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 (notified under document number C(2004) 1914) (Text with EEA relevance) (2004/535/EC)

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

(notified under document number C(2004) 1914)

(Text with EEA relevance)

(2004/535/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, particular consideration being given 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. For the purposes of this Decision, the terms 'passenger' and 'passengers' include crew members. 'Booking airline' means an airline with which the passenger made his original reservations or with which additional reservations were made after commencement of

the journey. 'Participating airlines' means any airline on which the booking airline has requested space, on one or more of its flights, to be held for a passenger.

(5) 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.

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

(7) The United States legislation in question concerns the enhancement of security and the conditions under which persons may enter and leave the country, matters on which the United States has the sovereign power to decide within its jurisdiction. The requirements laid down are not, moreover, inconsistent with any international commitments which the United States has undertaken. The United States 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 United States in the fight against terrorism within the limits imposed by Community law. Community law provides for striking the necessary balances between security concerns and privacy concerns. For example, Article 13 of Directive 95/46/EC provides that Member States may legislate to restrict the scope of certain requirements of that Directive, where it is necessary to do so for reasons of national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.

(9) The data transfers concerned involve specific controllers, namely airlines operating flights between the Community and the United States, and only one recipient in the United States, namely CBP.

(10) Any arrangement to provide a legal framework for PNR transfers to the United States, 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 United States agree that a review of the arrangements will be necessary.

(11) The processing by CBP of personal data contained in the PNR of air passengers transferred to it is governed by conditions set out in the Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP) of 11 May 2004 (hereinafter referred to as the Undertakings) and in United States domestic legislation to the extent indicated in the Undertakings.

(12) As regards domestic law in the United States, the Freedom of Information Act (FOIA) is relevant in the present context in so far as it controls the conditions under which CBP may resist requests for disclosure and thus keep PNR confidential. The Act governs the

disclosure of PNR to the person whom it concerns, closely linked to the data subject's right of access. It applies without distinction to United States and non-United States citizens.

(13) As regards the Undertakings, and as provided in paragraph 44 thereof, the statements in the Undertakings will be, or have already been, incorporated in statutes, regulations, directives or other policy instruments in the United States and will thus have varying degrees of legal effect. The Undertakings will be published in full in the Federal Register under the authority of the DHS. As such, they represent a serious and well considered political commitment on the part of the DHS and their compliance will be subject to joint review by the United States and the Community. Non-compliance could be challenged as appropriate through legal, administrative and political channels and, if persistent, would lead to the suspension of the effects of this Decision.

(14) 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.

(15) 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.

(16) 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.

(17) 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.

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

(19) 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. The exceptions provided for are broadly comparable with the restrictions which may be imposed by Member States under Article 13 of Directive 95/46/EC.

(20) 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. No other foreign, federal, State or local agency has direct electronic access to PNR data through CBP databases. CBP will refuse public disclosure of PNR, by virtue of exemptions from the relevant provisions of FOIA.

(21) CBP does not use sensitive data as referred to in Article 8 of Directive 95/46/EC, and, until a system of filters to exclude such data from PNR transferred to the United States is in place, undertakes to introduce the means to delete them and in the meantime not to use them.

(22) As regards the enforcement mechanisms to ensure compliance by CBP with these principles, the training and information of CBP staff is provided for, as well as sanctions with regard to individual staff members. 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 CBP, or if unresolved, to the DHS Chief Privacy Officer, directly or through data protection authorities in Member States. The DHS Privacy Office will address, on an expedited basis, complaints referred to it by data protection authorities in Member States on behalf of residents of the Community, if the resident believes his or her complaint has not been satisfactorily dealt with by CBP or the DHS Privacy Office. Compliance with the Undertakings will be the subject of annual joint review to be conducted by CBP, in conjunction with DHS, 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 United States authorities for passengers' data, which have guided the Commission throughout its negotiations with the DHS. The Commission has taken note of these opinions 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 (hereinafter referred to as 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.

Article 2

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 and shall not affect other 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 CBP in order to protect individuals with regard to the processing of their personal data in the following cases:

a where a competent United States authority has determined that CBP is in breach of the applicable standards of protection; or

b where there is a substantial likelihood that the standards of protection set out in the Annex are being infringed, there are reasonable grounds for believing that 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 CBP with notice and an opportunity to respond.

2 Suspension shall cease as soon as the standards of protection are assured and the competent authorities of the Member States concerned are 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 CBP as set out in the Annex 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 CBP as set out in the Annex is not effectively fulfilling its role, 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 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 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.

Article 8

This Decision is addressed to the Member States.

Done at Brussels, 14 May 2004.

For the Commission

Frederik BOLKESTEIN

Member of the Commission

ANNEX

UNDERTAKINGS OF THE DEPARTMENT OF HOMELAND SECURITY BUREAU OF CUSTOMS AND BORDER PROTECTION (CBP)

In support of the plan of the European Commission (Commission) to exercise the powers conferred on it by Article 25(6) of Directive 95/46/EC (the Directive) and to adopt a decision recognising the Department of Homeland Security Bureau of Customs and Border Protection (CBP) as providing adequate protection for the purposes of air carrier transfers of Passenger[(5)] Name Record (PNR) data which may fall within the scope of the Directive, CBP undertakes as follows:

Legal authority to obtain PNR

1. 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 United States, must provide CBP (formerly, the US Customs Service) with electronic access to PNR data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems (reservation systems).

Use of PNR data by CBP

2. Most data elements contained in PNR data can be obtained by CBP upon examining a data subject's airline ticket and other travel documents pursuant to its normal border control authority, but the ability to receive this data electronically will significantly enhance CBP's ability to facilitate bona fide travel and conduct efficient and effective advance risk assessment of passengers.

3. PNR data are used by CBP strictly for purposes of preventing and combating: 1. terrorism and related crimes; 2. other serious crimes, including organised crime, that are transnational in nature; and 3. flight from warrants or custody for the crimes described above. Use of PNR data for these purposes permits CBP to focus its resources on high-risk concerns, thereby facilitating and safeguarding bona fide travel.

Data requirements

4. Data elements which CBP require are listed herein at Attachment A. (Such identified elements are hereinafter referred to as 'PNR' for purposes of these Undertakings.) Although CBP requires access to each of those 34 (thirty-four) data elements listed in Attachment A, CBP believes that it will be rare that an individual PNR will include a full set of the identified data. In those instances where the PNR does not include a full set of the identified data, CBP will not seek direct access from the air carrier's reservation system to other PNR data which are not listed on Attachment A.

5. With respect to the data elements identified as 'OSI' and 'SSI/SSR' (commonly referred to as general remarks and open fields), CBP's automated system will search those fields for any of the other data elements identified in Attachment A. CBP personnel will not be authorised to manually review the full OSI and SSI/SSR fields unless the individual that is the subject of a PNR has been identified by CBP as high-risk in relation to any of the purposes identified in paragraph 3 hereof.

6. Additional personal information sought as a direct result of PNR data will be obtained from sources outside the government only through lawful channels, including through the use of mutual legal assistance channels where appropriate, and only for the purposes set forth in paragraph 3 hereof. For example, if a credit card number is listed in a PNR, transaction information linked to that account may be sought, pursuant

to lawful process, such as a subpoena issued by a grand jury or a court order, or as otherwise authorised by law. In addition, access to records related to e-mail accounts derived from a PNR will follow US statutory requirements for subpoenas, court orders, warrants, and other processes as authorised by law, depending on the type of information being sought.

7. CBP will consult with the European Commission regarding revision of the required PNR data elements (Attachment A), prior to effecting any such revision, if CBP becomes aware of additional PNR fields that airlines may add to their systems which would significantly enhance CBP's ability to conduct passenger risk assessments or if circumstances indicate that a previously non-required PNR field will be needed to fulfil the limited purposes referred to in paragraph 3 of these Undertakings.

8. CBP may transfer PNRs on a bulk basis to the Transportation Security Administration (TSA) for purposes of TSA's testing of its Computer Assisted Passenger Pre-screening System II (CAPPS II). Such transfers will not be made until PNR data from US domestic flights have first been authorised for testing. PNR data transferred under this provision will not be retained by TSA or any other parties directly involved in the tests beyond the period necessary for testing purposes, or be transferred to any other third party[(6)]. The purpose of the processing is strictly limited to testing the CAPPS II system and interfaces and, except in emergency situations involving the positive identification of a known terrorist or individual with established connections to terrorism, is not to have any operational consequences. Under the provision requiring an automated filtering method described in paragraph 10, CBP will have filtered and deleted 'sensitive' data before transferring any PNRs to TSA on a bulk basis under this paragraph.

Treatment of 'sensitive' data

9. CBP will not use 'sensitive' data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual) from the PNR, as described below.

10. CBP will implement, with the least possible delay, an automated system which filters and deletes certain 'sensitive' PNR codes and terms which CBP has identified in consultation with the European Commission.

11. Until such automated filters can be implemented CBP represents that it does not and will not use 'sensitive' PNR data and will undertake to delete 'sensitive' data from any discretionary disclosure of PNR under paragraphs 28 to 34[(7)].

Method of accessing PNR data

12. With regard to the PNR data which CBP access (or receive) directly from the air carrier's reservation systems for purposes of identifying potential subjects for border examination, CBP personnel will only access (or receive) and use PNR data concerning persons whose travel includes a flight into or out of[(8)] the United States.

13. CBP will 'pull' passenger information from air carrier reservation systems until such time as air carriers are able to implement a system to 'push' the data to CBP.

14. CBP will pull PNR data associated with a particular flight no earlier than 72 hours prior to the departure of that flight, and will re-check the systems no more than three (3) times between the initial pull, the departure of the flight from a foreign point and the flight's arrival in the United States, or between the initial pull and the departure of the flight from the United States, as applicable, to identify any changes in the information. In the event that the air carriers obtain the ability to 'push' PNR data,

CBP will need to receive the data 72 hours prior to departure of the flight, provided that all changes to the PNR data which are made between that point and the time of the flight's arrival in or departure from the United States, are also pushed to CBP[9]. In the unusual event that CBP obtains advance information that person(s) of specific concern may be travelling on a flight to, from or through the United States, CBP may pull (or request a particular push) of PNR data prior to 72 hours before departure of the flight to ensure that proper enforcement action may be taken when essential to prevent or combat an offence enumerated in paragraph 3 hereof. To the extent practicable, in such instances where PNR data must be accessed by CBP prior to 72 hours before the departure of the flight, CBP will utilise customary law enforcement channels.

Storage of PNR data

15. Subject to the approval of the National Archives and Records Administration (44 U.S.C. 2101, *et seq.*), CBP will limit online access to PNR data to authorised CBP users[10] for a period of seven (7) days, after which the number of officers authorised to access the PNR data will be even further limited for a period of three years and six months (3,5 years) from the date the data are accessed (or received) from the air carrier's reservation system. After 3,5 years, PNR data that have not been manually accessed during that period of time, will be destroyed. PNR data that have been manually accessed during the initial 3,5-year period will be transferred by CBP to a deleted record file[11], where they will remain for a period of eight (8) years before they are destroyed. This schedule, however, would not apply to PNR data that are linked to a specific enforcement record (such data would remain accessible until the enforcement record is archived). With respect to PNR which CBP accesses (or receives) directly from air carrier reservation systems during the effective dates of these Undertakings, CBP will abide by the retention policies set forth in the present paragraph, notwithstanding the possible expiration of the Undertakings pursuant to paragraph 46 herein.

CBP computer system security

16. Authorised CBP personnel obtain access to PNR through the closed CBP intranet system which is encrypted end-to-end and the connection is controlled by the Customs Data Center. PNR data stored in the CBP database are limited to 'read only' access by authorised personnel, meaning that the substance of the data may be programmatically reformatted, but will not be substantively altered in any manner by CBP once accessed from an air carrier's reservation system.

17. No other foreign, federal, State or local agency has direct electronic access to PNR data through CBP databases (including through the Interagency Border Inspection System (IBIS)).

18. Details regarding access to information in CBP databases (such as who, where, when (date and time) and any revisions to the data) are automatically recorded and routinely audited by the Office of Internal Affairs to prevent unauthorised use of the system.

19. Only certain CBP officers, employees or information technology contractors[12] (under CBP supervision) who have successfully completed a background investigation, have an active, password-protected account in the CBP computer system, and have a recognised official purpose for reviewing PNR data, may access PNR data.

20. CBP officers, employees and contractors are required to complete security and data privacy training, including passage of a test, on a biennial basis. CBP system auditing is used to monitor and ensure compliance with all privacy and data security requirements.

21. Unauthorised access by CBP personnel to air carrier reservation systems or the CBP computerised system which stores PNR is subject to strict disciplinary action (which may include termination of employment) and may result in criminal sanctions being imposed (fines, imprisonment of up to one year, or both) (see title 18, United States Code, section 1030).

22. CBP policy and regulations also provide for stringent disciplinary action (which may include termination of employment) to be taken against any CBP employee who discloses information from CBP's computerised systems without official authorisation (title 19, Code of Federal Regulations, section 103.34).

23. Criminal penalties (including fines, imprisonment of up to one year, or both) may be assessed against any officer or employee of the United States for disclosing PNR data obtained in the course of his employment, where such disclosure is not authorised by law (see title 18, United States Code, sections 641, 1030, 1905).

CBP treatment and protection of PNR data

24. CBP treats PNR information regarding persons of any nationality or country of residence as law-enforcement sensitive, confidential personal information of the data subject, and confidential commercial information of the air carrier, and, therefore, would not make disclosures of such data to the public, except as in accordance with these Undertakings or as otherwise required by law.

25. Public disclosure of PNR data is generally governed by the Freedom of Information Act (FOIA) (title 5, United States Code, section 552) which permits any person (regardless of nationality or country of residence) access to a US 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 that 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)).

26. CBP regulations (title 19, Code of Federal Regulations, section 103.12), which govern the processing of requests for information (such as PNR data) pursuant to the FOIA, specifically provide that (subject to certain limited exceptions in the case of requests by the data subject) the disclosure requirements of the FOIA are not applicable to CBP 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[13].

27. CBP will take the position in connection with any administrative or judicial proceeding arising out of a FOIA request for PNR information accessed from air carriers, that such records are exempt from disclosure under the FOIA.

Transfer of PNR data to other government authorities

28. With the exception of transfers between CBP and TSA pursuant to paragraph 8 herein, Department of Homeland Security (DHS) components will be treated as 'third agencies', subject to the same rules and conditions for sharing of PNR data as other government authorities outside DHS.

29. CBP, in its discretion, will only provide PNR data to other government authorities, including foreign government authorities, with counter-terrorism or law-enforcement functions, on a case-by-case basis, for purposes of preventing and combating offences identified in paragraph 3 herein. (Authorities with whom CBP may share such data shall hereinafter be referred to as the Designated Authorities).

30. CBP will judiciously exercise its discretion to transfer PNR data for the stated purposes. CBP will first determine if the reason for disclosing the PNR data to another Designated Authority fits within the stated purpose (see paragraph 29 herein). If so, CBP will determine whether that Designated Authority is responsible for preventing, investigating or prosecuting the violations of, or enforcing or implementing, a statute or regulation related to that purpose, where CBP is aware of an indication of a violation or potential violation of law. The merits of disclosure will need to be reviewed in light of all the circumstances presented.

31. For purposes of regulating the dissemination of PNR data which may be shared with other Designated Authorities, CBP is considered the 'owner' of the data and such Designated Authorities are obligated by the express terms of disclosure to: 1. use the PNR data only for the purposes set forth in paragraph 29 or 34 herein, as applicable; 2. ensure the orderly disposal of PNR information that has been received, consistent with the Designated Authority's record retention procedures; and 3. obtain CBP's express authorisation for any further dissemination. Failure to respect the conditions for transfer may be investigated and reported by the DHS Chief Privacy Officer and may make the Designated Authority ineligible to receive subsequent transfers of PNR data from CBP.

32. Each disclosure of PNR data by CBP will be conditioned upon the receiving agency's treatment of this data as confidential commercial information and law enforcement sensitive, confidential personal information of the data subject, as identified in paragraphs 25 and 26 hereof, which should be treated as exempt from disclosure under the Freedom of Information Act (5 U.S.C. 552). Further, the recipient agency will be advised that further disclosure of such information is not permitted without the express prior approval of CBP. CBP will not authorise any further transfer of PNR data for purposes other than those identified in paragraphs 29, 34 or 35 herein.

33. Persons employed by such Designated Authorities who without appropriate authorisation disclose PNR data, may be liable for criminal sanctions (title 18, United States Code, sections 641, 1030 and 1905).

34. No statement herein shall impede the use or disclosure of PNR data to relevant government authorities, where such disclosure is necessary for the protection of the vital interests of the data subject or of other persons, in particular as regards significant health risks. Disclosures for these purposes will be subject to the same conditions for transfers set forth in paragraphs 31 and 32 of these Undertakings.

35. No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law. CBP will advise the European Commission regarding the passage of any US legislation which materially affects the statements made in these Undertakings.

Notice, access and opportunities for redress for PNR data subjects

36. CBP will provide information to the travelling public regarding the PNR requirement and the issues associated with its use (i.e. general information regarding the authority under which the data are collected, the purpose for the collection, protection of the

data, data-sharing, the identity of the responsible official, procedures available for redress and contact information for persons with questions or concerns, etc., for posting on CBP's website, in travel pamphlets, etc.).

37. Requests by the data subject (also known as first party requesters) to receive a copy of PNR data contained in CBP databases regarding the data subject are processed under the Freedom of Information Act (FOIA). Such requests may be addressed to: Freedom of Information Act (FOIA) Request, US Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, DC 20229, if by mail; or such request may be delivered to the Disclosure Law Officer, US Customs and Border Protection, Headquarters, Washington, DC. Further information regarding the procedures for making FOIA requests is contained in section 103.5 of title 19 of the US Code of Federal Regulations. In the case of a first-party request, the fact that CBP otherwise considers PNR data to be confidential personal information of the data subject and confidential commercial information of the air carrier will not be used by CBP as a basis under FOIA for withholding PNR data from the data subject.

38. In certain exceptional circumstances, CBP may exercise its authority under FOIA to deny or postpone disclosure of all (or, more likely, part) of the PNR record to a first party requester, pursuant to title 5, United States Code, section 552(b) (e.g. if disclosure under FOIA 'could reasonably be expected to interfere with enforcement proceedings' or 'would disclose techniques and procedures for law enforcement investigations (...) (which) could reasonably be expected to risk circumvention of the law'). Under FOIA, any requester has the authority to administratively and judicially challenge CBP's decision to withhold information (see 5 U.S.C. 552(a)(4)(B); 19 CFR 103.7 to 103.9).

39. CBP will undertake to rectify[(14)] data at the request of passengers and crew members, air carriers or data protection authorities (DPAs) in the EU Member States (to the extent specifically authorised by the data subject), where CBP determines that such data is contained in its database and a correction is justified and properly supported. CBP will inform any Designated Authority which has received such PNR data of any material rectification of that PNR data.

40. Requests for rectification of PNR data contained in CBP's database and complaints by individuals about CBP's handling of their PNR data may be made, either directly or via the relevant DPA (to the extent specifically authorised by the data subject) to the Assistant Commissioner, Office of Field Operations, US Bureau of Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, DC 20229.

41. 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, who will review the situation and endeavour to resolve the complaint[(15)].

42. Additionally, the DHS Privacy Office will address on an expedited basis, complaints referred to it by DPAs in the European Union (EU) Member States on behalf of an EU resident to the extent such resident has authorised the DPA to act on his or her behalf and believes that his or her data-protection complaint regarding PNR has not been satisfactorily dealt with by CBP (as set out in paragraphs 37 to 41 of these Undertakings) or the DHS Privacy Office. The Privacy Office will report its conclusions and advise the DPA or DPAs concerned regarding actions taken, if any. The DHS Chief Privacy Officer will include in her report to Congress issues regarding

the number, the substance and the resolution of complaints regarding the handling of personal data, such as PNR[16].

Compliance issues

43. CBP, in conjunction with DHS, undertakes to conduct once a year, or more often if agreed by the parties, a joint review with the European Commission assisted as appropriate by representatives of European law-enforcement authorities and/or authorities of the Member States of the European Union[17], on the implementation of these Undertakings, with a view to mutually contributing to the effective operation of the processes described in these Undertakings.

44. CBP will issue regulations, directives or other policy documents incorporating the statements herein, to ensure compliance with these Undertakings by CBP officers, employees and contractors. As indicated herein, failure of CBP officers, employees and contractors to abide by CBP's policies incorporated therein may result in strict disciplinary measures being taken, and criminal sanctions, as applicable.

Reciprocity

45. In the event that an airline passenger identification system is implemented in the European Union which requires air carriers to provide authorities with access to PNR data for persons whose current travel itinerary includes a flight to or from the European Union, CBP shall, strictly on the basis of reciprocity, encourage US-based airlines to cooperate.

Review and termination of Undertakings

46. These Undertakings shall apply for a term of three years and six months (3,5 years), beginning on the date upon which an agreement enters into force between the United States and the European Community, authorising the processing of PNR data by air carriers for purposes of transferring such data to CBP, in accordance with the Directive. After these Undertakings have been in effect for two years and six months (2,5 years), CBP, in conjunction with DHS, will initiate discussions with the Commission with the goal of extending the Undertakings and any supporting arrangements, upon mutually acceptable terms. If no mutually acceptable arrangement can be concluded prior to the expiration date of these Undertakings, the Undertakings will cease to be in effect.

No private right or precedent created

47. These Undertakings do not create or confer any right or benefit on any person or party, private or public.

48. The provisions of these Undertakings shall not constitute a precedent for any future discussions with the European Commission, the European Union, any related entity, or any third State regarding the transfer of any form of data.

11 May 2004

ATTACHMENT A

PNR data elements required by CBP from air carriers

1. PNR record locator code

2. Date of reservation

3. Date(s) of intended travel

4. Name
5. Other names on PNR
6. Address
7. All forms of payment information
8. Billing address
9. Contact telephone numbers
10. All travel itinerary for specific PNR
11. Frequent flyer information (limited to miles flown and address(es))
12. Travel agency
13. Travel agent
14. Code share PNR information
15. Travel status of passenger
16. Split/divided PNR information
17. E-mail address
18. Ticketing field information
19. General remarks
20 Ticket number
21. Seat number
22. Date of ticket issuance
23. No show history
24. Bag tag numbers
25. Go show information
26. OSI information
27. SSI/SSR information
28. Received from information
29. All historical changes to the PNR
30. Number of travellers on PNR
31. Seat information
32. One-way tickets
33. Any collected APIS (Advanced Passenger Information System) information
34. ATFQ (Automatic Ticketing Fare Quote) fields

(**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).

(**2**) Title 49, United States Code, section 44909(c)(3).

(**3**) Title 19, Code of Federal Regulations, section 122.49b.

(**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 United States 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 2/2004 on the adequate protection of personal data contained in the PNR of air passengers to be 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://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf

(**5**) For the purposes of these Undertakings, the terms 'passenger' and 'passengers' shall include crew members.

(**6**) For purposes of this provision, CBP is not considered a party directly involved in the CAPPS II testing or a 'third party'.

(**7**) Prior to CBP's implementation of automated filters (as referenced in paragraph 10 hereof), if 'sensitive' data exists in a PNR which is the subject of a non-discretionary disclosure by CBP as described in paragraph 35 hereof, CBP will make every effort to limit the release of 'sensitive' PNR data, consistent with US law.

(**8**) This would include persons transiting through the United States.

(**9**) In the event that the air carriers agree to push the PNR data to CBP, the agency will engage in discussions with the air carriers regarding the possibility of pushing PNR data at periodic intervals between 72 hours before departure of the flight from a foreign point and the flight's arrival in the United States, or within 72 hours before the departure of the flight from the United States, as applicable. CBP seeks to utilise a method of pushing the necessary PNR data that meets the agency's needs for effective risk assessment, while minimising the economic impact upon air carriers.

(**10**) These authorised CBP users would include employees assigned to analytical units in the field offices, as well as employees assigned to the National Targeting Center. As indicated previously, persons charged with maintaining, developing or auditing the CBP database will also have access to such data for those limited purposes.

(**11**) Although the PNR record is not technically deleted when it is transferred to the Deleted Record File, it is stored as raw data (not a readily searchable form and, therefore, of no use for 'traditional' law enforcement investigations) and is only available to authorised personnel in the Office of Internal Affairs for CBP (and in some cases the Office of the Inspector General in connection with audits) and personnel responsible for maintaining the database in CBP's Office of Information Technology, on a 'need to know' basis.

(**12**) Access by 'contractors' to any PNR data contained in the CBP computer systems would be confined to persons under contract with CBP to assist in the maintenance or development of CBP's computer system.

(**13**) CBP would invoke these exemptions uniformly, without regard to the nationality or country of residence of the subject of the data.

(**14**) By 'rectify', CBP wishes to make clear that it will not be authorised to revise the data within the PNR record that it accesses from the air carriers. Rather, a separate record linked to the PNR record will be created to note that the data were determined to be inaccurate and the proper correction. Specifically, CBP will annotate the passenger's secondary examination record to reflect that certain data in the PNR may be or are inaccurate.

(**15**) The DHS Chief Privacy Officer is independent of any directorate within the Department of Homeland Security. She is statutorily obligated to ensure that personal information is used in a manner that complies with relevant laws (see footnote 13). The determinations of the Chief Privacy Officer shall be binding on the Department and may not be overturned on political grounds.

(**16**) Pursuant to section 222 of the Homeland Security Act of 2002 (the Act) (Public Law 107-296, dated 25 November 2002), the Privacy Officer for DHS is charged with conducting a 'privacy impact assessment' of proposed rules of the Department on 'the privacy of personal information, including the type of personal information collected and the number of people affected' and must report to Congress on an annual basis regarding the 'activities of the Department that affect privacy ...'. Section 222(5) of the Act also expressly directs the DHS Privacy Officer to hear and report to Congress regarding all 'complaints of privacy violations'.

(**17**) The composition of the teams on both sides will be notified to each other in advance and may include appropriate authorities concerned with privacy/data protection, customs control and other forms of law enforcement, border security and/or aviation security. Participating authorities will be required to obtain any necessary security clearances and will adhere to the confidentiality of the discussions and documentation to which they may be given access. Confidentiality will not however be an obstacle to each side making an appropriate report on the results of the joint review to their respective competent authorities, including the US Congress and the European Parliament. However, under no circumstances may participating authorities disclose any personal data of a data subject; nor may participating authorities disclose any non-public information derived from documents to which they are given access, or any operational or internal agency information they obtain during the joint review. The two sides will mutually determine the detailed modalities of the joint review.