EUROPEAN COMMISSION

Brussels, 23.11.2011
COM(2011) 805 final

2011/0383 (NLE)

Proposal for a

COUNCIL DECISION

on the signature of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security

EXPLANATORY MEMORANDUM

U.S. legislation empowers the Department of Homeland Security (DHS) to require each air carrier operating passenger flights to and from the U.S., to provide it with electronic access to Passenger Name Record (PNR) data prior to the passenger arriving or leaving the U.S. The requirements of the U.S. authorities are based on title 49, United States Code, section 44909c (3) and its implementing regulations (title 19, Code of federal regulations, section 122.49b).

This legislation aims at obtaining PNR data electronically in advance of a flight's arrival and therefore significantly enhances DHS ability to conduct efficient and effective advance risk assessment of passengers and to facilitate bona fide travel, thereby enhancing the security of the U.S. The Agreement will also foster international police and judicial cooperation through the transfer of analytical information flowing from PNR data by the U.S. to the competent Member States authorities as well as Europol and Eurojust within their respective competences.

PNR is a record of each passenger's travel requirements which contains all information necessary to enable reservations to be processed and controlled by air carriers.

Air carriers are under an obligation to provide the DHS with access to certain PNR data contained in the air carrier's automated reservation and departure control systems.

The data protection laws of the EU do not allow European and other carriers operating flights from the EU to transmit the PNR data of their passengers to third countries which do not ensure an adequate level of protection of personal data without adducing appropriate safeguards. A solution is required that will provide the legal basis for the transfer of PNR data from the EU to the U.S. as a recognition of the necessity and importance of the use of PNR data in the fight against terrorism and other serious transnational crime, whilst avoiding legal uncertainty for air carriers. In addition, this solution should be applied homogenously throughout the European Union in order to ensure a legal certainty for air carriers and respect of individuals' rights to the protection of personal data as well as their physical security.

The European Union signed an agreement in 2007 with the United States on the transfer and processing of PNR data based on a set of commitments by DHS in relation to the application of its PNR programme[1].

Following the entry into force of the Lisbon Treaty and pending the conclusion of the agreement, the Council sent the 2007 U.S. Agreement to the European Parliament for its consent for the conclusion. The European Parliament adopted a resolution[2] in which it decided to postpone its vote on the requested consent and requesting a renegotiation of the Agreement on the basis of certain criteria. Pending such renegotiation, the 2007 Agreement would remain provisionally applicable.

On 21 September 2010, the Council received a recommendation from the Commission to authorise the opening of negotiations for an Agreement between the European Union and the United States of America for the use and transfer of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crime.

---

1 OJ L204/16, 4.8.2007

2 P7_TA-(2010)0144, 5.5.2010

On 11 November 2010, the European Parliament adopted a resolution on the Recommendation from the Commission to the Council to authorise the opening of the negotiations.

On 2 December 2010, the Council adopted a Decision, together with a negotiation directive, authorising the Commission to open negotiations on behalf of the European Union. Following negotiations between the parties, the Agreement was initialled on 17 November 2011.

This Agreement takes into consideration and is consistent with the general criteria laid down in the Communication from the Commission on the Global Approach to the transfer of Passenger Name Record (PNR) data to third countries[3] and the negotiating directives given by the Council.

PNR has proven to be a very important tool in the fight against terrorism and serious crime. The Agreement has secured several important safeguards for those whose data will be transferred and used. In particular, the purpose of processing of PNR data is strictly limited to preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crime. The retention period of the PNR data is limited and PNR will be used for a shorter period in the fight against serious transnational crime and a longer one for terrorism. In addition, the data will be depersonalised after a period of 6 months. Individuals are provided with the right to access, correction, redress and information. The 'push' method of transfer is recognised as the standard mode of transfer, with which all carriers will need to comply within 2 years of the Agreement. Sensitive data is to be used in very exceptional cases and deleted after a very short timeframe. Compliance with these rules shall be subject to independent review and oversight by various Department Privacy Officers, as well as by the DHS Office of Inspector General, the Government Accountability Office and the U.S. Congress.

The Article 218(5) of the Treaty on the Functioning of the European Union states that the Council shall authorise the signing of international agreements.

The Commission therefore proposes to the Council to adopt a decision authorising the signing of the Agreement between the European Union and the United States of America on the use and transfer of Passenger Name Record data to the United States Department of Homeland Security.

[3] COM(2010)492.

2011/0383 (NLE)

Proposal for a

COUNCIL DECISION

on the signature of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 82(1)(d) and 87(2)(a), in conjunction with Article 218 (5) thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) On 2 December 2010, the Council adopted a Decision, together with negotiation directives, authorising the Commission to open negotiations on behalf of the European Union between the European Union and the United States of America for the transfer and use of Passenger Name Records (PNR) to prevent and combat terrorism and other serious transnational crime.

(2) The Agreement has been negotiated. The negotiations were successfully concluded by the initialling of the agreement.

(3) The Agreement should be signed subject to its conclusion at a later date.

(4) This Agreement respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, notably the right to private and family life, recognised in Article 7 of the Charter, the right to the protection of personal data, recognised in Article 8 of the Charter and the right to effective remedy and fair trial recognised by Article 47 of the Charter. This Agreement should be applied in accordance with those rights and principles.

(5) [In accordance with Article 3 of the Protocol 21 on the Position of the United Kingdom and Ireland in respect of the area of Freedom, Security and Justice annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, the United Kingdom and Ireland take part in the adoption of this Decision.]

(6) In accordance with Articles 1 and 2 of the Protocol 22 on the Position of Denmark annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Decision and is not bound by the Agreement or subject to its application,

HAS ADOPTED THIS DECISION:

Article 1

The signing of the Agreement between the European Union and the United States of America on the use and transfer of Passenger Name Records to the United States Department of Homeland Security is hereby approved, subject to its conclusion at a later date.

The text of the Agreement to be signed is attached to this Decision.

The Commission is authorised to designate the persons empowered to proceed to the signature, subject to its conclusion.

Article 2

The Declaration by the EU on the Agreement on the use and transfer of Passenger Name Records to the United States Department of Homeland Security ("the Agreement") in respect of its obligations under Articles 17 and 23 of the Agreement is hereby approved.

The text of the Declaration is attached to the present decision.

Article 3

This Decision shall enter into force on the day of its adoption.

Done at Brussels,

For the Council
The President

ANNEX I

AGREEMENT BETWEEN THE UNITED STATES OF AMERICA AND THE EUROPEAN UNION ON THE USE AND TRANSFER OF PASSENGER NAME RECORDS TO THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY

THE UNITED STATES OF AMERICA

and

THE EUROPEAN UNION,

Hereinafter referred to as "the Parties,"

DESIRING to prevent and combat terrorism and serious transnational crime effectively as a means of protecting their respective democratic societies and common values;

SEEKING to enhance and encourage cooperation between the Parties in the spirit of transatlantic partnership;

RECOGNIZING the right and responsibility of states to ensure the security of their citizens and protect their borders and mindful of the responsibility of all nations to protect the life and safety of the public including those using international transportation systems;

CONVINCED that information sharing is an essential component in the fight against terrorism and serious transnational crime and that in this context, the processing and use of Passenger Name Records (PNR) is a necessary tool that gives information that cannot be obtained by other means;

DETERMINED to prevent and combat terrorist offenses and transnational crime, while respecting fundamental rights and freedoms and recognizing the importance of privacy and the protection of personal data and information;

HAVING REGARD for international instruments, U.S. statutes and regulations requiring each air carrier operating passenger flights in foreign air transportation to or from the United States to make PNR available to the Department of Homeland Security (DHS) to the extent they are collected and contained in the air carrier's automated reservation/departure control systems, and comparable requirements that are or may be implemented in the EU;

NOTING that DHS processes and uses PNR for the purpose of preventing, detecting, investigating and prosecuting terrorist offenses and transnational crime in compliance with safeguards on privacy and the protection of personal data and information, as set out in this Agreement;

STRESSING the importance of sharing PNR and relevant and appropriate analytical information obtained from PNR by the United States with competent police and judicial authorities of Member States, and Europol or Eurojust as a means to foster international police and judicial cooperation;

ACKNOWLEDGING both Parties' longstanding traditions of respect for individual privacy, as reflected in their laws and founding documents;

MINDFUL of the EU's commitments pursuant to Article 6 of the Treaty on European Union on respect for fundamental rights, the right to privacy with regard to the processing of personal data as stipulated in Article 16 of the Treaty on the Functioning of the European Union, the principles of proportionality and necessity concerning the right to private and family life, the respect for privacy, and the protection of personal data under Article 8 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional Protocol 181, and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union;

MINDFUL that DHS currently employs robust processes to protect personal privacy and ensure data integrity, including physical security, access controls, data separation and encryption, audit capabilities and effective accountability measures;

RECOGNIZING the importance of ensuring data quality, accuracy, integrity, and security, and instituting appropriate accountability to ensure these principles are observed;

NOTING in particular the principle of transparency and the various means by which the United States ensures that passengers whose PNR is collected by DHS are made aware of the need for and use of their PNR;

FURTHER RECOGNIZING that the collection and analysis of PNR is necessary for DHS to carry out its border security mission, while ensuring that collection and use of PNR remains relevant and necessary for the purposes for which it is collected;

RECOGNIZING that, in consideration of this Agreement and its implementation, DHS shall be deemed to ensure an adequate level of data protection for the processing and use of PNR transferred to DHS;

MINDFUL that the United States and the European Union are committed to ensuring a high level of protection of personal information while fighting crime and terrorism, and are determined to reach, without delay, an agreement to protect personal information exchanged in the context of fighting crime and terrorism in a comprehensive manner that will advance our mutual goals;

ACKNOWLEDGING the successful Joint Reviews in 2005 and 2010 of the 2004 and 2007 Agreements between the Parties on the transfer of PNR;

NOTING the interest of the parties, as well as EU Member States, in exchanging information regarding the method of transmission of PNR as well as the onward transfer of PNR as set forth in the relevant articles of this Agreement, and further noting the EU's interest in having this addressed in the context of the consultation and review mechanism set forth in this Agreement;

AFFIRMING that this Agreement does not constitute a precedent for any future arrangements between the Parties, or between either of the Parties and any other party, regarding the processing, use, or transfer of PNR or any other form of data, or regarding data protection;

RECOGNIZING the related principles of proportionality as well as relevance and necessity that guide this Agreement and its implementation by the European Union and the United States; and

HAVING REGARD to the possibility of the Parties to further discuss the transfer of PNR data in the maritime mode;

HEREBY AGREE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Purpose

1. The purpose of this Agreement is to ensure security and to protect the life and safety of the public.

2. For this purpose, this Agreement sets forth the responsibilities of the Parties with respect to the conditions under which PNR may be transferred, processed and used, and protected.

Article 2

Scope

1. PNR, as set forth in the Guidelines of the International Civil Aviation Organization, shall mean the record created by air carriers or their authorized agents for each journey booked by or on behalf of any passenger and contained in carriers' reservation systems, departure control systems, or equivalent systems providing similar functionality (collectively referred to in this Agreement as reservation systems). Specifically, as used in this Agreement, PNR consists of the data types set forth in the annex to this Agreement.

2. This Agreement shall apply to carriers operating passenger flights between the European Union and the United States.

3. This Agreement shall also apply to carriers incorporated or storing data in the European Union and operating passenger flights to or from the United States.

Article 3

Provision of PNR

The Parties agree that carriers shall provide PNR contained in their reservation systems to DHS as required by and in accordance with DHS standards and consistent with this Agreement. Should PNR transferred by carriers include data beyond those listed in the annex to this Agreement, DHS shall delete such data upon receipt.

Article 4

Use of PNR

1. The United States collects, uses and processes PNR for the purposes of preventing, detecting, investigating, and prosecuting:

   (a) Terrorist offenses and related crimes, including

      i. Conduct that –

         1. involves a violent act or an act dangerous to human life, property, or infrastructure; and

         2. appears to be intended to –

            a. intimidate or coerce a civilian population;

            b. influence the policy of a government by intimidation or coercion; or

            c. affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.

      ii. Activities constituting an offense within the scope of and as defined in applicable international conventions and protocols relating to terrorism;

      iii. Providing or collecting funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the acts described in subparagraphs (i) or (ii);

      iv. Attempting to commit any of the acts described in subparagraphs (i), (ii), or (iii);

      v. Participating as an accomplice in the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

      vi. Organizing or directing others to commit any of the acts described in subparagraphs (i), (ii), or (iii);

      vii. Contributing in any other way to the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

      viii. Threatening to commit an act described in subparagraph (i) under circumstances which indicate that the threat is credible;

(b) Other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature.

A crime is considered as transnational in nature in particular if:

i. It is committed in more than one country;

ii. It is committed in one country but a substantial part of its preparation, planning, direction or control takes place in another country;

iii. It is committed in one country but involves an organized criminal group that engages in criminal activities in more than one country;

iv. It is committed in one country but has substantial effects in another country; or

v. It is committed in one country and the offender is in or intends to travel to another country.

2. PNR may be used and processed on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court.

3. PNR may be used and processed by DHS to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination.

4. Paragraphs 1, 2, and 3 of this Article shall be without prejudice to domestic law enforcement, judicial powers, or proceedings, where other violations of law or indications thereof are detected in the course of the use and processing of PNR.

CHAPTER II

SAFEGUARDS APPLICABLE TO THE USE OF PNR

Article 5

Data Security

1. DHS shall ensure that appropriate technical measures and organizational arrangements are implemented to protect personal data and personal information contained in PNR against accidental, unlawful or unauthorized destruction, loss, disclosure, alteration, access, processing or use.

2. DHS shall make appropriate use of technology to ensure data protection, security, confidentiality and integrity. In particular, DHS shall ensure that:

(a) encryption, authorization and documentation procedures recognized by competent authorities are applied. In particular, access to PNR shall be secured and limited to specifically authorized officials;

(b) PNR shall be held in a secure physical environment and protected with physical intrusion controls; and

(c) mechanism exists to ensure that PNR queries are conducted consistent with Article 4.

3. In the event of a privacy incident (including unauthorized access or disclosure), DHS shall take reasonable measures to notify affected individuals as appropriate, to mitigate the risk of harm of unauthorized disclosures of personal data and information, and to institute remedial measures as may be technically practicable.

4. Within the scope of this Agreement, DHS shall inform without undue delay the relevant European authorities about cases of significant privacy incidents involving PNR of EU citizens or residents resulting from accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, or any unlawful forms of processing or use.

5. The United States confirms that effective administrative, civil, and criminal enforcement measures are available under U.S. law for privacy incidents. DHS may take disciplinary action against persons responsible for any such privacy incident, as appropriate, to include denial of system access, formal reprimands, suspension, demotion, or removal from duty.

6. All access to PNR, as well as its processing and use, shall be logged or documented by DHS. Logs or documentation shall be used only for oversight, auditing, and system maintenance purposes or as otherwise required by law.

Article 6

Sensitive Data

1. To the extent that PNR of a passenger as collected includes sensitive data (i.e., personal data and information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning the health or sex life of the individual), DHS shall employ automated systems to filter and mask out sensitive data from PNR. In addition, DHS shall not further process or use such data, except in accordance with paragraphs 3 and 4 of this Article.

2. DHS shall provide to the European Commission within 90 days of the entry into force of this Agreement a list of codes and terms identifying sensitive data that shall be filtered out.

3. Access to, as well as processing and use of, sensitive data shall be permitted in exceptional circumstances where the life of an individual could be imperiled or seriously impaired. Such data may be exclusively accessed using restrictive processes on a case-by-case basis with the approval of a DHS senior manager.

4. Sensitive data shall be permanently deleted not later than 30 days from the last receipt of PNR containing such data by DHS. However, sensitive data may be retained for the time specified in U.S. law for the purpose of a specific investigation, prosecution or enforcement action.

Article 7

Automated Individual Decisions

The United States shall not make decisions that produce significant adverse actions affecting the legal interests of individuals based solely on automated processing and use of PNR.

Article 8

Retention of Data

1. DHS retains PNR in an active database for up to five years. After the initial six months of this period, PNR shall be depersonalized and masked in accordance with paragraph 2 of this Article. Access to this active database shall, unless otherwise permitted by this Agreement, be restricted to a limited number of specifically authorized officials.

2. To achieve depersonalization, personally identifiable information contained in the following PNR data types shall be masked out:

   (a) name(s);

   (b) other names on PNR;

   (c) all available contact information (including originator information);

   (d) General Remarks, including other supplementary information (OSI), special service information (SSI), and special service request (SSR); and

   (e) any collected APIS information.

3. After this active period, PNR shall be transferred to a dormant database for a period of up to ten years. This dormant database shall be subject to additional controls, including a more restricted number of authorized personnel, as well as a higher level of supervisory approval required before access. In this dormant database, PNR shall not be repersonalized except in connection with law enforcement operations and then only in connection with an identifiable case, threat or risk. As regards the purposes as set out in Article 4, paragraph (1)(b), PNR in this dormant database may only be repersonalized for a period of up to five years.

4. Following the dormant period, data retained must be rendered fully anonymized by deleting all data types which could serve to identify the passenger to whom PNR relate without the possibility of repersonalization.

5. Data that are related to a specific case or investigation may be retained in an active PNR database until the case or investigation is archived. This paragraph is without prejudice to data retention requirements for individual investigation or prosecution files.

6. The Parties agree that, within the framework of the evaluation as provided for in Article 23, paragraph 1, the necessity of a 10-year dormant period of retention will be considered.

Article 9

Non-discrimination

The United States shall ensure that the safeguards applicable to processing and use of PNR under this Agreement apply to all passengers on an equal basis without unlawful discrimination.

Article 10

Transparency

1. DHS shall provide information to the traveling public regarding its use and processing of PNR through:

   (a) publications in the Federal Register;

   (b) publications on its website;

   (c) notices that may be incorporated by the carriers into contracts of carriage;

   (d) statutorily required reporting to Congress; and

   (e) other appropriate measures as may be developed.

2. DHS shall publish and provide to the EU for possible publication its procedures and modalities regarding access, correction or rectification, and redress procedures.

3. The Parties shall work with the aviation industry to encourage greater visibility to passengers at the time of booking on the purpose of the collection, processing and use of PNR by DHS, and on how to request access, correction and redress.

Article 11

Access for Individuals

1. In accordance with the provisions of the Freedom of Information Act, any individual, regardless of nationality, country of origin, or place of residence is entitled to request his or her PNR from DHS. DHS shall timely provide such PNR subject to the provisions of paragraphs 2 and 3 of this Article.

2. Disclosure of information contained in PNR may be subject to reasonable legal limitations, applicable under U.S. law, including any such limitations as may be necessary to safeguard privacy-protected, national security, and law enforcement sensitive information.

3. Any refusal or restriction of access shall be set forth in writing and provided to the requesting individual on a timely basis. Such notification shall include the legal basis on which information was withheld and shall inform the individual of the options available under U.S. law for seeking redress.

4. DHS shall not disclose PNR to the public, except to the individual whose PNR has been processed and used or his or her representative, or as required by U.S. law.

Article 12

Correction or Rectification for Individuals

1. Any individual regardless of nationality, country of origin, or place of residence may seek the correction or rectification, including the possibility of erasure or blocking, of his or her PNR by DHS pursuant to the processes described in this Agreement.

2. DHS shall inform, without undue delay, the requesting individual in writing of its decision whether to correct or rectify the PNR at issue.

3. Any refusal or restriction of correction or rectification shall be set forth in writing and provided to the requesting individual on a timely basis. Such notification shall include the legal basis of such refusal or restriction and shall inform the individual of the options available under U.S. law for seeking redress.

Article 13

Redress for Individuals

1. Any individual regardless of nationality, country of origin, or place of residence whose personal data and personal information has been processed and used in a manner inconsistent with this Agreement may seek effective administrative and judicial redress in accordance with U.S. law.

2. Any individual is entitled to seek to administratively challenge DHS decisions related to the use and processing of PNR.

3. Under the provisions of the Administrative Procedure Act and other applicable law, any individual is entitled to petition for judicial review in U.S. federal court of any final agency action by DHS. Further, any individual is entitled to petition for judicial review in accordance with applicable law and relevant provisions of:

   (a) the Freedom of Information Act;

   (b) the Computer Fraud and Abuse Act;

   (c) the Electronic Communications Privacy Act; and

   (d) other applicable provisions of U.S. law.

4. In particular, DHS provides all individuals an administrative means (currently the DHS Traveler Redress Inquiry Program (DHS TRIP)) to resolve travel-related

inquiries including those related to the use of PNR. DHS TRIP provides a redress process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat. Pursuant to the Administrative Procedure Act and Title 49, United States Code, Section 46110, any such aggrieved individual is entitled to petition for judicial review in U.S. federal court from any final agency action by DHS relating to such concerns.

Article 14

Oversight

1. Compliance with the privacy safeguards in this Agreement shall be subject to independent review and oversight by Department Privacy Officers, such as the DHS Chief Privacy Officer, who:

   (a) have a proven record of autonomy;

   (b) exercise effective powers of oversight, investigation, intervention, and review; and

   (c) have the power to refer violations of law related to this Agreement for prosecution or disciplinary action, when appropriate.

   They shall, in particular, ensure that complaints relating to non-compliance with this Agreement are received, investigated, responded to, and appropriately redressed. These complaints may be brought by any individual, regardless of nationality, country of origin, or place of residence.

2. In addition, application of this Agreement by the United States shall be subject to independent review and oversight by one or more of the following entities:

   (a) the DHS Office of Inspector General;

   (b) the Government Accountability Office as established by Congress; and

   (c) the U.S. Congress.

   Such oversight may be manifested in the findings and recommendations of public reports, public hearings, and analyses.

CHAPTER III

MODALITIES OF TRANSFERS

Article 15

Method of PNR Transmission

1. For the purposes of this Agreement, carriers shall be required to transfer PNR to DHS using the "push" method, in furtherance of the need for accuracy, timeliness and completeness of PNR.

2. Carriers shall be required to transfer PNR to DHS by secure electronic means in compliance with the technical requirements of DHS.

3. Carriers shall be required to transfer PNR to DHS in accordance with paragraphs 1 and 2 of this Article, initially at 96 hours before the scheduled flight departure and additionally either in real time or for a fixed number of routine and scheduled transfers as specified by DHS.

4. In any case, the Parties agree that all carriers shall be required to acquire the technical ability to use the "push" method not later than 24 months following entry into force of this Agreement.

5. DHS may, where necessary, on a case-by-case basis, require a carrier to provide PNR between or after the regular transfers described in paragraph 3. Wherever carriers are unable, for technical reasons, to respond timely to requests under this Article in accordance with DHS standards, or, in exceptional circumstances in order to respond to a specific, urgent, and serious threat, DHS may require carriers to otherwise provide access.

Article 16

Domestic Sharing

1. DHS may share PNR only pursuant to a careful assessment of the following safeguards:

   (a) Exclusively as consistent with Article 4;

   (b) Only with domestic government authorities when acting in furtherance of the uses outlined in Article 4;

   (c) Receiving authorities shall afford to PNR equivalent or comparable safeguards as set out in this Agreement; and

   (d) PNR shall be shared only in support of those cases under examination or investigation and pursuant to written understandings and U.S. law on the exchange of information between domestic government authorities.

2. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraph 1 of this Article shall be respected.

Article 17

Onward Transfer

1. The United States may transfer PNR to competent government authorities of third countries only under terms consistent with this Agreement and only upon ascertaining that the recipient's intended use is consistent with these terms.

2. Apart from emergency circumstances, any such transfer of data shall occur pursuant to express understandings that incorporate data privacy protections comparable to those applied to PNR by DHS as set out in this Agreement.

3. PNR shall be shared only in support of those cases under examination or investigation.

4. Where DHS is aware that PNR of a citizen or a resident of an EU Member State is transferred, the competent authorities of the concerned Member State shall be informed of the matter at the earliest appropriate opportunity.

5. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraphs 1-4 of this Article shall be respected.

Article 18

Police, Law Enforcement and Judicial Cooperation

1. Consistent with existing law enforcement or other information-sharing agreements or arrangements between the United States and any Member State of the EU or Europol and Eurojust, DHS shall provide to competent police, other specialized law enforcement or judicial authorities of the Member States and Europol and Eurojust within the remit of their respective mandates, as soon as practicable, relevant, and appropriate, analytical information obtained from PNR in those cases under examination or investigation to prevent, detect, investigate, or prosecute within the European Union transnational crime as described in Article 4, paragraph 1(b) or conduct or activities related to terrorist offenses.

2. A police or judicial authority of a Member State of the EU, or Europol or Eurojust, may request, within its mandate, access to PNR or relevant analytical information obtained from PNR that are necessary in a specific case to prevent, detect, investigate, or prosecute within the European Union a terrorist offense or transnational crime as described in Article 4, paragraph 1(b). DHS shall, subject to the agreements and arrangements noted in paragraph 1 of this Article, provide such information.

3. Pursuant to paragraphs 1 and 2 of this Article, DHS shall share PNR only following a careful assessment of the following safeguards:

   (a) Exclusively as consistent with Article 4;

   (b) Only when acting in furtherance of the uses outlined in Article 4; and

   (c) Receiving authorities shall afford to PNR equivalent or comparable safeguards as set out in this Agreement.

4. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraphs 1-3 of this Article shall be respected.

CHAPTER IV

IMPLEMENTING AND FINAL PROVISIONS

Article 19

Adequacy

In consideration of this Agreement and its implementation, DHS shall be deemed to provide, within the meaning of relevant EU data protection law, an adequate level of protection for PNR processing and use. In this respect, carriers which have provided PNR to DHS in compliance with this Agreement shall be deemed to have complied with applicable legal requirements in the EU related to the transfer of such data from the EU to the United States.

Article 20

Reciprocity

1. The Parties shall actively promote the cooperation of carriers within their respective jurisdictions with any PNR system operating or as may be adopted in the other's jurisdiction, consistent with this Agreement.

2. Given that the establishment of an EU PNR system could have a material effect on the Parties' obligations under this Agreement, if and when an EU PNR system is adopted, the Parties shall consult to determine whether the present Agreement would need to be adjusted accordingly to ensure full reciprocity. Such consultations shall in particular examine whether any future EU PNR system would apply less stringent data protection standards than those provided for in the present Agreement, and whether, therefore, it should be amended.

Article 21

Implementation and Non-Derogation

1. This Agreement shall not create or confer, under U.S. law, any right or benefit on any person or entity, private or public. Each Party shall ensure that the provisions of this Agreement are properly implemented.

2. Nothing in this Agreement shall derogate from existing obligations of the United States and Member States, including under the Agreement on Mutual Legal Assistance between the European Union and the United States of 25 June 2003 and the related bilateral mutual legal assistance instruments between the United States and Member States.

Article 22

Notification of Changes in Domestic Law

The Parties shall advise each other regarding the enactment of any legislation that materially affects the implementation of this Agreement.

Article 23

Review and Evaluation

1. The Parties shall jointly review the implementation of this Agreement one year after its entry into force and regularly thereafter as jointly agreed. Further, the Parties shall jointly evaluate this Agreement four years after its entry into force.

2. The Parties shall jointly determine in advance the modalities and terms of the joint review and shall communicate to each other the composition of their respective teams. For the purpose of the joint review, the European Union shall be represented by the European Commission, and the United States shall be represented by DHS. The teams may include appropriate experts on data protection and law enforcement. Subject to applicable laws, participants in the joint review shall be required to have appropriate security clearances and to respect the confidentiality of the discussions. For the purpose of the joint review, DHS shall ensure appropriate access to relevant documentation, systems, and personnel.

3. Following the joint review, the European Commission shall present a report to the European Parliament and the Council of the European Union. The United States shall be given an opportunity to provide written comments which shall be attached to the report.

Article 24

Resolution of Disputes and Suspension of Agreement

1. Any dispute arising from the implementation of this Agreement, and any matters related thereto, shall give rise to consultations between the Parties, with a view to reaching a mutually agreeable resolution, including providing an opportunity for either Party to cure within a reasonable time.

2. In the event that consultations do not result in a resolution of the dispute, either Party may suspend the application of this Agreement by written notification through diplomatic channels, with any such suspension to take effect 90 days from the date of such notification, unless the Parties otherwise agree to a different effective date.

3. Notwithstanding any suspension of this Agreement, all PNR obtained by DHS pursuant to this Agreement prior to its suspension shall continue to be processed and used in accordance with the safeguards of this Agreement.

Article 25

Termination

1. Either Party may terminate this Agreement at any time by written notification through diplomatic channels.

2. Termination shall take effect 120 days from the date of such notification, unless the Parties otherwise agree to a different effective date.

3. Prior to any termination of this Agreement, the Parties shall consult each other in a manner which allows sufficient time for reaching a mutually agreeable resolution.

4. Notwithstanding any termination of this Agreement, all PNR obtained by DHS pursuant to this Agreement prior to its termination shall continue to be processed and used in accordance with the safeguards of this Agreement.

Article 26

Duration

1. Subject to Article 25, this Agreement shall remain in force for a period of seven years from the date of its entry into force.

2. Upon the expiry of the period set forth in paragraph 1 of this Article, as well as any subsequent period of renewal under this paragraph, the Agreement shall be renewed for a subsequent period of seven years unless one of the Parties notifies the other in writing through diplomatic channels, at least twelve months in advance, of its intention not to renew the Agreement.

3. Notwithstanding the expiration of this Agreement, all PNR obtained by DHS under the terms of this Agreement shall continue to be processed and used in accordance with the safeguards of this Agreement. Similarly, all PNR obtained by DHS under the terms of the Agreement Between the United States of America and the European Union on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS), signed at Brussels and Washington July 23 and 26, 2007, shall continue to be processed and used in accordance with the safeguards of that Agreement.

Article 27

Final provisions

1. This Agreement shall enter into force on the first day of the month after the date on which the Parties have exchanged notifications indicating that they have completed their internal procedures for this purpose.

2. This Agreement, as of the date of its entry into force, shall supersede the July 23 and 26, 2007 Agreement .

3. This Agreement will only apply to the territory of Denmark, the United Kingdom or Ireland, if the European Commission notifies the United States in writing that Denmark, the United Kingdom or Ireland has chosen to be bound by this Agreement.

4. If the European Commission notifies the United States before the entry into force of this Agreement that it will apply to the territory of Denmark, the United Kingdom or Ireland, this Agreement shall apply to the territory of such State on the same day as for the other EU Member States bound by this Agreement.

5. If the European Commission notifies the United States after entry into force of this Agreement that it applies to the territory of Denmark, the United Kingdom or Ireland, this Agreement shall apply to the territory of such State on the first day following receipt of the notification by the United States.

Done at…this…day of…2011, in two originals.

Pursuant to EU law, this Agreement shall also be drawn up by the EU in the Bulgarian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish languages.

ANNEX

PNR Data Types

1. PNR record locator code
2. Date of reservation/issue of ticket
3. Date(s) of intended travel
4. Name(s)
5. Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.)
6. Other names on PNR, including number of travelers on PNR
7. All available contact information (including originator information)
8. All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)
9. Travel itinerary for specific PNR
10. Travel agency/travel agent
11. Code share information
12. Split/divided information
13. Travel status of passenger (including confirmations and check-in status)
14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote
15. All baggage information
16. Seat information, including seat number
17. General remarks including OSI, SSI and SSR information
18. Any collected Advance Passenger Information System (APIS) information
19. All historical changes to the PNR listed in numbers 1 to 18

ANNEX II

Declaration by the EU on the Agreement on the use and transfer of Passenger Name Records to the United States Department of Homeland Security ("the Agreement"), in respect of its obligations under Articles 17 and 23 of the Agreement.

1. In the context of the joint review and evaluation mechanism set out in Article 23 of the Agreement, and without prejudice to other matters that may be raised through this mechanism, the European Union will seek information from the US on the exchange of information where appropriate, regarding the transfers of European Union citizens' and residents' PNR data to the authorities of third countries as laid down in Article 17 of the Agreement;

2. In the context of the consultation and review mechanism set out in Article 23 of the Agreement, the EU will request from the US all appropriate information on the implementation of the conditions governing those transfers in accordance with the provisions of Article 17;

3. The EU, in the context of the consultation and review mechanism set out in Article 23 of the Agreement, will pay particular attention to the respect of all the safeguards for the implementation of the provisions of Article 17(2), so as to be satisfied that third countries receiving such data have agreed to afford to the data the privacy protections comparable to those provided to PNR by DHS under the Agreement.