

Frequently Asked Questions Regarding Customs and Border Protection Receipt of Passenger Name Records Related to Flights between the European Union and the United States

United States law requires airlines operating flights to or from the United States (U.S.) to provide the Department of Homeland Security, Customs and Border Protection (CBP), with certain passenger data to facilitate safe and efficient travel. The European Commission has determined that U.S. laws, in conjunction with CBP policies regarding the protection of personal data and the U.S.-EU Passenger Name Record Agreement signed on May 17, 2004, are adequate to permit transfers of PNR data to the U.S. For more information see http://europa.eu.int/comm/internal_market/privacy/index_en.htm. For a comprehensive explanation of the manner in which CBP handles PNR collected from flights between the European Union (EU) and the U.S., please refer to the Undertakings of the Department of Homeland Security, Customs and Border Protection ("PNR Undertakings") http://www.dhs.gov/interweb/assetlibrary/CBP-DHS_PNRUndertakings5-25-04.pdf.

1. Why is my Passenger Name Record being transferred to U.S. Customs and Border Protection prior to travelling to, from, or through the United States?

The overriding purpose of collecting PNR information in advance of flights is to facilitate secure and efficient travel between the U.S. and the EU. CBP uses Passenger Name Record (PNR) data from flights between the U.S. and the EU strictly for the purposes of preventing and combating:

- a. Terrorism and related crimes;
- b. Other serious crimes, including organized crime, that are transnational in nature; and
- c. Flight from warrants or custody for crimes described above.

Use of PNR data allows CBP to facilitate *bona fide* travel and to conduct efficient and effective advance risk assessment of passengers.

Most information contained in PNR data can be obtained at the port of entry by CBP upon examining an individual's airline ticket and other travel documents pursuant to its normal border search authority. The ability to receive this PNR data electronically in advance of passengers' arrival at or departure from ports of entry in the U.S. significantly enhances CBP's ability to facilitate *bona fide* travel and to conduct efficient and effective advance risk assessment of passengers.

2. What U.S. and EU laws allow 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 U.S. must provide CBP with electronic access to PNR data to the extent it is collected and contained in the air carrier's reservation and/or departure control systems.

In order to permit transfers of PNR data to the U.S., the European Commission has determined that U.S. laws, in conjunction with CBP policies regarding the protection of personal data, are adequate. An U.S.-EU Passenger Name Record Agreement reflecting this was signed on May 17, 2004.

3. What type of information will CBP receive about me through PNR?

CBP will receive certain PNR data concerning persons traveling on flights to, from or through the U.S. Airlines create PNR data in the reservation systems for each itinerary booked for a passenger. Such PNR data may also be contained in the air carrier departure control systems.

The PNR data contain a variety of information provided routinely by a customer, 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). The PNR may include other information voluntarily provided by a customer during the booking process (such as affiliation with a frequent flier program).

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 CBP. Such "sensitive" PNR data would include certain information revealing the passenger's racial or ethnic origin, political opinion, religion, health status or sexual preference. CBP will not use for any purpose certain "sensitive" PNR data that it receives from air carrier reservation systems or departure control systems in the EU. CBP will be installing a filtering program so that "sensitive" PNR data is deleted.

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

PNR data received in connection with flights between the U.S. and the EU may be shared with other domestic and foreign government authorities that have counter-terrorism or law enforcement functions, on a case-by-case basis, for purposes of preventing and combating terrorism and other serious criminal offenses; other serious crimes, including organized 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 the passenger who is the subject of the PNR data or of

other persons, in particular as regards to significant health risks, or as otherwise required by law.

6. Who will have access to my PNR data?

CBP will have access to PNR data in connection with flights between the U.S. and the EU. This PNR data may be transferred to other domestic and foreign government authorities with counter-terrorism or law enforcement functions, on a case-by-case basis, for purposes of preventing and combating terrorism and related crimes; other serious crimes, including organized 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 the passenger who is the subject of the PNR data or of other persons, in particular as regards to significant health risks, or as otherwise required by law.

7. How long will CBP store my PNR data?

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

8. How will my PNR data be secured?

CBP will keep PNR data from flights between the U.S. and the EU secure and confidential. Careful safeguards, including appropriate data security and access controls, will ensure that the PNR data is not used or accessed improperly.

9. Who will exercise oversight of compliance with the PNR Undertakings?

The Department of Homeland Security Chief Privacy Officer is statutorily obligated to ensure that personal information is handled in a manner that complies with relevant law. She is independent of any directorate within DHS and will exercise oversight over the program to ensure strict compliance by CBP and to verify that proper safeguards are in place.

10. May I request a copy of my PNR data that is collected by CBP?

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

As permitted by the Freedom of Information Act and other U.S. laws, regulations, and policies, CBP will consider a request by a passenger for documents, including PNR documents in its possession. CBP 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 for a law enforcement investigation).

In cases where CBP denies access to PNR data pursuant to an exemption under the Freedom of Information Act, such a determination can be administratively appealed 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 U.S. law.

11. Can I request that corrections be made to my PNR?

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

12. Whom do I contact in the U.S. 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 CBP or seek access to PNR data held by CBP about you, you may mail a request 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).

Concerns, Complaints, and Correction Requests

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

Decisions by CBP 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 as may be deemed appropriate.

13. Whom do I contact if my complaint is not resolved?

In the event that a complaint cannot be resolved by CBP, the complaint may be directed, in writing to the Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528. The Chief Privacy Officer shall review the situation and endeavor to resolve the complaint.

Complaints received from the European Union Member States on behalf of an EU resident, to the extent such resident has authorized the DPA to act on his or her behalf, shall be handled on an expedited basis.

14. What is the role of the Chief Privacy Officer of the Department of Homeland Security?

The DHS Chief Privacy Officer is statutorily obligated to ensure that personal information is handled in a manner that complies with relevant law. She is independent of any directorate within DHS. Her determination is binding on the Department.