EU/USA Agreement: use and transfer of passenger name records (PNR) to the US Department of Homeland Security

2011/0382(NLE) - 26/04/2012 - Final act

PURPOSE: to conclude 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.

NON-LEGISLATIVE ACT: Council Decision 2012/472/EU on the conclusion 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.

BACKGROUND: 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 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.

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. 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 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**. (please refer to RSP/2010/2657). Pending such renegotiation, the 2007 Agreement would remain provisionally applicable.

On 2 December 2010, the Council adopted a decision authorising the Commission to open negotiations between the Union and the United States of America on the transfer and use of passenger name records (PNR) to prevent and combat terrorism and other serious transnational crime. In accordance with Council Decision 2012/471/EU, the Agreement was signed on 14 December 2011, subject to its conclusion.

It is now appropriate to conclude the Agreement.

This Agreement replaces the previous one that has been provisionally applied since 2007.

CONTENT: this Decision concludes 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 main points of the Agreement are as follows:

Purpose: the purpose of the Agreement is to ensure security and to protect the life and safety of the public.

PNR data: this is the information provided by passengers and collected by air carriers during the reservation and check-in procedures. It includes information such as name, dates of travel and travel itinerary, ticket information, address and phone numbers, means of payment used, credit card number, travel agent, seat number and baggage information.

Scope: the Agreement shall apply to carriers operating passenger flights between the European Union and the United States, and also apply to carriers incorporated or storing data in the EU and operating passenger flights to or from the United States.

Use of PNR data: the US collects, uses and processes PNR for the purposes of preventing, detecting, investigating, and prosecuting terrorist offences and related crimes, and serious crimes that are transnational in nature, as defined in the text. In its implementation, the agreement shall be strictly limited to the use of PNR data for the prevention and detection of terroriost offences or transnational crime.

Sensitive data: 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. 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 imperilled or seriously impaired.

Sensitive data shall be **permanently deleted not later than 30 days** from the last receipt of PNR containing such data by DHS, except under specified circumstances.

Guarantees: in accordance with the agreement, provisions are made for the following guarantees for individuals:

- **Correction or rectification for individuals**: 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.

- **Redress for individuals**: 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 the Agreement may seek effective administrative and judicial redress in accordance with US law.

Data retention: DHS retains PNR in an **active database for up to five years**. After the initial **six months of this period, PNR shall be depersonalised and masked**. Access to this active database shall be restricted to a limited number of specifically authorised officials.

After this active period, PNR shall be transferred to a **dormant database for a period of up to ten years,** where PNR shall not be repersonalised except in connection with law enforcement operations and then only in connection with an identifiable case, threat or risk. As regards serious transnational crime, PNR in this dormant database may only be repersonalised for a period of up to five years.

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

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.

The Parties agree that the necessity of a 10-year dormant period of retention will be considered when the Agreement is evaluated.

EU access to data: DHS shall provide to competent police, or other authorities of the EU 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 EU terrorist offences and related crimes or transnational crime as described in the text.

Furthermore, a police or judicial authority of an EU Member State, 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 terrorist offences and related crimes or transnational crime as described.

Monitoring compliance: 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.

Respect for fundamental rights: the 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, the right to the protection of personal data, and the right to effective remedy and fair trial recognised by the Charter.

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

Review and evaluation: the Parties shall jointly review the implementation of the Agreement one year after its entry into force and regularly thereafter as jointly agreed, and they will jointly evaluate the Agreement four years after its entry into force.

Following the joint review, the European Commission shall present a report to the European Parliament and the Council, and the US shall be given an opportunity to provide written comments which shall be attached to the report.

Duration: the Agreement shall remain in force for a period of seven years from the date of its entry into force, and may be renewed for a further period of seven years.

Territorial provisions: the United Kingdom and Ireland are taking part in the adoption of the Decision, but Denmark is not taking part in the adoption of this Decision and is not bound by the Agreement or subject to its application.

ENTRY INTO FORCE: the Decision enters into force on 12 August 2012. The Agreement enters into force the first day of the month following the date on which the parties have notified that they have completed the necessary internal procedures.