11733/04/EN
WP 97

Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America

Adopted on 30th September 2004

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof,

has adopted the present Opinion:

In its Decision of 14 May 2004[2], the Commission considered the United States' Bureau of Customs and Border Protection (CBP) to ensure an adequate level of protection for PNR data transferred from the Community concerning flights to or from the United States.

This Decision concerns the adequacy of protection provided by CBP with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC. It does not affect other conditions or restrictions implementing other provisions of that Directive that pertain to the processing of personal data within the Member States. One of them is the obligation by data controllers to inform data subjects about the main elements of the data processing. Therefore, data controllers carrying out processing of PNR data subject to national laws of EU Member States adopted pursuant to Directive 95/46/EC are obliged to provide passengers with complete and accurate information on the transfer of PNR data to CBP, in accordance with those national laws adopted pursuant to Articles 10 and 11 of the Directive.

The Working Party has adopted the information notices included as Annex 1 and 2 to the present Opinion. They should serve as guidance as regards the information that should be provided to passengers on transatlantic flights, and should be used as broadly as possible by air carriers, travel agents and Computer Reservation Systems taking part in the booking process.

Done at Brussels, on 30th September 2004

For the Working Party

The Chairman

Peter Schaar

---

1 Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (C(2004) 1914), OJ L 235, 6.7.2004, p. 11

ANNEX 1

Short Notice for Travel between the European Union and the United States

Under U.S. Law, U.S. Customs and Border Protection (CBP) will receive certain travel and reservation information, known as Passenger Name Record or PNR data, about passengers flying between the European Union and the U.S.
CBP has undertaken that it uses this PNR data for the purposes of preventing and combating terrorism and other transnational serious crimes. The PNR may include information provided during the booking process or held by airlines or travel agents.

The 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 or link directly to the CBP's web site]*

ANNEX 2

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 Customs and Border Protection (CBP), part of the U.S. Department of Homeland Security, with certain passenger data to facilitate safe travel and to secure U.S. security.

XXX-airline has to comply with these requirements

The European Commission has determined that CBP provides an adequate level of protection so permitting transfers of PNR data to the U.S. For more information see: http://www.europa.eu.int/comm/internal_market/privacy/adequacy_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 safe travel between the EU and the U.S. and to safeguard U.S. security. CBP uses Passenger Name Record (PNR) data from flights between the EU and the U.S. 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.

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 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 U.S. significantly enhances CBP's ability to conduct efficient and effective advance risk assessment of passengers.

2. 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 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.

The European Commission has determined that CBP is considered as providing an adequate level of protection to the data transferred. These transfers are covered by an International Agreement between the European Community and the U.S.

The Commission decision was based on the Undertakings of CBP and its commitment to comply with them. Non-compliance could be challenged appropriately and, if persistent, would lead to the suspension of the effects of that decision.

The competent authorities in EU Member States may exercise their existing powers to suspend data flows to CBP in order to protect individuals with regard to the processing of their personal data in cases of breach by CBP of the applicable standards of protection as prescribed by the Commission decision.

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

CBP will receive certain PNR data concerning persons travelling 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 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).

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 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. CBP will be installing an automated 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 EU and the U.S. 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 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 that passenger or of other persons, in particular as regards to significant health risks, or as otherwise required by law.

6. How long will CBP store my PNR data?

PNR data from flights between the EU and the U.S. will be kept by CBP for a period of three years and six months, unless CBP manually consults that particular 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.

7. How will my PNR data be secured?

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

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

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

9. ***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 regardless of his nationality or country of residence 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 used in 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.

10. 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.

11. 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.

12. 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 endeavour to resolve the complaint.

The Chief Privacy Officer has committed to handle complaints received from the Data Protection Authorities of 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, on an expedited basis.

13. How can I get more information?

You can obtain more information about transfers of PNR data to the U.S. by contacting the Data Protection Supervisory Authority in your country.

For [NAME OF EU Member State], the contact details are as follows:

[Contact details for the DPA in each EU Member State]