

**EUROPEAN COMMISSION/US CUSTOMS TALKS ON PNR TRANSMISSION
BRUSSELS, 17/18 FEBRUARY
JOINT STATEMENT**

1. Senior officials of the European Commission and the US Administration, led by Director General for External Relations Guy Legras and Deputy US Customs Commissioner Douglas Browning, met in Brussels on 17/18 February 2003 to find a solution to the problems resulting for airlines operating flights to or from the US due to the new Passenger Name Record (PNR) transmission requirements contained in the Aviation and Transportation Security Act 2001. It was necessary in particular to reconcile US requirements with the requirements of data protection law in the EU.

2. The Commission side emphasised its full solidarity with the US objective of preventing and combating terrorism and underlined the need for practicable solutions that would provide legal certainty for all concerned. The two sides agreed to take all necessary steps as quickly as possible to reconcile and respect fully legal obligations on both sides leading towards mutually satisfactory solution, providing legal certainty (see paragraph 6).

3. Compliance by airlines and reservation systems with US PNR requirements as from 5 March 2003 will not involve unlimited on-line access by US Customs to EU-based data bases, but rather the processing of PNR data for persons whose current travel itinerary includes flights into, out of, or through the US. As a result, US Customs will facilitate legitimate travel to, from or through the US.

4. Pending a Commission decision under Article 25.6 of the Data Protection Directive and in view of the good faith effort of US Customs to provide the necessary information and undertakings (including those reflected in the annex) which would allow the Commission to take such a decision, the European Commission will keep under review the enforcement of Article 11 of the Computer Reservation Systems (CRS) Regulation. In view of the above process, the Commission side considered that EU data protection authorities may not find it necessary to take enforcement actions against airlines complying with the US requirements.

5. The Commission side noted the undertakings by US Customs with regard to the treatment of personal data (see annex). In addition, it is the understanding of both sides that:

- (a) In accessing the PNR data in the territory of the Community, US Customs undertakes to respect the principles of the Data Protection Directive.
- (b) In so far as data of a sensitive nature, as defined in Article 8 of the Data Protection Directive, are processed by airlines in their PNR records, in accordance with the applicable EU law, measures to protect these data will need to be jointly developed, after consultation with the airline industry, preferably before 5 March 2003.
- (c) As concerns a first party request for disclosure of data by the data subject, US Customs will proceed with disclosure under the Freedom of Information Act (FOIA).
- (d) US Customs and the European Commission will consult with each other on a regular basis concerning implementation of this statement and possible enhancements which may be applied, consistent with US law and practice. Such discussions would include

the results of any audits or other findings regarding in particular personnel access to information in US Customs databases.

(e) US Customs may provide information to other US law enforcement authorities only for purposes of preventing and combating terrorism and other serious criminal offences, who specifically request PNR information from US Customs.

6. The two sides agreed to work together towards a bilateral arrangement under which the Commission, in response to information and undertakings provided by the US side about the way transferred data would be handled and protected in the US, will adopt a decision under Article 25 paragraph 6 of the Data Protection Directive. The information and undertakings would reflect existing law and practice, coupled if necessary with additional undertakings especially as regards the necessity and proportionality of data processing. Such a decision will provide legal certainty in particular as regards the international transfer aspects of the transmission of PNR data. It was agreed that the information and undertakings to be provided would need to cover in particular: definition of the purposes for which the data will be used and limitation of use to these purposes; conditions and limits of data sharing and onward transfer; protection of data from unauthorised access; duration and conditions of data storage; additional measures for the protection of sensitive data; remedies for passengers, including possibilities to review and correct data held by US Customs; reciprocity.

7. For this purpose both sides will engage in an intensive dialogue to reach a mutually satisfactory solution without delay. The next discussions will take place before the end of February 2003. The two sides will report to the EU-US Summit on 25 June 2003.

8. The US side took note of the Commission side's view that a multilateral agreement was necessary in the longer run, the Commission believing it to be entirely impractical for all airlines collecting and processing data in the EU to have to operate under multiple unilaterally imposed or bilaterally agreed requirements. In the Commission's view, the best framework for such an agreement would be ICAO.

ANNEX

The United States Customs Service represents that:

- 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), air carriers operating passenger flights in foreign air transportation to, from or through the United States, must provide Customs with electronic access to PNR data contained in the automated reservation/ departure control systems ("reservation systems");
- most data elements contained in PNR data can be obtained by Customs upon examining a data subject's airline ticket and other travel documents pursuant to its normal border control authority, but that such examinations would result in significant delays in the processing of flights to and from the U.S.;
- PNR data is used by Customs strictly for enforcement purposes, including use in threat analysis to identify and interdict potential terrorists and other threats to national and public security, and to focus Customs resources on high risk concerns, thereby facilitating and safeguarding *bona fide* traveller;
- with regard to the PNR data which Customs accesses directly from the air carrier's reservation systems, Customs will only view PNR data concerning persons whose travel includes a flight into, out of or through the United States;
- Customs will access air carrier reservation systems as an accommodation to the air carriers to obviate the need for costly technical changes required to allow the air carriers to transmit the data to Customs;
- Customs treats PNR information regarding persons of any origin as law enforcement sensitive, confidential personal information of the data subject, and confidential commercial information of the air carrier;
- disclosure of PNR data is generally governed by the Freedom of Information Act (FOIA) (title 5, United States Code, section 552) which permits public access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from public disclosure by an applicable exemption under the FOIA;
- among its exemptions, the FOIA permits an agency to withhold a record (or a portion thereof) from disclosure where the information is confidential commercial information, where disclosure of the information would constitute a clearly unwarranted invasion of personal privacy, or where the information is compiled for law enforcement purposes, to the extent disclosure may reasonably be expected to constitute an unwarranted invasion of personal privacy (title 5, United States Code, sections 552(b)(4), (6), (7)(C));
- Customs regulations (title 19, Code of Federal Regulations, section 103.12), which govern the processing of requests for information pursuant to the FOIA, specifically provide that the disclosure requirements of the FOIA are not applicable to Customs records relating to (1) confidential commercial information, (2) material involving personal privacy where the disclosure would constitute a clearly unwarranted invasion of personal privacy; and (3) information compiled for law enforcement purposes, where disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy;

- Customs would take the position in connection with any administrative or judicial proceeding arising out of a FOIA request for PNR information, that such records are exempt from disclosure under the FOIA;
- authorized Customs personnel obtain access to PNR through the closed Customs intranet system which is encrypted end-to-end and the connection is controlled by Customs Data Center;
- PNR data is accessed by Customs pursuant to its statutory authority (49 U.S.C. 44909) and stored in Customs databases, access to which is controlled by Customs;
- PNR data stored in a Customs database is limited to "read only" access by authorized personnel, meaning that the substance of the data may be programmatically reformatted, but will not be substantively altered in any manner by Customs once accessed from an air carrier's reservation system;
- details regarding personnel access to information in Customs databases is recorded and routinely audited by Customs Office of Internal Affairs to prevent unauthorized use of the system;
- only certain Customs employees who have completed a background investigation, have an active, password-protected account in the Customs computer system, and have a recognized official purpose for reviewing PNR data may access PNR data through Customs electronic connection to an air carrier's reservation system;
- Customs employees are required to complete security and data privacy training, including passage of a test, on a biennial basis;
- Customs policy and regulations provide for stringent disciplinary action (which may include termination of employment) to be taken against any Customs employee who discloses information from Customs computerized systems without official authorization (title 19, Code of Federal Regulations, section 103.34);
- criminal penalties (including fines and imprisonment of up to one year) may be assessed against any officer or employee of the United States for disclosing confidential business information obtained in the course of his employment, where such disclosure is not authorized by law (title 18, United States Code, section 1905);
- no other foreign, federal, state or local agency has access to PNR through Customs databases;
- other law enforcement entities may specifically request PNR information from Customs and Customs, in its discretion, may provide such information for national security or in furtherance of other legitimate law enforcement purposes;
- for purposes of regulating the dissemination of PNR data which may be shared with other law enforcement entities, Customs is considered the "owner" of the data and such entities are obligated by the terms of disclosure to obtain Customs express authorization for any further dissemination (sometimes referred to as the "Third Agency Rule");

- PNR data subjects (or their authorized representative) may, either through the air carrier or directly, contact Customs, Office of Field Operations, to seek amendment of any data which Customs has stored in its databases that the data subject believes is inaccurate and Customs may, in its discretion and if properly supported, create a record of such amendment.
- Customs stores PNR data accessed from air carrier reservation systems on a Sun Unix server, running Oracle 8i, located in Newington, Virginia;
- Customs will retain the data no longer than is required for the purpose for which it was stored, after which such data will be transferred to a “deleted record file” in the form of raw data, available only to authorized personnel in the Office of Internal Affairs and personnel responsible for maintaining the database in the Office of Information Technology, on a “need to know basis”.