Personal data protection

1990/0287(COD) - 14/05/2004 - Implementing legislative act

PURPOSE : to establish the level of protection for PNR data transferred from the Community concerning flights to or from the United States, pursuant to Directive 95/46/EC.

LEGISLATIVE ACT : Commission Decision 2004/535/CE 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

CONTENT : Pursuant to Directive 95/46/EC, Member States are required to provide that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection and if the Member States' laws implementing other provisions of the Directive are complied with prior to the transfer.

In the framework of air transport, the 'Passenger Name Record' (PNR) is a record of each passenger's travel requirements which contains all information necessary to enable reservations to be processed and controlled by the booking and participating airlines.

It should be noted that the Council has adopted Decision 2004/496/EC on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection. (Please refer to CNS/2004/0064.) This Decision was adopted in the context of the fight against terrorism.

The United States Bureau of Customs and Border Protection (CBP) of the Department of Homeland Security (DHS) requires each carrier, operating passenger flights in foreign air transportation to or from the United States, to provide it with electronic access to PNR to the extent that PNR is collected and contained in the air carrier's automated reservation system.

This Decision provides that for the purposes of Article 25(2) of Directive 95/46/EC, the United States' Bureau of Customs and Border Protection (CBP) is considered to ensure an adequate level of protection for PNR data transferred from the Community concerning flights to or from the United States, in accordance with the Undertakings set out in the Annex. The Decision aims to establish a framework of rules for data to be transferred.

The transfer of date by EU airlines will be governed by certain "Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection(CBP) **.** The standards by which CBP will process passengers' PNR data on the basis of United States legislation and the Undertakings cover the basic principles necessary for an adequate level of protection for natural persons:

- As regards the purpose limitation principle, air passengers' personal data contained in the PNR transferred to CBP will be processed for a specific purpose and subsequently used or further communicated only in so far as this is not incompatible with the purpose of the transfer. In particular, PNR data will be used strictly for 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 those crimes.

- As regards the data quality and proportionality principle, which need to be considered in relation to the important public interest grounds for which PNR data are transferred, PNR data provided to CBP will not

subsequently be changed by it. A maximum of 34 PNR data categories will be transferred and the United States authorities will consult the Commission before adding any new requirements. Additional personal information sought as a direct result of PNR data will be obtained from sources outside the government only through lawful channels. As a general rule, PNR will be deleted after a maximum of three years and six months, with exceptions for data that have been accessed for specific investigations, or otherwise manually accessed.

-As regards the transparency principle, CBP will provide information to travellers as to the purpose of the transfer and processing, and the identity of the data controller in the third country, as well as other information.

-As regards the security principle, technical and organisational security measures are taken by CBP which are appropriate to the risks presented by the processing.

It should be noted that the rights of access and rectification are recognised, in that the data subject may request a copy of PNR data and rectification of inaccurate data.

Onward transfers will be made to other government authorities, including foreign government authorities, with counter-terrorism or law-enforcement functions, on a case-by-case basis, for purposes that correspond to those set out in the statement of purpose limitation. Transfers may also be made for the protection of the vital interests of the data subject or of other persons, in particular as regards significant health risks, or in any criminal judicial proceedings or as otherwise required by law. Receiving agencies are bound by the express terms of disclosure to use the data only for those purposes and may not transfer the data onwards without the agreement of CBP.

The competent authorities in 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 certain cases.

The Decision will expire three years and six months after the date of its notification, unless extended in accordance with the procedure set out in Article 31(2) of Directive 95/46/EC.

ENTRY INTO FORCE: Member States shall take all the measures necessary to comply with the Decision within four months of the date of its notification.