Frequently asked questions about the transmission of passenger details to US authorities for flights between the European Union and the United States of America

1. Which passenger details are forwarded to the US authorities?

The United States require airlines operating flights to, from and via the United States (USA) to transmit certain passenger details to the US Department of Homeland Security (DHS) or the Transportation Security Administration (TSA). The purpose of transmitting such data is to ensure the safety of passenger flights and the internal security of the United States by allowing a risk assessment to be carried out prior to the arrival of passengers. The passenger details are subdivided into three groups.

> 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, and meal or wheelchair requests) 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;

> Secure Flight Passenger Data (SFPD): This includes the full name as shown on the official photo identification document, the date of birth, gender and redress number (if available: persons incorrectly identified can apply for a redress number at www.dhs.gov/trip to avoid incorrect identification in future). The secure flight information is collected after the booking has been made and is then forwarded to the TSA for checking against the watch lists.

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 international agreement and the accompanying letter of DHS, which are published in the Official Journal of the European Communities L 204 of 4 August 2007, available here:
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_235/l_23520040706en00110022.pdf

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

DHS uses passenger name records (PNR) for 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.

PNR may be used where necessary for the protection of the vital interests of an individual, or in any criminal judicial proceedings, or as otherwise required by law.

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 PNR data collected and contained in the air carrier's reservation and/or departure control systems.

DHS explained in a letter of 26 July 2007 how it handles the collection, use and storage of PNR.
(http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_235/l_23520040706en00110022.pdf)

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 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 and has put in place an automated filtering program so that sensitive PNR data is not used in principle.

However, sensitive PNR data may be used in exceptional cases, such as where the life of an individual could be imperilled or is in serious danger.

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

DHS may share PNR data with other US government authorities that have counter-terrorism, law enforcement or public security functions, for purposes of preventing and combating terrorism, transnational crime and public security (including threats, flights, individuals and routes of concern).

DHS may share PNR data with government authorities in third countries, but only after they have considered the intended use of the information and the ability to protect it. Unless it is an emergency, any exchanges of data require data protection measures to be

incorporated that are comparable to those set out in the international agreement between the EU and the US.

6. How long will DHS store my PNR data?

DHS will keep PNR data for fifteen years. Information related to a specific case or investigation can be kept longer until the case or investigation is archived.

DHS will keep a log of access to any sensitive PNR data and will delete the data within 30 days once the purpose for which it has been accessed is accomplished, and it is not required by law to keep it for longer. DHS will provide notice, normally within 48 hours, to the European Commission (DG JLS) that sensitive data has been accessed.

7. *Can I request a copy of my PNR data that is collected by DHS, and can I request that corrections be made to my PNR?*

Any passenger, regardless of their nationality or country of residence, may request information about their PNR and have inaccuracies corrected.

You can find information on DHS policies an access to records and personal information at http://www.dhs.gov/xfoia/editorial_0579.shtm.

DHS policies on redress can be found at www.dhs.gov/trip.