenschutzes, in denen PNR-Daten von EU-Bürgern oder von Personen mit Wohnsitz in der EU versehentlich oder unrechtmäßig vernichtet wurden oder versehentlich verloren gegangen sind, geändert, unrechtmäßig offengelegt oder in anderer unrechtmäßiger Weise verarbeitet oder verwendet wurden oder in denen Unbefugte darauf zugegriffen haben.
- (5) Die Vereinigten Staaten bestätigen, dass sie in ihren Datenschutzvorschriften über wirksame verwaltungs-, zivil- und strafrechtliche Durchsetzungsmaßnahmen in Falle von Verletzungen des Datenschutzes verfügen. Das DHS kann Disziplinarmaßnahmen gegen Personen verhängen, die für solche Verletzungen des Datenschutzes verantwortlich sind, darunter den Zugang zum System sperren, förmliche Verweise erteilen, Personen vorübergehend oder endgültig vom Dienst suspendieren oder gegebenenfalls degradieren.
- (6) Jeglicher Zugriff auf PNR-Daten sowie die Verarbeitung und Verwendung der Daten werden vom DHS protokolliert und dokumentiert. Die Protokolle und Dokumentationen werden ausschließlich zu Aufsichts-, Prüfungs- und Systemwartungszwecken oder zu anderen gesetzlich vorgeschriebenen Zwecken verwendet.

ARTIKEL 6

Sensible Daten

- (1) Soweit die PNR-Daten eines Fluggastes sensible Daten enthalten (das heißt personenbezogene Daten und Informationen, die Aufschluss über die Rasse, ethnische Herkunft, politische Überzeugung, die Religion oder Weltanschauung, die Mitgliedschaft in einer Gewerkschaft oder die Gesundheit und das Sexualleben des Betroffenen geben), filtert das DHS mit Hilfe automatisierter Systeme die sensiblen Daten aus den PNR-Daten heraus und macht sie unkenntlich. Das DHS darf diese Daten nicht weiter verarbeiten oder verwenden, außer nach Maßgabe der Absätze 3 und 4.
- (2) Das DHS übermittelt der Europäischen Kommission binnen 90 Tagen nach Inkrafttreten dieses Abkommens eine Liste mit Codes und Begriffen zur Auffindung sensibler Daten, die herauszufiltern sind.
- (3) Der Zugriff auf sensible Daten sowie deren Verarbeitung und Verwendung ist in Ausnahmefällen zulässig, wenn eine Gefahr für Leib und Leben von Personen besteht. Auf solche Daten darf nur im Einzelfall unter Verwendung restriktiver Verfahren und nur mit Genehmigung eines leitenden DHS-Bediensteten zugegriffen werden.
- (4) Sensible Daten werden spätestens 30 Tage, nachdem das DHS die letzten PNR-Daten mit den sensiblen Daten erhalten hat, endgültig gelöscht. Sensible Daten dürfen jedoch zwecks Ermittlungen, Strafverfolgungs- oder Strafvollzugsmaßnahmen in einem konkreten Fall für die in den Vorschriften der Vereinigten Staaten vorgesehene Dauer aufbewahrt werden.

ARTIKEL 7

Automatisierte Einzelentscheidungen

Die Vereinigten Staaten treffen keine Entscheidungen, die sich allein auf die automatisierte Verarbeitung und Verwendung von PNR-Daten stützen und die die rechtlichen Interessen der betroffenen Personen erheblich verletzen.

ARTIKEL 8

Speicherung der Daten

(1) Das DHS speichert die PNR-Daten bis zu fünf Jahre lang in einer aktiven Datenbank. Nach den ersten sechs Monaten der Speicherung werden die PNR-Daten gemäß Absatz 2 des vorliegenden Artikels anonymisiert und unkenntlich gemacht. Der Zugang zu dieser aktiven Datenbank wird auf eine begrenzte Anzahl besonders hierzu befugte Bedienstete beschränkt, es sei denn, dieses Abkommen lässt einen anderen Zugang zu.

(2) Zur Anonymisierung von personenbezogenen Daten in den PNR-Datensätzen sind folgende Arten von Daten unkenntlich zu machen:

a) Name(n),

- b) andere Namen im PNR-Datensatz,
- c) sämtliche verfügbaren Kontaktinformationen, einschließlich Informationen zur Identifizierung des Dateneingebers;
- d) allgemeine Eintragungen, u. a. OSI- (Other Supplementary Information), SSI- (Special Service Information) und SSR-Informationen (Special Service Request) sowie
- e) etwaig erfasste APIS-Daten (APIS - Advance Passenger Information System).

(3) Nach der Speicherung in der aktiven Datenbank werden die PNR-Daten in eine ruhende Datenbank überführt, wo sie bis zu zehn Jahre verbleiben. Diese ruhende Datenbank unterliegt zusätzlichen Kontrollen; der Zugang ist auf eine noch begrenztere Anzahl befugter Bediensteter beschränkt und nur mit Genehmigung von noch höherer Ebene gestattet. Die Anonymisierung der PNR-Daten in dieser Datenbank wird nur zu Zwecken von Strafverfolgungsmaßnahmen und nur für einen konkreten Fall, eine konkrete Bedrohung oder ein konkretes Risiko rückgängig gemacht. Für die Zwecke des Artikels 4 Absatz 1 Buchstabe b ist eine Rückgängigmachung der Anonymisierung der in dieser ruhenden Datenbank gespeicherten PNR-Daten nur für einen Zeitraum von höchstens fünf Jahren zulässig.

(4) Nach der Speicherung in der ruhenden Datenbank werden die Daten gänzlich anonymisiert, indem alle Arten von Daten, mit denen der Fluggast, auf den sich die PNR-Daten beziehen, ermittelt werden könnte auf eine Weise gelöscht werden, dass eine Rückgängigmachung der Anonymisierung nicht mehr möglich ist.

(5) Daten zu einem konkreten Fall oder für bestimmte Ermittlungen können in der aktiven PNR-Datenbank gespeichert werden, bis der Fall oder die Ermittlungen archiviert sind. Dieser Absatz gilt unbeschadet der Vorgaben für die Speicherung der Daten zu einzelnen Ermittlungs- oder Strafverfolgungsakten.

(6) Die Notwendigkeit eines Zehnjahreszeitraums für die Speicherung in der ruhenden Datenbank wird im Rahmen der Evaluierung nach Artikel 23 Absatz 1 überprüft.

ARTIKEL 9

Diskriminierungsverbot

Die Vereinigten Staaten sorgen dafür, dass die in diesem Abkommen vorgesehenen Garantien für die Verarbeitung und Verwendung von PNR-Daten für alle Fluggäste gleichermaßen gelten und keinen Fluggast unrechtmäßig diskriminieren.

ARTIKEL 10

Transparenz

(1) Das DHS informiert die Fluggäste folgendermaßen über die Verwendung und Verarbeitung von PNR-Daten:

a) Veröffentlichung im Bundesregister (Federal Register);

- b) Veröffentlichung auf der DHS-Website;
- c) Vermerke, die die Fluggesellschaften in ihre Beförderungsverträge aufnehmen können;
- d) gesetzlich vorgeschriebene Berichterstattung an den Kongress und
- e) andere geeignete Maßnahmen.

(2) Das DHS veröffentlicht seine Verfahren und Modalitäten für den Zugang, die Berichtigung oder Bereinigung sowie für Rechtsbehelfe und gibt diese Informationen an die EU weiter, die diese veröffentlichen kann.

(3) Die Parteien arbeiten mit den Fluggesellschaften zusammen, um die Fluggäste bei der Buchung besser über die Zwecke der Erfassung, Verarbeitung und Verwendung von PNR-Daten durch das DHS und die Möglichkeiten zur Beantragung des Zugangs, der Berichtigung und über Rechtsbehelfsmöglichkeiten zu informieren.

ARTIKEL 11

Zugang von Einzelpersonen

(1) Gemäß dem Freedom of Information Act ist jede Person unabhängig von ihrer Staatsangehörigkeit, ihrem Herkunfts- oder Wohnsitzland berechtigt, beim DHS ihre PNR-Daten zu verlangen. Das DHS legt die PNR-Daten vorbehaltlich der Absätze 2 und 3 des vorliegenden Artikels innerhalb eines angemessenen Zeitraums vor.

(2) Die Offenlegung von in den PNR-Datensätzen enthaltenen Informationen kann angemessenen rechtlichen Beschränkungen nach dem Recht der Vereinigten Staaten unterworfen werden, beispielsweise Beschränkungen zum Schutz sensibler Informationen, darunter personenbezogener Informationen, die dem Datenschutz unterliegen, und für die nationale Sicherheit oder für Strafverfolgungszwecke relevanter Informationen.

(3) Eine Verweigerung oder Einschränkung des Zugangs ist dem Antragsteller innerhalb eines angemessenen Zeitraums schriftlich mitzuteilen. In der Mitteilung sind die Vorschriften zu nennen, die die Verweigerung oder Einschränkung des Zugangs begründen, und ist der Betroffene über Rechtsbehelfe aufzuklären, die ihm nach dem Recht der Vereinigten Staaten zur Verfügung stehen.

(4) Das DHS legt PNR-Daten nicht der Öffentlichkeit offen, außer dem Betroffenen, dessen PNR-Daten verarbeitet und verwendet wurden, oder seinem Rechtsvertreter oder anderen Personen, oder wenn dies nach den Rechtsvorschriften der Vereinigten Staaten erforderlich ist.

ARTIKEL 12

Recht von Einzelpersonen auf Berichtigung oder Bereinigung

(1) Jede Person ist unabhängig von ihrer Staatsangehörigkeit, ihrem Herkunfts- oder Wohnsitzland berechtigt, nach den in diesem Abkommen vorgegebenen Verfahren beim DHS die Berichtigung oder Bereinigung ihrer PNR-Daten, darunter auch die Löschung oder Sperrung von Daten, zu verlangen.

(2) Das DHS setzt den Antragsteller ohne unangemessene Verzögerung schriftlich von seiner Entscheidung über die Berichtigung oder Bereinigung der fraglichen PNR-Daten in Kenntnis.

(3) Eine Verweigerung der Berichtigung oder Bereinigung oder nur beschränkte Berichtigung oder Bereinigung ist dem Antragsteller innerhalb eines angemessenen Zeitraums schriftlich mitzuteilen. In der Mitteilung sind die Vorschriften zu nennen, die die Verweigerung oder beschränkte Berichtigung oder Bereinigung begründen, und ist der Betroffene über Rechtsbehelfe aufzuklären, die ihm nach dem Recht der Vereinigten Staaten zur Verfügung stehen.

ARTIKEL 13

Rechtsbehelf für Einzelpersonen

(1) Jeder Person, deren personenbezogene Daten und Informationen in einer Art und Weise verarbeitet und verwendet wurden, die nicht mit diesem Abkommen vereinbar ist, stehen unabhängig von ihrer Staatsangehörigkeit, ihrem Herkunfts- oder Wohnsitzland wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe nach dem Recht der Vereinigten Staaten zur Verfügung.

(2) Jede Person ist berechtigt, Verwaltungsbeschwerde gegen DHS-Entscheidungen über die Verwendung und Verarbeitung von PNR-Daten einzulegen.

(3) Nach dem Administrative Procedure Act und anderen einschlägigen Vorschriften ist jede Person berechtigt, bei einem Bundesgericht der Vereinigten Staaten Rechtsmittel gegen eine endgültige Entscheidung des DHS einzulegen. Darüber hinaus ist jede Person berechtigt, nach geltendem Recht und folgenden Gesetzen Rechtsmittel einzulegen:

a) Freedom of Information Act,

- b) Computer Fraud and Abuse Act,
- c) Electronic Communications Privacy Act und
- d) anderen einschlägigen Rechtsvorschriften der Vereinigten Staaten.

(4) Das DHS hat ein Verwaltungsverfahren (derzeit Traveler Redress Inquiry Program des DHS (DHS TRIP)) eingeführt, das jeder Person für Anfragen zu Reisen, darunter zur Verwendung von PNR-Daten, zur Verfügung steht. Das TRIP des DHS bietet einen Rechtsbehelf für Personen, die der Ansicht sind, dass ihnen der Einstieg in ein Verkehrsflugzeug erst verspätet gestattet oder verwehrt wurde weil sie fälschlicherweise als Bedrohung identifiziert wurden. Nach dem Administrative Procedure Act und Titel 49 des United States Codes, Abschnitt 46110, ist jeder Geschädigte berechtigt, bei einem Bundesgericht der Vereinigten Staaten Rechtsmittel gegen eine entsprechende endgültige Entscheidung des DHS einzulegen.

ARTIKEL 14

Aufsicht

(1) Die Einhaltung der Datenschutzgarantien dieses Abkommens wird von unabhängigen Datenschutzbeauftragten der jeweiligen Einrichtung, wie dem obersten Datenschutzbeauftragten des DHS (DHS Chief Privacy Officer), überprüft und beaufsichtigt, die

- a) nachweislich unabhängig Entscheidungen treffen,

- b) wirksame Aufsichts-, Ermittlungs-, Interventions- und Prüfungsvollmachten haben und
- c) befugt sind, bei Zuwiderhandlungen im Zusammenhang mit diesem Abkommen gegebenenfalls eine strafrechtliche Verfolgung einleiten oder Disziplinarmaßnahmen verhängen zu lassen.

Die Datenschutzbeauftragten tragen insbesondere dafür Sorge, dass Beschwerden betreffend Verstöße gegen das Abkommen entgegengenommen, untersucht und beantwortet werden und angemessene Abhilfemaßnahmen ergriffen werden. Jede Person ist unabhängig von ihrer Staatsangehörigkeit, ihrem Herkunfts- oder Wohnsitzland berechtigt, Beschwerde einzulegen.

(2) Die Anwendung des Abkommens durch die Vereinigten Staaten wird zudem einer unabhängigen Überprüfung und Aufsicht durch eine oder mehrere der folgenden Einrichtungen unterstellt:

- a) des Office of Inspector General des DHS,
- b) des vom Kongress eingerichteten Government Accountability Office sowie
- c) des Kongresses der Vereinigten Staaten.

Die Ergebnisse der Aufsichtsmaßnahmen und Empfehlungen können in öffentlichen Berichten, Anhörungen und Analysen veröffentlicht werden.

KAPITEL III

ÜBERMITTLUNGSMODALITÄTEN

ARTIKEL 15

Verfahren zur Übermittlung von PNR-Daten

- (1) Für die Zwecke dieses Abkommens sind die Fluggesellschaften verpflichtet, PNR-Daten nach dem Push-Verfahren zu übermitteln, damit die erforderliche Genauigkeit, Schnelligkeit und Vollständigkeit der PNR-Datenübermittlung gewährleistet sind.
- (2) Die Fluggesellschaften sind verpflichtet, die PNR-Daten auf gesichertem elektronischem Wege entsprechend den technischen Anforderungen des DHS an das DHS zu übermitteln.
- (3) Die Fluggesellschaften sind verpflichtet, die PNR-Daten gemäß den Absätzen 1 und 2 zunächst 96 Stunden vor planmäßigem Abflug an das DHS zu übermitteln und erneut entweder bei jeder Eingabe neuer PNR-Daten, in regelmäßigen Abständen oder nach einem von der DHS festgelegten Zeitplan für die Übermittlungen.
- (4) In jedem Fall sind alle Fluggesellschaften verpflichtet, spätestens 24 Monate nach Inkrafttreten dieses Abkommens die technischen Anforderungen für die Anwendung des Push-Verfahrens zu erfüllen.

(5) Das DHS kann im Einzelfall gegebenenfalls von einzelnen Fluggesellschaften verlangen, zwischen den regulären Übermittlungen gemäß Absatz 3 oder danach weitere PNR-Daten zu übermitteln. Ist eine Fluggesellschaft aus technischen Gründen nicht in der Lage, die nach diesem Artikel verlangten Daten gemäß den DHS-Anforderungen rechtzeitig zu übermitteln, oder in Ausnahmefällen bei einer spezifischen, unmittelbaren und schweren Bedrohung kann das DHS von der Fluggesellschaft verlangen, die Daten auf anderem Wege zur Verfügung zu stellen.

ARTIKEL 16

Weitergabe der Daten innerhalb der Vereinigten Staaten

- (1) Das DHS darf PNR-Daten nur nach sorgfältiger Prüfung folgender Garantien weitergeben:
 - a) Die Weitergabe erfolgt ausschließlich nach Maßgabe des Artikels 4.
 - b) Die Daten werden ausschließlich an innerstaatliche Staatsbehörden und nur zu den in Artikel 4 angegebenen Zwecken weitergegeben.
 - c) Die Empfänger wenden auf die PNR-Daten die in diesem Abkommen festgelegten oder vergleichbare Garantien an.
 - d) PNR-Daten werden nur für Untersuchungs- oder Ermittlungszwecke in konkreten Fällen und nur auf der Grundlage schriftlicher Vereinbarungen und nach Maßgabe der Vorschriften der Vereinigten Staaten über den Austausch von Informationen zwischen innerstaatlichen Behörden weitergegeben.

(2) Werden analytische Informationen übermittelt, die im Rahmen dieses Abkommens aus PNR-Daten gewonnen wurden, so sind die in Absatz 1 des vorliegenden Artikels festgelegten Garantien einzuhalten.

ARTIKEL 17

Übermittlung von Informationen in Drittländer

(1) Die Vereinigten Staaten dürfen PNR-Daten nur in Einklang mit diesem Abkommen und nach Vergewisserung, dass die vom Empfänger beabsichtigte Verwendung der Daten die Bedingungen des Abkommens erfüllt, an zuständige Behörden von Drittländern weitergeben.

(2) Für eine solche Datenübermittlung bedarf es einer ausdrücklichen Vereinbarung, in der Datenschutzgarantien festgelegt sind, die den vom DHS angewendeten Garantien für PNR-Daten nach diesem Abkommen entsprechen, es sei denn, es handelt sich um einen Notfall.

(3) PNR-Daten werden nur zu Untersuchungs- und Ermittlungszwecken in konkreten Fällen weitergegeben.

(4) Ist dem DHS bekannt, dass PNR-Daten eines Bürgers eines EU-Mitgliedstaats oder einer in einem Mitgliedstaat ansässigen Person weitergegeben werden, so sind die zuständigen Behörden des betreffenden Mitgliedstaats zum frühestmöglichen Zeitpunkt davon zu unterrichten.

(5) Werden analytische Informationen übermittelt, die im Rahmen dieses Abkommens aus PNR-Daten gewonnen wurden, so sind die in den Absätzen 1 bis 4 festgelegten Garantien zu beachten.

ARTIKEL 18

Zusammenarbeit zwischen Polizei-, Strafverfolgungs- und Justizbehörden

- (1) Gemäß geltenden Abkommen oder Vereinbarungen über die Strafverfolgung oder den Informationsaustausch zwischen den Vereinigten Staaten und EU-Mitgliedstaaten oder Europol und Eurojust übermittelt das DHS, sobald dies praktisch möglich, relevant und angebracht ist, analytische Informationen, die aus den PNR gewonnen wurden, je nach Zuständigkeit an die jeweiligen Polizeibehörden, andere spezialisierte Strafverfolgungs- oder Justizbehörden der EU-Mitgliedstaaten sowie an Europol und Eurojust zu Untersuchungs- und Ermittlungszwecken in konkreten Fällen mit dem Ziel, terroristische und damit verbundener Straftaten und grenzübergreifende Straftaten im Sinne von Artikel 4 Absatz 1 Buchstabe b in der Europäischen Union zu verhindern, aufzudecken, zu untersuchen oder strafrechtlich zu verfolgen.
- (2) Polizei- oder Justizbehörden eines EU-Mitgliedstaats, Europol und Eurojust können im Rahmen ihres Auftrags den Zugang zu PNR-Daten oder einschlägigen analytischen Informationen, die aus PNR-Daten gewonnen wurden, beantragen, wenn dies in einem konkreten Fall zur Verhinderung, Aufdeckung, Untersuchung oder strafrechtlichen Verfolgung einer terroristischen und damit verbundener Straftaten oder grenzübergreifender Straftaten im Sinne von Artikel 4 Absatz 1 Buchstabe b in der Europäischen Union erforderlich ist. Das DHS liefert diese Informationen vorbehaltlich der in Absatz 1 genannten Abkommen und Vereinbarungen.
- (3) Gemäß den Absätzen 1 und 2 gibt das DHS PNR-Daten nur nach sorgfältiger Prüfung folgender Garantien weiter:
 - a) Die Weitergabe erfolgt ausschließlich nach Maßgabe des Artikels 4.

- b) Die Daten werden ausschließlich zu den in Artikel 4 genannten Zwecken weitergegeben und
 - c) die Empfänger wenden auf die PNR-Daten die in diesem Abkommen festgelegten oder vergleichbare Garantien an.
- (4) Werden analytische Informationen übermittelt, die im Rahmen dieses Abkommens aus PNR-Daten gewonnen wurden, sind die in den Absätzen 1 bis 3 des vorliegenden Artikels festgelegten Garantien zu beachten.

KAPITEL IV

DURCHFÜHRUNGS- UND SCHLUSSBESTIMMUNGEN

ARTIKEL 19

Angemessenheit

Im Hinblick auf dieses Abkommen und seine Anwendung wird davon ausgegangen, dass das DHS die PNR-Daten im Sinne der einschlägigen Datenschutzvorschriften der EU bei der Verarbeitung und Verwendung angemessen schützt. Wenn Fluggesellschaften dem DHS nach Maßgabe dieses Abkommens PNR-Daten übermittelt haben, gelten die einschlägigen rechtlichen Anforderungen in der EU bezüglich der Übermittlung solcher Daten aus der EU an die Vereinigten Staaten als erfüllt.

ARTIKEL 20

Gegenseitigkeit

(1) Die Parteien wirken im Einklang mit diesem Abkommen in ihrem jeweiligen Gebiet aktiv darauf hin, dass die Fluggesellschaften mit dem PNR-System kooperieren, das im Gebiet der anderen Partei verwendet wird oder dort eingeführt werden könnte.

(2) Da die Einführung eines PNR-Systems der EU wesentliche Auswirkungen auf die Verpflichtungen der Parteien nach diesem Abkommen haben könnte, beraten sich die Parteien – falls und sobald die EU ein PNR-System einführt – darüber, ob dieses Abkommen entsprechend geändert werden muss, um die volle Gegenseitigkeit sicherzustellen. Insbesondere wird dabei geprüft, ob bei dem künftigen PNR-System der EU weniger strenge Datenschutzstandards angewandt werden als nach diesem Abkommen und ob dieses Abkommen daher geändert werden sollte.

ARTIKEL 21

Durchführung und Ausnahmeverbot

(1) Durch dieses Abkommen werden nach dem Recht der Vereinigten Staaten 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) Dieses Abkommen weicht in keinem Punkt von bestehenden Verpflichtungen der Vereinigten Staaten und der EU-Mitgliedstaaten, darunter aus dem Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Rechtshilfe vom 25. Juni 2003 und den damit verbundenen zweiseitigen Rechtshilfeabkommen zwischen den Vereinigten Staaten und den EU-Mitgliedstaaten, ab.

ARTIKEL 22

Mitteilung von Änderungen des geltenden Rechts

Die Parteien teilen einander den Erlass von Rechts- und Verwaltungsvorschriften mit, die wesentliche Auswirkungen auf die Durchführung dieses Abkommens haben.

ARTIKEL 23

Überprüfung und Evaluierung

(1) Die Parteien überprüfen ein Jahr nach Inkrafttreten dieses Abkommens und danach regelmäßig gemeinsam seine Durchführung. Zudem evaluieren die Parteien gemeinsam das Abkommen vier Jahre nach seinem Inkrafttreten.

(2) Die Parteien legen vor einer gemeinsamen Überprüfung gemeinsam deren Einzelheiten und Bedingungen fest und unterrichten einander über die Zusammensetzung ihrer jeweiligen Überprüfungsteams. Für die Zwecke der gemeinsamen Überprüfung wird die Europäische Union durch die Europäische Kommission vertreten; die Vereinigten Staaten werden durch das DHS vertreten. Die Überprüfungsteams können auch geeignete Fachleute für Datenschutz und Strafverfolgungsexperten umfassen. Vorbehaltlich geltender Rechtsvorschriften müssen die an der gemeinsamen Überprüfung Beteiligten einer angemessenen Sicherheitsüberprüfung unterzogen werden und die Vertraulichkeit der Beratungen wahren. Für die Zwecke der gemeinsamen Überprüfung gewährt das DHS einen angemessenen Zugang zu den jeweiligen Unterlagen, Systemen und Mitarbeitern.

(3) Im Anschluss an eine gemeinsame Überprüfung unterbreitet die Europäische Kommission dem Europäischen Parlament und dem Rat der Europäischen Union einen Bericht. Den Vereinigten Staaten wird Gelegenheit zur schriftlichen Stellungnahme gegeben, die dem Bericht beigefügt wird.

ARTIKEL 24

Streitbeilegung und Aussetzung des Abkommens

(1) Bei Streitigkeiten über die Durchführung dieses Abkommens sowie bei allen damit zusammenhängenden Fragen konsultieren die Parteien einander, um eine einvernehmliche Lösung zu erzielen, die es beiden Parteien ermöglicht, innerhalb eines angemessenen Zeitraums Abhilfe zu schaffen.

(2) Falls die Konsultationen keine Beilegung des Streits bewirken, kann jede Partei durch schriftliche Notifikation auf diplomatischem Wege die Anwendung dieses Abkommens aussetzen; sofern die Parteien keinen anderen Zeitpunkt vereinbaren, wird eine solche Aussetzung 90 Tage ab dem Datum ihrer Notifikation wirksam.

(3) Ungeachtet der Aussetzung dieses Abkommens werden alle PNR-Daten, die dem DHS aufgrund dieses Abkommens vor der Aussetzung übermittelt wurden, weiter im Einklang mit den Garantien dieses Abkommens verarbeitet und verwendet.

ARTIKEL 25

Kündigung

(1) Dieses Abkommen kann von jeder Partei durch schriftliche Notifikation auf diplomatischem Wege jederzeit gekündigt werden.

(2) Die Kündigung wird 120 Tage ab dem Datum ihrer Notifikation wirksam, sofern die Parteien keinen anderen Zeitpunkt vereinbaren.

(3) Vor einer etwaigen Kündigung dieses Abkommens konsultieren die Parteien einander in einer Weise, die ausreichend Zeit lässt, um zu einer einvernehmlichen Lösung zu gelangen.

(4) Ungeachtet der Kündigung dieses Abkommens werden alle PNR-Daten, die dem DHS aufgrund dieses Abkommens vor der Kündigung übermittelt wurden, weiter im Einklang mit den Garantien dieses Abkommens verarbeitet und verwendet.

ARTIKEL 26

Laufzeit

(1) Vorbehaltlich Artikel 25 gilt dieses Abkommens für einen Zeitraum von sieben Jahren ab dem Zeitpunkt seines Inkrafttretens.

(1) Am Ende des in Absatz 1 des vorliegenden Artikels 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) Ungeachtet des Auslaufens dieses Abkommens werden alle PNR-Daten, die dem DHS aufgrund dieses Abkommens übermittelt wurden, weiter im Einklang mit den Garantien dieses Abkommens verarbeitet und verwendet. Entsprechend werden alle PNR-Daten, die das DHS nach Maßgabe des am 23. beziehungsweise am 26. Juli 2007 in Brüssel beziehungsweise in Washington unterzeichneten Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security erhalten hat, weiterhin nach Maßgabe jenen Abkommens verarbeitet und verwendet.

ARTIKEL 27

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 notifiziert haben.
- (2) Dieses Abkommen tritt ab dem Tag seines Inkrafttretens an die Stelle des am 23. beziehungsweise 26. Juli 2007 unterzeichneten Abkommens.
- (3) Dieses Abkommen gilt nur dann für das Hoheitsgebiet Dänemarks, des Vereinigten Königreichs oder Irlands, wenn die Europäische Kommission den Vereinigten Staaten schriftlich notifiziert, dass Dänemark, das Vereinigte Königreich oder Irland beschlossen hat, durch dieses Abkommen gebunden zu sein.
- (4) Notifiziert die Europäische Kommission den Vereinigten Staaten vor Inkrafttreten dieses Abkommens, dass es auf das Hoheitsgebiet Dänemarks, des Vereinigten Königreichs oder Irlands Anwendung findet, so gilt das Abkommen für das Hoheitsgebiet des betreffenden Staates ab dem gleichen Tag wie für die anderen durch dieses Abkommen gebundenen EU-Mitgliedstaaten.

(5) Notifiziert die Europäische Kommission den Vereinigten Staaten nach Inkrafttreten dieses Abkommens, dass es auf das Hoheitsgebiet Dänemarks, des Vereinigten Königreichs oder Irlands Anwendung findet, gilt das Abkommen für das Hoheitsgebiet des betreffenden Staates ab dem ersten Tag nach Eingang der Notifikation bei den Vereinigten Staaten.

Geschehen zu ... am ... 2011 in zwei Urschriften.

Nach EU-Recht wird das Abkommen von der EU 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.

Arten von PNR-Daten

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 zum Dateneingabe
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
-