



XXXX/07/EN  
WP132

### ANNEX 1

#### *Short notice for travel between the European Union and the United States*

Under US Law and in accordance with an International Agreement between the European Union and the United States, the US Department of Homeland Security (DHS) will receive certain travel and reservation data (PNR) about passengers flying between the European Union and the United States.

DHS has undertaken that it uses this information primarily for the purposes of preventing and combating terrorism and other transnational serious crimes. These and other data may also be used for checking against lists of passengers raising aviation security concerns.

The PNR information will be retained for at least three years and six months and may be shared with other authorities.

Further information about these arrangements, including measures to safeguard your personal data can be obtained from your airline or travel agent. *[the airline or travel agent may then provide the information contained in the long version]*

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate E (Services, Intellectual and Industrial Property, Media and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.

Website: [www.europa.eu.int/comm/privacy](http://www.europa.eu.int/comm/privacy)

## ANNEX 2

### **Frequently asked questions regarding the transfer of passenger information to US authorities related to flights between the European Union and the United States**

#### ***1. What sort of passenger information will be transferred to US authorities?***

United States law requires airlines operating flights to, from, or through the United States (US) to provide the US Department of Homeland Security (DHS) with certain passenger data to facilitate safe travel and to secure US security. The passenger data falls into two categories.

- Passenger Name Record (PNR) : This includes a variety of information provided during the booking process or held by airlines or travel agents, such as the passenger's name, contact details, details of the travel itinerary (such as date of travel, origin and destination, seat number, and number of bags) and details of the reservation (such as travel agency and payment information) or other information (such as affiliation with a frequent flier program);
- Advanced Passenger Information (API): this includes mainly information contained on a passenger's passport and is often collected at check-in. This information is provided prior to arrival to frontier control authorities. This is also used to screen passengers against lists of persons believed to pose a threat to aviation security.

These FAQs relate primarily to PNR data as this is regulated in accordance with the International Agreement signed on 16 October 2006 between the European Union and the United States. The European Union will make sure that air carriers comply with these obligations. [Name of the Airline] airline has to comply with these requirements.

For a more detailed explanation of the way DHS handles PNR collected from flights between the European Union (EU) and the US, please refer to the Undertakings of the Department of Homeland Security, Customs and Border Protection ("PNR Undertakings") published in the US Federal Register, Volume 64, No 131, p.41543. You can also access them as an Annex to Commission Decision 2004/535/EC, available [click here](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_235/l_23520040706en00110022.pdf). [hyperlink to page: [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l\\_235/l\\_23520040706en00110022.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_235/l_23520040706en00110022.pdf)] [link to be edited to the different linguistic versions of the OJ as this notice gets translated]

#### ***2. Why is my Passenger Name Record being transferred to US DHS before I travel to, from, or through the United States?***

The main purpose of collecting PNR information in advance of flights is to facilitate safe travel between the EU and the US and to safeguard US security. DHS uses Passenger Name Record (PNR) data from flights between the EU and the US for the purposes of preventing and combating:

- terrorism and related crimes;
- other serious crimes, including organised crime, that are transnational in nature; and
- flight from warrants or custody for crimes described above.

DHS can obtain most of the information contained in PNR data when they examine an individual's airline ticket and other travel documents as part of its normal border control functions. The ability to receive this PNR data electronically in advance of passengers' arrival at or departure from ports of entry in the US significantly enhances DHS's ability to carry out efficient and effective advance risk assessment of passengers.

### ***3. What is the legal framework for the transfer of PNR data?***

By legal statute (title 49, United States Code, section 44909(c)(3)) and its implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), each air carrier operating passenger flights in foreign air transportation to or from the US must provide DHS with electronic access to PNR data collected and contained in the air carrier's reservation and/or departure control systems.

DHS has published Undertakings to use these data in accordance with certain conditions which concern, in particular:

- the purpose of the processing;
- the data used;
- the method of accessing the data;
- the maximum storage time;
- the security measures used;
- the disclosure of the data to other parties; and
- how you can access your data and make a complaint.

Based on DHS implementing the Undertakings, the European Union and the United States concluded an International Agreement signed on 16 October 2006, and the European Union will now make sure that air carriers provide DHS with PNR data.

The competent authorities in EU Member States, in particular national Data Protection Authorities, may use their existing powers to suspend data flows to DHS to protect individuals with regard to the processing of their personal data in cases where DHS breaches the applicable standards of protection as set out in the Undertakings.

### ***4. Is sensitive data included in the PNR data transfer?***

Certain PNR data identified as "sensitive" may be included in the PNR when it is transferred from reservation and/or air carrier departure systems in the EU to DHS. Such "sensitive" PNR data would include certain information revealing the passenger's racial or ethnic origin, political opinion, religion, health status or sexual preference. DHS has undertaken that it will not use any "sensitive" PNR data that it receives from air carrier reservation systems or departure control systems in the EU. DHS has put in place an automated filtering program so that "sensitive" PNR data is not used.

**5. Will my PNR data be shared with other authorities?**

PNR data received in connection with flights between the EU and the US may be shared with other domestic and foreign government authorities that have counter-terrorism or law enforcement functions, on a case-by-case basis and under specific data protection guarantees, for purposes of preventing and combating terrorism and other serious criminal offences; other serious crimes, including organised crime, that are transnational in nature; and flight from warrants or custody for the crimes described above.

PNR data may also be provided to other relevant government authorities, when necessary, to protect the vital interests of that passenger or of other persons, in particular as regards to significant health risks, or as otherwise required by law.

**6. How long will DHS store my PNR data?**

PNR data from flights between the EU and the US will be kept by DHS for a period of three years and six months, unless DHS manually consults that particular PNR data. In such cases, PNR data will be kept by DHS for an additional eight years. Additionally, information that is linked to a specific enforcement record will be maintained by DHS until the enforcement record is archived.

**7. How will my PNR data be secured?**

DHS will keep PNR data from flights between the EU and the US secure and confidential. Careful safeguards, including appropriate data security and access controls, will make sure that the PNR data is not used or accessed improperly.

**8. Who will make sure that the PNR Undertakings are complied with?**

The Department of Homeland Security Chief Privacy Officer is statutorily obliged to make sure that all parts of that Department handle personal information in a manner that complies with relevant law. He is independent of any directorate within DHS and his findings are binding on the Department. He will exercise oversight over the program to ensure strict compliance by DHS and to verify that proper safeguards are in place.

**9. Can I request a copy of my PNR data that is collected by DHS?**

Any passenger may request more information about the types of PNR shared with DHS and may ask for a copy of that passenger's PNR data contained in DHS databases.

As permitted by the Freedom of Information Act and other US laws, regulations, and policies, DHS will consider a request for documents by a passenger regardless of their nationality or country of residence, including PNR documents in its possession. DHS may deny or postpone disclosure of all or part of a PNR in certain circumstances (e.g., if it could be reasonably expected to interfere with pending enforcement proceedings or would disclose techniques and procedures used in law enforcement investigation).

In cases where DHS denies access to PNR data under an exemption of the Freedom of Information Act, you can administratively appeal this decision to the Chief Privacy Officer of DHS, who is responsible for both privacy protection and disclosure policy for DHS. A final agency decision may be judicially challenged under US law.

### ***10. Can I request that corrections be made to my PNR?***

Yes. Passengers may seek to correct their PNR data that is contained in DHS databases by contacting the offices indicated below in FAQ 12. DHS will note corrections that it determines are justified and properly supported.

### ***11. Who do I contact in the US regarding this program?***

*General inquiries about PNR data or inquiries about my PNR data*

If you wish to make an inquiry about PNR data shared with DHS or seek access to PNR data held by DHS about you, please write to: Freedom of Information Act (FOIA) Request, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229. For further information regarding the procedures for making such a request, you may refer to section 19 Code of Federal Regulations, section 103.5 ([www.dhs.gov/foia](http://www.dhs.gov/foia)).

*Concerns, complaints, and correction requests*

If you wish to file a concern, complaint, or request for correction regarding PNR data, please write to: Assistant Commissioner, DHS Office of Field Operations, US Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229.

Decisions by DHS may be reviewed by the Chief Privacy Officer of the Department of Homeland Security, Washington, DC 20528. An inquiry, complaint or request for correction of PNR data may also be referred by a passenger to the Data Protection Authority (DPA) within their EU Member State for further consideration if appropriate.

### ***12. Who do I contact if my complaint is not resolved?***

If your complaint cannot be resolved by DHS, the complaint may be directed, in writing to the Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528. The Chief Privacy Officer will review the situation and try to resolve the complaint. You can make a complaint via the DPA in your country. For contact details of the DPA in your country, please [click here](#). [Link to Europa web page with DPA addresses: [http://ec.europa.eu/justice\\_home/fsj/privacy/nationalcomm/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm)]

The Chief Privacy Officer has committed to deal with complaints received from the Data Protection Authorities of European Union Member States on behalf of an EU resident, when that resident has authorised the DPA to act on their.

### ***13. How can I get more information?***

You can get more information about how your airline handles your personal data by contacting your airline in your country.

For [Airline], the contact details are as follows:

[...]