Draft

COMMISSION DECISION

of […]

on the adequate protection of personal data contained in the PNR of air passengers transferred to the United States' Bureau of Customs and Border Protection

(Text with EEA relevance)
(2004/…/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community,

having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1], and in particular Article 25(6) thereof,

Whereas:

(1) 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.

(2) The Commission may find that a third country ensures an adequate level of protection. In that case, personal data may be transferred from the Member States without additional guarantees being necessary.

(3) Pursuant to Directive 95/46/EC the level of data protection should be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations, and giving particular consideration to a number of elements relevant for the transfer and listed in Article 25(2) thereof.

(4) 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.

(5) The United States Bureau of Customs and Border Protection (U.S. CBP) requires each carrier operating passenger flights in foreign air transportation to or from the United

[1] OJ L 281, 23.11.1995, p. 31; Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p.1).

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.

(6) The requirements for personal data contained in the PNR of air passengers to be transferred to the U.S. CBP, are based on a statute adopted by the U.S. Congress in November 2001[2], and upon implementing regulations adopted by U.S. CBP under that Statute[3].

(7) The U.S. legislation in question concerns the enhancement of security and the conditions under which persons may enter and leave the country. These are matters on which the U.S. has the sovereign power to decide within its jurisdiction and the requirements laid down are moreover not inconsistent with any international commitments which the U.S. has undertaken. The U.S. is a democratic country, governed by the rule of law and with a strong civil liberties tradition. The legitimacy of its law-making process and strength and independence of its judiciary are not in question. Press freedom is a further strong guarantee against the abuse of civil liberties.

(8) The Community is fully committed to supporting the U.S. in the fight against terrorism. The Community should not interpret and apply its own rules in a way incompatible with this commitment or raise obstacles to U.S. measures to protect its own borders unless these are clearly dictated by law of the Community or the European Union. It should further be borne in mind that Article 13 of Directive 95/46/EC provides that Member States may legislate to restrict the scope of certain requirements of the Directive, where necessary for reasons of national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.

(9) The data transfers concerned involve specified airlines operating flights between the Community and the U.S. and only one recipient in the U.S., namely the Customs and Border Protection agency of the Department of Homeland Security.

(10) Any arrangement to provide a legal framework for PNR transfers to the U.S., in particular through this Decision should be time-limited. A period of three and a half years has been agreed. During this period, the context may change significantly and the Community and the U.S. agree that a review of the arrangements will be necessary.

(11) The processing by U.S. CBP of personal data contained in the PNR of air passengers transferred to it is governed by conditions set out in the Undertakings of XXX and in U.S. domestic legislation to the extent indicated in the Undertakings.

(12) As regards domestic law in the U.S., the Freedom of Information Act (FOIA) is relevant in the present context in so far as it controls the conditions under which U.S. CBP may resist requests for disclosure and thus keep PNR confidential and it governs the disclosure of PNR to the person whom it concerns, closely linked to the data subject's right of access. The FOIA applies without distinction to U.S. and non-U.S. citizens.

---

[2] Title 49, United States Code, section 44909(c)(3).
[3] Title 19, Code of Federal Regulations, section 122.49b.

(13) As regards the Undertakings, and as provided in paragraph 44 thereof, the content of paragraphs …. will be incorporated in Regulations in the US and thus have legal effect. The Undertakings will be published in full in the Federal Register and will also be promulgated under the personal authority of the Homeland Security Secretary. As such, they represent a serious and well-considered political commitment on the part of the U.S. Department of Homeland Security (DHS) and their compliance will be subject to Joint Review by the U.S. and the Community. Non-compliance could be challenged through legal, administrative and political channels and if persistent, would give rise to the suspension of the effects of this Decision.

(14) The standards by which the U.S. CBP will process passengers' PNR data on the basis of U.S. legislation and the Undertakings cover the basic principles necessary for an adequate level of protection for natural persons.

(15) As regards the purpose limitation principle, air passengers' personal data contained in the PNR transferred to the U.S. CBP will be processed for a specific purpose and subsequently used or further communicated only insofar 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 organized crime, that are trans-national in nature; and flight from warrants or custody for those crimes.

(16) As regards the data quality and proportionality principle, which needs to be considered in relation to the important public interest grounds for which PNR data are transferred, PNR data provided to U.S. CBP will not subsequently be changed by it. A maximum of 34 PNR data categories will be transferred and the U.S. authorities will consult the Commission before adding any new requirements. Data derived from PNR items may only be accessed by U.S. CBP subject to the usual U.S. judicial and procedural safeguards. As a general rule, PNR will be deleted after a maximum of 3 years and 6 months, with exceptions for data that have been accessed for specific investigations, or otherwise manually accessed.

(17) As regards the transparency principle, U.S. 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.

(18) As regards the security principle, technical and organisational security measures are taken by the U.S. CBP, which are appropriate to the risks presented by the processing.

(19) The rights of access and rectification are recognized, in so far as the data subject may request a copy of PNR data and rectification of inaccurate data. The exceptions foreseen are broadly comparable with the restrictions which may be imposed by Member States under Article 13 of Directive 95/46/EC.

(20) Onward transfers are limited to case by case transfers to other U.S. law enforcement agencies, on request, for purposes that correspond to those set out in the statement of purpose limitation, and those agencies may only use the data for the uses for which it was requested and may not transfer the data onwards without the agreement of U.S. CBP. No agencies other than U.S. CBP have direct electronic access to the data base in which PNR is stored. U.S. CBP will deny public disclosure of PNR on the basis of exemptions from the relevant provisions of FOIA.

(21) U.S. CBP does not use sensitive data in the sense of Article 8 of Directive 95/46/EC, and until a system of filters to exclude such data from PNR transferred to the U.S. is in place, undertakes to delete them.

(22) As regards the enforcement mechanisms to ensure compliance by U.S.-CBP with these principles, the training and information of U.S.-CBP staff is provided for, as well as sanctions with regard to individual staff members. U.S. CBP's respect for privacy in general will be under the scrutiny of the DHS's Chief Privacy Officer, who is an official of the DHS but has a large measure of organisational autonomy and must report annually to Congress. Persons whose PNR data has been transferred may address complaints to the DHS Chief Privacy Officer, directly or through Data Protection Authorities in Member States, which the DHS Chief Privacy Officer will address on an expedited basis. Compliance with the Undertakings will be the subject of annual joint review to be conducted by U.S.-CBP and a Commission-led team.

(23) In the interest of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify the exceptional circumstances in which the suspension of specific data flows may be justified, notwithstanding the finding of adequate protection.

(24) The Working Party on Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of Directive 95/46/EC has delivered opinions on the level of protection provided by the U.S. authorities for Passengers' data, which have been taken into account in the preparation of this Decision[4].

(25) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 31(1) of Directive 95/46/EC,

HAS ADOPTED THIS DECISION:

Article 1

For the purposes of Article 25(2) of Directive 95/46/EC, the United States' Bureau of Customs and Border Protection (U.S. CBP) is considered as providing an adequate level of protection for PNR data transferred from the Community concerning flights to or from the U.S., in accordance with the Undertakings set out in Annex I .

Article 2

This Decision concerns the adequacy of protection provided in the U.S. CBP with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and shall not affect other

---

[4] Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, adopted by the Working Party on 24 October 2002, available at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp66_en.pdf;
Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, adopted by the Working Party on 13 June 2003, available at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf;
Opinion X/2004 on the adequate protection of personal data contained in the PNR of air passengers transferred to the United States' Bureau of Customs and Border Protection (US CBP), adopted by the Working Party on 29 January 2004, available at http///XXXXXXXXXXXXX.

conditions or restrictions implementing other provisions of that Directive that pertain to the processing of personal data within the Member States.

Article 3

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to the U.S. CBP in order to protect individuals with regard to the processing of their personal data in the following cases:

   (a) where a competent U.S. authority has determined that the U.S. CBP is in breach of the applicable standards of protection;

   (b) where there is a substantial likelihood that the standards of protection set out in Annex I are being infringed, there are reasonable grounds for believing that the U.S. CBP is not taking or will not take adequate and timely steps to settle the case at issue, the continuing transfer would create an imminent risk of grave harm to data subjects and the competent authorities in the Member State have made reasonable efforts in the circumstances to provide the U.S. CBP with notice and an opportunity to respond.

2. The suspension shall cease as soon as the standards of protection are assured and the competent authority of the Member States concerned is notified thereof.

Article 4

1. Member States shall inform the Commission without delay when measures are adopted pursuant to Article 3.

2. The Member States and the Commission shall inform each other of any changes in the standards of protection and of cases where the action of bodies responsible for ensuring compliance with the standards of protection by the U.S. CBP as set out in Annex I fails to secure such compliance.

3. If the information collected pursuant to Article 3 and pursuant to paragraphs 1 and 2 of this Article provides evidence that the basic principles necessary for an adequate level of protection for natural persons are no longer being complied with, or that any body responsible for ensuring compliance with the standards of protection by the U.S. CBP as set out in Annex I is not effectively fulfilling its role, the U.S. CBP shall be informed and, if necessary, the procedure referred to in Article 31(2) of Directive 95/46/EC shall apply with a view to repealing or suspending this Decision.

Article 5

The functioning of this Decision shall be monitored and any pertinent findings reported to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the finding in Article 1 of this Decision that protection of personal data contained in the PNR of air passengers transferred to the U.S. CBP is adequate within the meaning of Article 25 of Directive 95/46/EC.

Article 6

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

Article 7

This Decision shall expire 3 years and 6 months after the date of its notification.

Article 8

This Decision is addressed to the Member States.

Done at Brussels, at

For the Commission

Member of the Commission

ANNEX I

[text of the Undertakings]