EUROPEAN
COMMISSION

Brussels, 27.11.2013
SEC(2013) 630 final

Joint Review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security

Accompanying

the Report from the Commission to the European Parliament and to the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security

{COM(2013) 844 final}

TABLE OF CONTENTS

1. BACKGROUND AND PROCEDURAL ASPECTS OF THE JOINT REVIEW

Following the 11 September 2001 terrorist attack, the United States enacted a statute in November 2001[1] and regulations[2] implementing this statute, requiring each air carrier operating passenger flights to and from the United States to transfer to the U.S. Customs and Border Protection ('CBP') personal data contained in the Passenger Name Record ('PNR') of air carriers. In June 2002 the Commission informed the U.S. authorities that these requirements could conflict with European and Member States' legislation on data protection which impose conditions on the transfer of personal data to third countries.

As a result, the EU and the U.S. entered into negotiations aimed at reaching agreement on sharing air passenger data while securing an adequate level of data protection. To avoid repetitions as to the background of PNR Agreements, reference is made to the joint review reports of 2006 and 2010.[3]

According to Article 23(1) of the Agreement on the use and transfer of passsenger name records to the United States Department of Homeland Security (DHS)[4], the Parties shall jointly review the implementation of the Agreement one year after its entry into force and regularly thereafter as jointly agreed. In line with this requirement, the first joint review of the Agreement was carried out one year after its entry into force on 1 July 2012, i.e. in Washington on 8 and 9 July 2013. Under the terms of Article 23(2), the EU would be represented by the European Commission, and the U.S. would be represented by DHS. The EU Commissioner for Home Affairs delegated this task to Reinhard Priebe, Director in DG Home Affairs, while the U.S. Secretary of Homeland Security delegated this task to Jonathan Cantor, Acting Chief Privacy Officer, DHS Privacy Office. Both officials nominated teams to assist them in their tasks. A full list of the members of both teams appears in Annex B. It is noted that the EU team included two experts to assist it in its tasks, namely a data protection expert and a law enforcement expert.

The methodology which was developed and followed for the joint review exercise was the following:

- The EU team was composed of 5 Commission officials and 2 external experts.
- The Commission had sent out a questionnaire to DHS in advance of the joint review. This questionnaire contained specific questions in relation to the implementation of the Agreement by DHS. DHS provided written replies to the questionnaire prior to the joint review.
- The EU team was granted access to DHS premises and carried out a field visit at DHS National Targeting Center (NTC).
- The EU team was given the opportunity to watch the databases being operated in real time with the results shown and explained on screen by a senior analyst.

---

1 Aviation and Transportation Security Act (ATSA).

2 US Regulation 19 CFR 122.49d on PNR information.

3 Commission staff working paper on the joint review of the implementation by the U.S. Bureau of Customs and Border Protection of the Undertakings set out in Commission Decision 2004/535/EC of 14 May 2004, 20-21 September 2005, Redacted version, 12.12.2005. Report on the joint review of the implementation of the Agreement between the European union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), 8-9 February 2010, Brussels, 7.4.2010.

4 OJ L 215/5, 11.08.2012.

- The EU team had the opportunity to have direct exchanges with DHS personnel responsible for the PNR program and targeters and analysts who use and have access to PNR data.
- The replies to the questionnaire were discussed in detail with DHS. The EU team also had the opportunity and the time to raise further questions to DHS officials and address all the various parameters of the Agreement. A full day meeting was dedicated to this purpose.
- At the request of DHS, all members of the EU team signed a copy of a non-disclosure agreement as a condition for their participation in this review exercise.
- DHS had the opportunity to ask questions to the EU team about the status of the EU PNR proposal.
- In preparation of the joint review exercise, the DHS Privacy Office prepared its own report on the use and transfer of Passenger Name Records between the European Union and the United States.[5]
- For the preparation of this report, the EU team used information contained in the written replies that DHS provided to the EU questionnaire, information obtained from its discussions with DHS personnel, information contained in the aforementioned DHS Privacy Office report, as well as information contained in other publicly available DHS documents.

Due to the sensitive nature of the PNR program, there were limitations on the provision of some internal operational documents. Each member of the EU team received a copy of two internal operational documents for review during the meeting on 9 July 2013. One document concerned a Customs and Border Protection (CBP) Directive on the use and disclosure of PNR data. It outlines the use, handling, and disclosure of PNR data and provides a framework for granting access to PNR to authorized personnel within DHS and for sharing PNR with DHS's domestic and international partners. The other document consists of internal guidelines on quarterly reviews of travel targeting scenarios, targeting rules and analysis, aimed at minimizing the impact of the use of such scenarios and rules on civil rights, civil liberties and privacy.

Other information was provided to the EU team with the condition that it would be treated as classified up to the level of EU Restricted. The present report should be read in the light of these limitations, as well as in the light of the fact that all members of the EU team had to sign non-disclosure agreements exposing them to criminal and/or civil sanctions for breaches.

It has to be noted that the joint review is not an inspection of DHSs PNR policies and the EU team had no investigative powers.

In spite of such limitations, before, during, and after the review there has been an exchange of views in an open and constructive spirit which covered all the questions of the EU team. Therefore the Commission would like to acknowledge the good cooperation on the part of all DHS and other US personnel and express its gratitude for the way in which the questions of the review team have been replied to.

The Commission also acknowledges the professional and constructive assistance it received from the data protection and law enforcement experts who participated in the EU team.

---

[5] DHS Privacy Office, a report on the use and transfer of Passenger Name Records between the European Union and the United States, 3 July 2013, available at http://www.dhs.gov/sites/default/files/publications/dhs-pnr-privacy-review-20130703.pdf.

The joint review also allowed for a preliminary assessment whether the Agreement serves its purpose and contributes to the fight against terrorism and serious crime. Finally, it should be noted that the procedure for the issuance of this report was agreed with the U.S. team. The EU team prepared a draft report, which was sent to DHS, providing DHS with the opportunity to comment on inaccuracies and on information that could not be disclosed to public audiences. It is clarified that this is the report of the EU team as delegated by the Commissioner for Home Affairs, and is not a joint report of the EU and U.S. teams.

The present report has received the unanimous agreement of the members of the EU team.

2. THE OUTCOME OF THE JOINT REVIEW

This Chapter provides the main findings resulting from the joint review of the EU team.

In order to comply with the Agreement, the U.S. incorporated the terms thereof into a System of Records Notice (SORN) for the system that holds the PNR data, the Automated Targeting System (ATS), published on 22.5.2012.[6] DHS had to introduce changes to the technology of the ATS (specifically the module referred to as ATS-Passenger) in order to comply with the Agreement, such as introduce a depersonalization mechanism and a repersonalization functionality as part of the retention requirements under Article 8 of the Agreement.

Notwithstanding Article 23(1) on a joint evaluation of the Agreement four years after its entry into force, a preliminary assessment of the question whether PNR serves the purpose of supporting the fight against terrorism and other crimes that are transnational in nature showed that PNR provides DHS with the possibility of carrying out pre-departure assessments of all passengers up to 96 hours which gives DHS sufficient time to carry out all the background checks before the arrival of a passenger and prepare its response. This processing also supports DHS when deciding if a passenger should board a plane or not. It also provides DHS with the opportunity to perform risk assessments on the basis of scenario-based targeting rules in order to identify the 'unknown' potential high-risk individuals.[7] PNR further provides the possibility to make associations between passengers and identify criminals who belong to the same organised crime group. According to DHS PNR is also successfully used for identifying trends of how criminals tend to behave when they travel, for example by understanding which routes they use.

As regards the implementation of the Agreement, the overall finding is that DHS has implemented the Agreement in line with the conditions set out therein. This is reflected in more detail in the list of the main findings outlined below.

2.1. Main findings

2.1.1 Scope (Article 2)

Although most flights operate directly between the U.S. and a foreign airport, the ATS system uses flight numbers and airport codes to identify flights with a U.S. nexus. First, the ATS selects PNR of flights that contain a U.S. segment, for example Flight #103 Singapore-Brussels-New York. Then the ATS screens the data again, this time using airport codes to identify those parts of Flight #103 that have a U.S. nexus, i.e. the segment Brussels-New York. As a result of this selection, ATS will filter out the PNRs of those travellers that only take the Singapore-Brussels segment.

---

6 http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.

7 Joint Review Discussion July 8 & 9, 2013

DHS also deploys an override mechanism, allowing it to obtain PNRs from passengers on flights that do not have a U.S. airport code, in case such a flight intends to land on U.S. soil for unforeseen reasons such as weather conditions. In order to activate the override mechanism, a DHS officer must have authority to access PNRs on flights with a U.S. nexus. The use of the override mechanism is reviewed every 24 hours for validation.[8] During the period of 1 July 2012-31 March 2013, 192 overrides were registered. In three cases it had not been entirely clear why the override mechanism had been used. The DHS managers overseeing the use of this mechanism found that in two cases the use was the result of a mistaken interpretation of an airport code, which are used to differentiate between flights with an U.S. nexus and those which are not. In the other case there was a transmission of Advance Passenger Information (API) [9] which triggered the officer to take a look at the related PNR data but the review of the use of the override mechanism revealed that this API transmission was mistaken and that as a result also the consultation of the PNR data should not have taken place.

DHS clarified that the consultation of the 192 overrides concerned the consultation of 192 individual PNRs.

Conclusion: DHS has a filtering mechanism in place to filter out flights with no clear U.S. nexus using flight numbers and airport codes. This mechanism has been reviewed as part of the DHS Privacy Office internal review. DHS also deploys user access controls and a review mechanism 24 hours after the override occurred to see if this mechanism was used correctly.

The number of cases in which the override mechanism was used, show a limited use, in particular when compared to the figure mentioned in the 2010 joint review report. The 2010 joint report signalled that since the override mechanism was established in October 2009, it had been used to access 2500 individual PNRs for 198 flights during a period of 4 months (October 2009 – 8 February 2010, i.e. the date of the then joint review).[10]

DHS respects the obligation under the Agreement to only use PNRs of flights with a U.S. nexus. The use of the override mechanism is submitted to a number of conditions, used in a limited way and overseen.

2.1.2. Provision of PNR (Article 3)

DHS has a filtering mechanism in place to filter out PNR data beyond those listed in the Annex to the Agreement. This mechanism has also been reviewed as part of the DHS Privacy Office internal review. It applies irrespective of whether the data are “pushed” or “pulled”.

DHS indicated that it has not encountered any problems in receiving PNR as listed in the Annex to the Agreement and that it sees no need to reduce or expand the current list of PNR.

At the request of the EU team about the usefulness of the PNR data types listed in the Annex to the Agreement, DHS outlined that it uses 18 out of the 19 data types (except for historical PNR) for matching against their scenario-based targeting rules. However DHS underlined that there are differences depending on the kind of situation. In case there is a (short term) lookout for a particular passenger, notably the PNR data types indicating the dynamics (changes) will be of importance, whereas PNR is used differently in case of a more static situation.

---

8 Joint Review Discussion July 8 & 9, 2013.

9 API data contain information held in a passport or other travel document.

10 DHS clarified that the majority of the 2500 individual PNRs for 198 flights during the four month period was result of an officer inappropriately using the system. Necessary steps were taken to avoid such an incident in the future.

Conclusion: DHS filters out PNR data elements that it receives which are outside the 19 data elements listed in the Annex to the Agreement.

2.1.3. Use of PNR (Article 4)

Different data sets are used to vet passengers when applying to travel, prior to departure and upon arrival: visa data or alternatively if no visa is required, data collected under the Electronic System for Travel Authorisation (ESTA); booking information; check-in information; and information collected upon the departure of a flight.

For the year 2012, the number of individuals targeted by ATS for further attention was 101 805 (out of an average number of 110 million air travellers), which is 0.09%. Of those 101 805 air passengers, 52 734 arrived to the U.S. by European flights.[11] Persons that have been identified as a result of manual processing by a targeter are marked for the border guards' attention. The border guard who receives such a person at the border will make his or her own assessment whether this person should be cleared, sent to secondary screening, arrested or denied entry into the U.S.

In its reply to the questionnaire, DHS explains to quite some extent the nature of the Regional Carriers Liaison Groups Program, the Immigration Advisory Program and the Secure Flight Program. DHS mentioned that the Secure Flight system does not utilize PNR. For this reason the discussions focused on the other two programs with the aim to obtain further insight into the way PNR supports those programs.

DHS explained that the Immigration Advisory Program (IAP) and the Regional Carriers Liaison Groups Program (RCLG) are complementary. In fact, the IAP, implemented since 2004, is used at 11 non-U.S. airports located in 9 countries[12], whereas the RCLG covers around 250 other airports around the world using three regional RCLG offices based in the U.S., each covering a part of the world.

Under the IAP, the role of DHS staff is to assist airlines and security personnel with document examination and traveller security assessment.[13] The CBP liaison officers evaluate passengers selected by the targeters of the DHS National Targeting Center through further questions and assessment and, where appropriate, contact the airline for coordination. Eventually, the liaison officer will inform the air carrier if a passenger will be denied entry into the U.S. upon arrival and on this basis will recommend that the air carrier not carry this passenger on the aircraft. The IAP thus is intended to increase the number of travellers who are prevented from boarding an aircraft to the U.S., rather than permitting travellers to board but then deny them entry into the U.S. upon their arrival. This program concerns people who are not listed in the no-fly database which is used under the Secure Flight Program.

The RCLG, implemented since 2010, basically is an extension of the IAP to locations where the U.S. does not have liaison officers at non-U.S. airports. Under the RCLG, which works otherwise in the same way as the IAP, the DHS National Targeting Centre makes direct contact with the carrier and recommends that it not carry the specific passenger, rather than having a CBP liaison officer making contact with the air carrier.

The IAP led in 2012 to 3600 global cases where travellers did not board a flight to the U.S. In the case of the RCLG, the number of global cases in 2012 amounted to 600 travellers, which brings the total number for 2012 under both programs to 4200 travellers. According to DHS,

---

11 Joint Review Discussion July 8 & 9, 2013

12 In the EU these are: Roissy (Charles De Gaulle) (FR), Frankfurt (DE), Heathrow, Manchester and Gatwick (UK), Schiphol (NL), and Madrid (ES).

13 CBP Fact sheet on the IAP, http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/travel.

in most of the cases the inadmissibility is determined on the basis of the lack of a visa, or the use of a stolen or otherwise not valid passport. If the denial of boarding is a denial generated as a result of an ESTA, the passenger will need to obtain a visa.

DHS explained that the CBP officers decide themselves to what extent they want to consult a PNR if they analyse a specific case as part of the IAP or the RCLG. DHS (CBP) does not engage into a systematic cross-checking of PNR under the IAP and the RCLG but instead reviews all available data, including PNR, when a specific passenger is being looked at. The relevance of PNR will depend on what kind of information a CBP officer wants to look at following the information s/he received from other agencies. For example a PNR may be looked at if the officer considers it necessary to check if the passenger travels with another person, as PNR may provide such information.

Also, if available law enforcement information includes a telephone number, the officer may consult a PNR as a telephone number may be included in the passenger's booking information. Also the name in a PNR constitutes an important data element, not in the least because it is available at an earlier stage (at 96 hours prior to scheduled flight departure) compared to the name as part of the API (passport) data, which are only collected upon check-in.

DHS further explained that the Secure Flight Program (SFP) is a separate program and is meant to identify known or suspected terrorists under the U.S no-fly or selectee list.[14] It is a terrorism related and aviation security related program. A passenger identified under the SFP who is on the no-fly list is not allowed to board a flight to the U.S., including flights overflying U.S. airspace. Passengers on the selectee list must be subject to a physical check by airport security officials prior to boarding. The SFP requires air carriers to send the passengers' full name as mentioned in their passport or other ID document used for travelling, gender and date of birth. In addition the air carrier has to send the itinerary, including arrival time/departure time information (depending on whether the flight is an inbound or outbound flight) to prioritise analysis. The program has no access to PNR. If available, air carriers are also requested to send known trusted traveller information.

In the case of the SFP the air carriers have to follow a no-fly decision made by DHS (its component Transportation Security Administration). DHS mentioned that the SFP on average results in 5 to 6 no-fly cases per day (qualified as true matches, i.e. not including any possible false positives).

Article 4(3) enables DHS to use and process PNR to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the U.S. or who may require further examination. It concerns one of the ways in which PNR is used, i.e. allowing DHS to focus on air passengers upon arrival that require further attention from a security perspective and clarifies that PNR may, in accordance with its purpose and scope, be processed to identify persons who may require further examination. On a daily basis the data enable DHS to select around 1% of air passengers for closer examination by targeters from the DHS National Targeting Centre followed by a final decision taken by CBP staff at the border on whether the passenger should be permitted to enter, sent to secondary inspection, arrested or denied entry into the U.S. Between July 2012 and April 2013 CBP collected 68 million PNR. 10 902 passengers were targeted due to an analysis of PNR only, or 0.016%.

Under Article 4(2), PNR may be used on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interest of any individual or if ordered by a court.

[14] Http://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-secure-flight-update-09042013.pdf

In the light of media revelations about US surveillance programmes, the EU team enquired if under Article 4(2) of the Agreement, which allows PNR to be "*used and processed on a case-by-case basis [….] if ordered by court*", if an order from the Foreign Intelligence Surveillance Act (FISA) Court would be considered as an "order by court" within the meaning of Article 4(2). DHS replied that it had not received any FISA Court order. In subsequent discussions in the ad hoc EU-US Working Group on Data Protection, the US side further clarified that the FISA Court only has jurisdiction to hear applications for surveillance measures under FISA.

Under Article 4(4), subpoenas or other legally mandated disclosures are responded to with the assistance from DHS or CBP Counsel. Between 1 July 2012 and 31 March 2013, users logged 15 disclosures for these purposes. DHS furthermore confirmed that none of these subpoenas or other legally mandated disclosure were from the FISA Court.

Conclusion: The way in which DHS uses PNR is consistent with the use of such data by other countries deploying PNR systems. The various ways in which PNR is used follows an approach allowing it to maximize the added value of using PNR for law enforcement purposes.

The exceptions to the main purposes of the Agreement are used in a limited manner. As outlined under 2.1.13.1. on domestic sharing, ,the system logged 589 disclosures, of which two are related to disclosures with third countries under Article 17. Of the remaining 587 disclosures, another 15 took place under Article 4(4) of the Agreement. This means that 572 disclosures took place under Article 4(2). Of those 572 disclosures, DHS made seven disclosures to the U.S. Center for Disease Control and Prevention to coordinate responses to health associated with international air transportation.

2.1.4. Data security (Article 5)

DHS reported that no privacy incidents, including unauthorised access or disclosure, occurred since the Agreement entered into force.

In its reply to the EU questionnaire, DHS referred to a CBP Directive regarding use and disclosure of PNR data. This Directive (hereinafter referred to as the "CBP Directive") updated to reflect the current Agreement, outlines the use, handling, and disclosure of PNR data.

At the request of the EU team, DHS provided a copy of this internal Directive to each of the team members for review during the meeting on 9 July.

Article 5(2) requires DHS to make appropriate use of technology to ensure data protection, security, confidentiality and integrity. The DHS Privacy Office internal review report indicates that, in order to promote data integrity, "*DHS provides individuals with the means to seek correction or rectification of their PNR*".[15]

With regard to accountability measures, the report outlines in more detail the layers of oversight ensuring compliance with data security requirements. The report mentions that with regard to the risk of unauthorized access or use of PNR, "*CBP's Office of Internal Affairs audits the use of ATS and the CBP Office of Intelligence and Investigation Liaison (OIIL) verifies that users with PNR access are authorized to retain that access. To guard against unintended or inappropriate disclosure of PNR data, OIIL conducts audits of all disclosures within and outside DHS. The CBP Privacy Office oversees the results of these audits and takes appropriate corrective action if warranted. OIIL, in coordination with CBP's Office of Field Operations (OFO) and Office of Information and Technology (OIT), is responsible for*

[15] DHS Privacy Office internal review report, Chapter 5, page 17.

maintaining updated technical/security procedures by which PNR is accessed by DHS and Non-DHS Users. CBP completed a security Plan for ATS and in 2011 received its certification and accreditation (C&A) under the Federal Information Security Management Act (FISMA) and Authority to Operate ATS for three years."[16]

The report also mentions that between 1 July 2012 and 31 March 2013 the DHS Privacy Office did not receive reports of the loss or compromise of EU PNR.[17]

Conclusion: DHS applies a series of measures to ensure data security of the ATS. It limits access to ATS to those with a need to know basis, including a further limitation by confining access to what is required to conduct assigned duties. It deploys access controls, has put audit trails in place, data separation and data encryption, and provides training to staff. The use of ATS is also the subject of various accounting measures. The CBP Directive regarding the use and disclosure of PNR has been reviewed by the EU team members during the meeting of 9 July 2013. It outlines the conditions set by the Agreement accurately and is in line with the Agreement.

2.1.5. Sensitive data (Article 6)

DHS mentioned that certain codes and terms that may appear in a PNR have been identified as sensitive. These sensitive codes and terms are blocked from view in CBP's systems and are deleted after 30 days. According to DHS' explanations, access to sensitive codes and terms may be granted only upon approval by the Deputy Commissioner of CBP, in consultation with other senior CBP and DHS executive officers. Access to sensitive codes or terms in PNR without proper permission will result in suspension of the user's access to PNR and/or ATS-P system access.[18]

If sensitive codes or terms in PNR are accessed, the system will notify CBP Headquarters managers within 24 hours. In such a case the managers will conduct a review of the access and examine any supporting documentation. Although not required under the Agreement, under DHS rules the DHS Office of International Affairs will provide notice to the European Commission within 48 hours.[19]

DHS confirmed that it did not access and use sensitive data for operational purposes[20].

In accordance with Article 6(2), DHS provided the European Commission within 90 days of the entry into force of the Agreement a list of codes and terms identifying sensitive data that shall be filtered out.

Conclusion: Until the date of the joint review (i.e. 8-9 July 2013), DHS has not accessed and used sensitive data for the exceptional circumstances outlined in the Agreement. For this reason DHS cannot provide the EU with any information about the performance of the DHS senior manager overseeing such exceptional access and use. DHS also notified to the Commission the list of sensitive codes and terms filtered by their system.

Although not required under the Agreement, under DHS rules the DHS Office of International Affairs will provide notice to the European Commission within 48 hours in case sensitive data would have been accessed by DHS staff.

---

16 Ibid., Chapter 7, pages 20-21.

17 Ibid., Chapter 7, page 21.

18 Joint Review Discussion July 8 & 9, 2013

19 Ibid.

20 DHS only used sensitive data three times to test the system's access notification functionality.

2.1.6. Automated individual decisions(Article 7)

The EU team did not raise questions as regards Article 7 of the Agreement on "automated individual decision". The explanations provided in U.S. documents explaining the way in which the system handling PNR data functions[21] show that DHS does not take decisions producing significant adverse actions affecting the legal interests of individuals on the sole basis of an automated processing and use of PNR.

The DHS Privacy Office internal review report mentions that it received statistics from DHS showing its use of PNR. The report mentions that internal instructions[22] "*require that no decisions concerning travelers are to be based solely on the automated processing and use of PNR*". [23]

2.1.7. Retention of data (except for the start of the depersonalization mechanism)

*(Article 8)*During the meeting at the National Targeting Center, DHS staff outlined that in its experience, individuals may try to hide their criminal intentions, but the information in a PNR often helps to detect this. As outlined under point 2.1.2, DHS uses 18 out of the 19 PNR data types for matching against their scenario-based –targeting rules, with the exception of historical PNR. Historical data are used to match and verify actual data, so if the data of a person "known" to DHS have changed, the comparison between the historical data and the real time data may again trigger matches. With regard to historical PNR, DHS indicated that it is difficult from an operational perspective to identify how long one should go back in time. In case of matching new PNR against historical PNR, the system will actually read the latest PNR against the entirety of PNRs generated in the past.

Article 8(1) of the Agreement stipulates that after the initial six months of the five years retention period during which PNR are retained in an active database, PNR shall be depersonalised and masked. Such depersonalisation and masking had to start under the Agreement as from 1 January 2013. During the meeting at the National Targeting Center the EU team asked DHS what its experiences are with masking and with re-personalisation. DHS replied that it is able to maintain its operations despite the masking of PNR. DHS also mentioned that the re-personalisation functionality is operable as from March 2013. Between March 2013 and the joint review, there have been 29 cases of repersonalisation of PNR records.[24]

Also in Article 8(1), the Agreement specifies that access to the active database shall be restricted to a limited number of specifically authorised officials. DHS clarified that out of the approximate 40 000 users having direct access to the ATS-P, 12 448 users have direct access to the PNR kept in the active PNR database within the ATS-P. Of those 12 448 users, 1049 are DHS users with supervisory PNR access.[25] The access to ATS-P needs supervisory approval and is approved or denied by CBP Headquarters. Access is submitted to supervisory review. There are automated safeguards, as passwords have to be renewed after 30 days and inactive accounts are locked after 90 days.[26] Audits are conducted every 6 months to verify that the user continues to require PNR access, and to review user profile information and user role.

---

21 DHS proceeded in June 2012 with an update of the Privacy Impact Assessment for the system holding amongst others PNR data, with the aim to inform the public about the changes in this system It can be found at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.

22 The CBP Directive.

23 DHS Privacy Office internal review report, Chapter 3, page 13.

24 Joint Review Discussion July 8 & 9, 2013.

25 Ibid.

26 Ibid.

Article 8(3) on the transfer of PNR from the active database to a dormant database will only become relevant at the moment the primary five-year period starts expiring as from the effective date of the agreement, 1 July 2012. As indicated in the reply to the questionnaire, for this reason no PNR are scheduled to be transferred to a dormant database until 1 July 2017.

In case of sharing of PNR data with a law enforcement agency because the record meets the requirements for sharing, the agency shall afford to that record equivalent and comparable safeguards as set out in the Agreement as outlined in Article 16(1)(d).

Conclusion: DHS has developed automated processes to depersonalise PNR. DHS has also limited the number of users that has access to the active PNR database.

The implementation of Article 8(3) will only become relevant as from 1 July 2017.

2.1.8. Non-discrimination (Article 9)

The DHS Privacy Office, together with the DHS Office of Civil Rights and Civil Liberties and the DHS Office of the General Counsel proceed on a quarterly basis with ex-post reviews of the targeting rules DHS runs against PNR to identify high-risk travellers based on specific risk scenarios as identified on the basis of intelligence. This is a new feature of the oversight role the Privacy office plays as regards the use of PNR. The quarterly reviews aim to ensure, amongst others, that DHS does not use PNR to unlawfully discriminate against passengers. To achieve this, the three Offices review all travel targeting scenarios, targeting rules and analysis to ensure that they are tailored to minimize the impact on bona fide travellers' civil rights, civil liberties and privacy.[27] The DHS Privacy Office underlined that a result of its internal review process, is the further assurance that targeting rules are not unlawfully discriminatory.[28] The DHS Privacy Office also underlined that the DHS targeting rules are timely defined, i.e. they are adapted regularly to reflect the changes in the intelligence they are based on, and narrowly defined in order to meet their objective of identifying high-risk travellers.

Conclusion: The quarterly review assists DHS in respecting the non-discrimination requirement of the Agreement. The EU review team was provided with a copy of the document outlining such reviews and was given the possibility to review this document during the meeting on 9 July. The document respects the Agreement.

2.1.9. Transparency (Article 10)

The DHS Privacy Office internal review report mentions that CBP's Frequently Asked Questions and PNR Privacy Policy "*reflected the 2007 PNR Agreement rather than the 2011 Agreement*". It recommended to promptly amending these documents to provide full transparency.[29] The report mentions that information on the Agreement (additional to the ones mentioned in the DHS reply) can be found under the Reports section of its website. DHS has updated those documents in June 2013.

The report further signals (in relation to Article 11 on access) that information on a number of programs providing passengers with information about travelling to the U.S is available online.[30]

Conclusion: The FAQs and the DHS Privacy Policy Document were updated 11 months after the entry into force of the Agreement. The EU team fully concurs with the recommendation of

[27] DHS Privacy Office internal review report, Chapter 2, page 12.
[28] Joint Review Discussion July 8 & 9, 2013.
[29] DHS Privacy Office review report, Overview, page 5.
[30] Ibid., Chapter 6, page 18.

the DHS Privacy Office that a prompt amendment of those documents was needed to meet the transparency requirements under the Agreement and notes with satisfaction that DHS has updated the documents accordingly. Together with other information provided on its website and through notice to passengers via the carriers, there is a wide range of information available on how DHS handles PNR. However, this conclusion should be read together with the conclusion made under 2.2.4 which addresses the need for more transparency on the redress mechanisms available to passengers.

2.1.10. Access, correction/rectification (Articles 11-12)

2.1.10.1. Access (Article 11)

DHS specified that during 1 July 2012 to 31 March 2013, it received 21 606 requests for access to information, of which 16 875 were requests for traveller data. Of those 16 875 requests, 27 came from requesters asking for access to their PNR. Of those 27 requesters, none provided an EU place of birth, citizenship or mailing address.[31]

The DHS Privacy Office reviewed the activities of the CBP Customer Service Center, the CBP Freedom of Information Act (FOIA)/Privacy Act Program and DHS TRIP, because these programs accept requests for access to PNR from individuals regardless of their status within the U.S.. Information on how to submit an access request under these programs is available to passengers online.[32] The DHS Privacy Office internal review report mentions that during 1 July 2012 to 31 March 2013, the CBP Customer Service Centre did not receive specific requests related to PNR. It also indicates that in case a traveller would submit a PNR access request to the CBP Customer Service Centre, the latter would direct the requester to submit a Freedom of Information Act (or FOIA) request or a Privacy Act request.[33]

The report signals that PNR-specific FOIA requests were handled on average within 38 days, which is also the average response time for all CBP FOIA requests. In this respect the report highlights that this is a significant improvement compared to the situation reported on in its 2008 Privacy Report, which signalled that some PNR requests took more than a year to be handled.[34]

Following recommendations made by the DHS Privacy Office in 2008 and 2010, CBP developed "*Processing Instructions for PNR*", including instructions on how to conduct searches in the ATS database in response to a FOIA request for access to PNR. The internal review of these instructions by the DHS Privacy Office revealed that none of the 27 PNR-related access requests were EU related within the definition used by CBP (i.e. a request is EU-related if the requester claims citizenship, a mailing address, or place of birth in the EU). The internal review also revealed that in one instance, personal information of another person contained in the requester's PNR was made available to a requester. This finding has led to a new rule to double check all FOIA responses before they are sent.[35]

The Privacy Office did not find any cases where access to PNR following a FOIA request was refused or restricted.[36]

Conclusion: The CBP tracking system tracks if the request for access is a specific request related to PNR, and tracks if requests are made by individuals that provide an EU place of

---

31 Ibid., Chapter 6, page 19.

32 Http://www.cbp.gocv/xp/cgov/travel/customerservice; http://foia.cbp.gov/palMain.aspx; http://www.dhs.gov/dhs-trip.

33 DHS Privacy Office internal review report, Chapter 6, page 18.

34 Ibid., Chapter 6, page 19.

35 Ibid., Overview, page 6 and Chapter 6, page 19.

36 Ibid., Chapter 6, page 19.

birth, citizenship or mailing address. The processing time of such requests has been greatly improved, as outlined in the review of the DHS Privacy Office. DHS took steps to ensure that only the requester's PNR is included in responses to FOIA requests for access to PNR.

DHS also issued new recommendations on how to search for PNRs in ATS to best meet the requirement under the Agreement and under the FOIA to provide a requester access to his or her PNR.

The above-mentioned changes introduced by DHS in relation to access to PNR should be welcomed and acknowledged.

2.1.10.2.Correction (Article 12)

In its reply to the EU questionnaire DHS reported that it had not received any request to correct, rectify, erase or block PNR.

The DHS Privacy Office internal review report mentions that several options are available to those who want to seek correction of personal information (such as PNR) held by DHS. In case a traveller is not an U.S. citizen or a lawful permanent resident, s/he may request a correction of his or her PNR by filing a Privacy Act Amendment Request through the CBP FOIA Headquarters Office, either online or by mail. A traveller may also file a request for correction by contacting the Assistant Commissioner, CBP Office of Field Operations. Alternatively a traveller may also address him or herself directly to the Office of the DHS Chief Privacy Officer by email or in writing.[37]

Conclusion: Several avenues are available to passengers to seek correction, but until the date of the joint review Article 12 has not been applied to any request for correction of PNR.

2.1.10.3.Redress (except for transparency on redress mechanisms) (Article 13)

The DHS Traveller Redress Inquiry Program (TRIP)[38] provides all individuals an administrative means to seek a resolution for travel-related inquiries including those related to the use of PNR. TRIP provides a redress process for individuals who believe they have been unfairly or incorrectly delayed, denied boarding or identified for additional screening at U.S. airports or other U.S. transportation hubs.

According to DHS, pursuant to the Administrative Procedure Act and Title 49, United States Code, Section 46110, as applicable given the particular facts of a given case, any individual is entitled to petition for judicial review in an U.S. federal court against any final agency action taken by DHS relating to the above-mentioned concerns.

The Privacy Office reviewed the DHS TRIP program and found that during the period 1 July 2012 to 31 March 2013, this program had received over 13 000 inquiries, of which two specifically related to PNR. These inquiries did not involve inquiries from EU individuals.

Conclusion: Until the date of the joint review Article 13 has not been applied as none of the TRIP inquiries involved PNR-related inquiries from EU individuals.

2.1.11. Oversight (Article 14)

The DHS Privacy Office has the authority to investigate and review all programs, such as ATS, and policies for their privacy impact. The DHS Privacy Office internal review report mentions that the Privacy Office *"conducts ongoing oversight of ATS and has conducted*

[37] Ibid.

[38] http://www.dhs.gov/dhs-trip.

formal reviews of the system many times, including PIA and SORN updates and previous PNR Reports".[39]

The report highlights the central role in relation to oversight of the CBP Directive regarding use and disclosure of PNR data. Because of its rules on issues such as maintaining records of access to PNR and records on sharing PNR both within DHS and with Non-DHS users, the Directive provides the framework for auditing and oversight by CBP.

The report observed that during the reporting period the DHS Privacy Office did not receive any complaints related to non-compliance with the current PNR Agreement or any complaints related to a misuse of PNR.[40]

Besides the Privacy Office, other DHS components, such as the CBP Privacy Officer and the CBP Office of Internal Affairs have oversight functions. The CBP Privacy Officer keeps copies of all requests for PNR by Non-DHS users and the correspondence regarding PNR disclosures for audit purposes and maintains a record of access determinations for oversight purposes. As mentioned earlier, the CBP Office of Internal Affairs audits the use of ATS-P to guard against unauthorized use.

Conclusion: The CBP Directive of 2010 on the use and disclosure of PNR was updated in June 2013 to reflect the current PNR Agreement. The EU team concurs with the DHS Privacy Office recommendation to promptly update this Directive, notably in view of the role this document plays in the day-to-day use of PNR by DHS staff. The EU team notes with satisfaction that DHS updated the Directive reflecting the requirements of the Agreement and related PIA and SORN, and that this Directive is available to all DHS staff with PNR access.

The EU team also noted the new task conferred upon the DHS Privacy Office, together with the DHS Office of Civil Rights and Civil Liberties and the DHS Office of the General Counsel, to quarterly review targeting rules used in relation to PNR to ensure that DHS does not use PNR to unlawfully discriminate against individuals. This new task should be welcomed and acknowledged as another important step towards ensuring that PNR meets the purposes as outlined in Article 4 of the Agreement whilst ensuring the protection of civil rights and liberties.

2.1.12. Method of PNR transmission (except for ad hoc "pulls") (Article 15)

Air carriers can provide PNR to DHS electronically via a service provider or they can provide the data directly. Only for very small carriers the data are provided manually to DHS instead of electronically.

According to DHS, out of the 47 air carriers affected by the Agreement, 15 use the "pull" method. Those carriers include EU based and US based air carriers and air carriers based at other countries.

In relation to the requirement under Article 15(4) of the Agreement "*that all carriers shall be required to acquire the technical ability to use the 'push' method not later than 24 months following entry into force of this Agreement*", DHS mentioned that the transition from a "pull" method to a "push" method might be influenced by the introduction of a new transmission standard called PNRGOV, which is being tested by an IATA member. DHS will not make PNRGOV a compulsory standard for air carriers, although the Agreement provides that carriers shall be required to acquire the technical ability to "push" data prior to July 1, 2014. Each of the remaining carriers indicated that they are working towards implementing PNR

[39] Ibid., Chapter 8, page 21.

[40] Ibid.

push. As an alternative to utilizing a service provider that does not have PNR push capability, carriers do have the option of changing to a service provider that already has PNR push capabilities. At the EU team request whether it will be feasible for air carriers to meet the deadline for transition from "pull" to "push" (which is 1 July 2014, i.e. two years after the Agreement entered into force), DHS showed confidence that the remaining air carriers will indeed be in a position to meet this deadline. DHS also mentioned that it welcomes and actively supports the development and use of the common PNRGOV "push" standard within the relevant WCO/ICAO/IATA working party. The EU team underlined the importance of respecting the 1 July 2014 deadline.

The Commission also sent questionnaires to the stakeholders in the air industry to further understand the use of the "push" and "pull" methods under the Agreement.

According to the information provided, DHS continues to have access to PNR held by air carriers via the "pull" method by having access to terminals which provide direct access to airline's reservation system. This was confirmed by DHS during the joint review.

DHS noted that the direct "pull" access is tightly controlled. DHS specified that no staff outside the Customs and Border Protection (CBP) component of DHS has access to PNR in this way, with the exception of 40 staff members working for another component of DHS, namely Immigration and Customs Enforcement (ICE), the investigative agency in DHS tasked with enforcing the U.S.' immigration and customs laws. According to DHS, within CBP only a limited number of staff, i.e. 901, that has access to air carriers' databases. According to DHS the PNR retrieved is logged, and the "pull" access appears in the system as if CBP were an air carrier ("CBP air carrier"). CBP has a workforce of over 58 000 employees, of which 21 180 officers inspect and examine passengers and cargo at over 300 ports of entry.

The DHS Privacy Office internal review report mentions that DHS (CBP) has made significant progress to ensure that airlines "push" PNR to CBP and that as of 22 April 2013 68% of air carriers operating flights between the U.S and the EU has moved to the "push" method, an increase of 20 air carriers since the 2010 review report of the DHS Privacy Office.[41]

CBP is informing those air carriers using the "push" method that it seeks to receive PNR at 96 hours before scheduled flight departure. DHS confirmed that it has started preparations to allow transfer of PNR data starting at 96 hours prior to scheduled departure.

Conclusion: It is recommended to ensure as quickly as possible a full move to the "push" method and in any case by 1 July 2014, as required under Article 15(4) of the Agreement. DHS (CBP) is working with air carriers to implement the "push" method in view of this deadline. As of 1 June 2013, 15 air carriers still use the "pull" method, whereas 32 use the "push" method. This is a considerable improvement compared to the situation on 1 January 2010 (reported in the 2010 joint review report), when only 13 air carriers used the "push" method.

DHS makes substantial efforts for the implementation of the push system internationally through the WCO/ICAO/IATA working party on common PNR standards.

[41] Ibid.

2.1.13. Domestic sharing and onward transfers (Articles 16-17)

2.1.13.1. Domestic sharing (Article 16)

As outlined in its reply to the EU questionnaire, DHS referred to a specific message which appears as part of written understandings entered into with each domestic agency with which individual PNRs are shared.

DHS further indicated that PNRs are shared with other U.S. government authorities only for the purposes of Article 4 of the Agreement, i.e. the requesting agency should perform law enforcement, public security or counterterrorism functions and require the PNRs as part of examinations or investigations undertaken as part of those functions pursuant to their lawful authority.[42]

DHS also outlined that all disclosures of PNR are logged in ATS-P. Because of this logging, it has been established that between 1 July 2012 and 31 March 2013, PNR users proceeded with 589 disclosures.[43] This figure includes all sharing of PNRs outside DHS, so also sharing with foreign agencies under Article 17. Of those 589 disclosures, 15 disclosures resulted from subpoenas or other legally mandated instruments under U.S. law.[44] Another 7 disclosures took place with the Center of Disease Control and Prevention (see also Article 4(2) of the Agreement under 2.1.3). DHS further specified that sometimes it may disclose the same PNR more than once. Also, sometimes there may be more than one individual record in a disclosure. For these reasons the figures represent the number of times DHS disclosed PNR.

DHS has declared that it shares PNR with the U.S. Intelligence Community if there is a confirmed case with a clear nexus to terrorism and always under the terms of the Agreement. During the review period, DHS made 23 disclosures of PNR data to the US National Security Agency (NSA) on a case-by-case basis in support of counterterrorism cases, consistent with the specific terms of the Agreement.

Conclusion: The sharing of PNR with other domestic agencies takes place on a case-by-case basis and concerns the sharing of individual PNRs. Prior to the sharing DHS determines whether the requesting agency has a need to know the information to carry out its functions. The sharing takes place on the basis of written understandings referring to the sensitiveness of the data. The sharing of PNR with other domestic agencies remains limited.

2.1.13.2. Onward transfer (Article 17)

DHS indicated that between 1 July 2012 and 31 March 2013, it shared PNR on a case-by-case basis with two international partners (Canada and the United Kingdom). One case concerned the sharing of extracts of data from 14 PNR[45] with the UK in view of the 2012 Olympics. The other case concerned the sharing of PNR with the Canadian Border Services Agency (CBSA). Sharing with CBSA takes place under an information sharing arrangement in place since 2006 and updated in 2009 and which is designed to ensure that only PNR records with a nexus to terrorism or serious transnational crime are transmitted. DHS requires an express understanding that the recipient will treat PNR as sensitive and confidential, including privacy protections that are comparable to those applied to PNR by DHS, and that it will not provide PNR to any other third party without DHS' prior written authorization. The sharing takes

---

42 Joint Review Discussion July 8 & 9, 2013.

43 Ibid.

44 Ibid.

45 Ibid.

place for specific cases and only after DHS determines that the recipient has a need to know the information to carry out its law functions.[46]

In reviewing the sharing of PNR with foreign agencies, the DHS Privacy Office found that CBP shared PNR with one non-EU international partner pursuant to an existing arrangement and that this sharing was not notified to EU Member States as required under the Agreement. The DHS Privacy Office thus recommends that CBP should provide the DHS Office of International Affairs with notification about such disclosures and that in turn this DHS Office should notify EU Member States as appropriate, in a timely manner and develop a consistent approach on notifications.[47] DHS informed the EU team that it has put protocols in place to improve the information sharing with EU Member States in case of the sharing of EU PNR with its international partners, following the recommendation made in the DHS Privacy Office internal report.

Conclusion: The sharing of PNR with international agencies takes place on a case-by-case basis and concerns the sharing of individual PNRs. Prior to the sharing DHS determines whether the requesting agency has a need to know the information to carry out its functions. The sharing takes place on the basis of written understandings referring to the sensitiveness of the data. ATS logs the sharing, which can be used for auditing purposes.

The sharing of individual PNRs with international agencies is very limited.

Measures beyond the Agreement's requirements

Lastly, DHS also implemented measures that go beyond the Agreements' requirements.

First, DHS foresees a notification to the European Commission within 48 hours of access to sensitive PNRs.

Secondly, DHS has installed a new procedure to quarterly oversee and review the implementation of the ATS travel targeting scenarios, analysis and rules to ensure that they are proportionate to minimize the impact on bona fide travellers' civil rights, civil liberties and privacy, and to avoid unlawful discrimination against travellers.

Conclusion: The EU team welcomes and acknowledges these measures.

2.2. Issues to be further addressed

Despite the implementation of the Agreement, some improvements are necessary in the following areas.

2.2.1. Retention of data – the start of the depersonalization mechanism (Article 8)

In relation to Article 8(1) of the Agreement, the EU team noted that the DHS Privacy Office internal report refers to an automated depersonalisation six months from the last update of a PNR in the ATS. This observation by the DHS Privacy Office triggered some discussion on what is meant in Article 8(1) of the Agreement by "*After the initial six months of this period* (i.e. the five years during which the data are retained in an active database), *PNR shall be depersonalised and masked in accordance with paragraph 2 of this Article*." DHS gave an example of how the depersonalisation in ATS-P works. The example of a depersonalized PNR showed that DHS received the initial PNR of a given passenger on 8 July 2012 (ATS Load Date) and showed 25 July 2012 as the Last ATS Update, meaning that the PNR of that particular passenger was updated for the last time on that date. According to the example the

[46] DHS Privacy Office review report, Chapter 3, page 14.

[47] Ibid., Overview, pages 5-6.

calculation of the depersonalization period started on 25 July 2012, i.e. the depersonalization date in ATS-P is 25 January 2013.

Recommendation: The EU team recommends that the six months period should start as from the day the PNR is loaded in ATS (the so-called ATS Load Date) which is the first day the data are stored in ATS, instead of the current practice, which delays applying the six months period until the last Update of the PNR in ATS.

2.2.2. Method of PNR transmission – ad hoc "pulls" (Article 15)

DHS explained that there are three different reasons why it requires ad-hoc "pulls":

1. Technical reason: the air carrier is not in a position to send the data via the "push" method it normally uses;

2. Threat reason: there is a need to provide PNR between or after the regular PNR transfers in order to respond to a specific, urgent and serious threat;

3. Override reason: in case a flight with no U.S. nexus will land on U.S soil for reasons linked to weather conditions or other unforeseen reasons.

The ATS system does not record the reason why an ad-hoc "pull" is requested, so it is not possible to know how many times an ad-hoc "pull" was requested for each of the three different reasons. DHS specified that in case PNR is accessed for the third reason mentioned above, i.e. for a flight with no U.S. nexus because the flight will land on U.S soil for unforeseen reasons, access is monitored via the override functionality. In such a case a review mechanism is triggered by ATS through sending an email to CBP Headquarters managers, allowing them to monitor and check overrides 24 hours after the override occurred.

The total number of ad-hoc "pulls" in 2011 was 570 401, or 0.72% of the total of PNRs received that year, which was 79 005 866. [48] The total number of ad-hoc "pulls" for 2012 were 243 120, or 0.3% of the total of PNRs received, which was 81 252 544. The total number of ad hoc "pulls" during the first six months of 2013 were 55 886, or 0.13 % of the total of PNRs received during that period, which was 42 164 105. DHS clarified that these numbers refer to individual PNR records and do not include the number of times PNR are pulled in case air carriers still use a "pull" method for regular PNR transfers. These numbers cover the three ways of collecting PNR through the ad hoc "pull" method as outlined above.

DHS further clarified that even in the case where all air carriers affected by the Agreement will use a "push" method for transmitting the data, this would not affect the use by DHS of the ad-hoc "pull". DHS underlined that currently air carriers are not in a position to provide DHS with an ad-hoc "push" service available on a 24 hours, seven days a week basis. Air carriers therefore cannot provide PNR data by way of a "push" method between or after the regular data transfers, in cases of technical failure of their "push" system, or in cases where a flight without U.S. nexus intends to land on U.S. soil for unforeseen reasons. This is the case for all carriers, whether they are European carriers, U.S. carriers or other.

At the request of the EU team to illustrate the application of Article 15(5) in more detail, DHS mentioned that the requests made under this provision are made when the air carrier fails to push the data to CBP due to a carrier system failure. In this instance, CBP pulls the information it is legally authorized to collect. CBP has developed a process whereby the system reviews the number of travellers on a given flight and compares that to the number of PNRs received. When there is a discrepancy, CBP automated systems retrieve the PNR from the air carrier. For example, the automated messages are received from the system when

[48] DHS reply to the EU questionnaire in relation to Article 15 of the Agreement.

PNRs have not been received from an airline or a reservation service provider. The timeframe will vary based on established levels of anticipated volume. Upon receipt of an automated alert, troubleshooting will occur to determine if the issue is due to CBP hardware/software or failure by the airline or the service provider.

In relation to the ad hoc "pulls", the DHS Privacy Office internal review report indicates that during 1 July 2012 to 31 March 2013, on one single occasion, DHS (CBP) requested one retransmission of PNR by an EU-based service provider as the PNR had not been provided timely.[49]

Recommendation: The EU team recommends that particular attention should be paid to the use of the ad hoc "pull" method. It is recommended to DHS, in addition to its current logging of ad hoc "pulls", keeps better records of the reason why the ad hoc "pull" method is applied in each case DHS uses this method, which would allow for a better assessment of the proportionality and a more effective auditing thereof. In this respect it would be welcomed if the discussions in WCO/ICAO/IATA on a common PNRGOV "push" standard also would lead to a common standard for ad hoc "push".

2.2.3. Police, law enforcement and judicial cooperation (Article 18)

DHS explained that it needs to further look at how to exchange information under Article 18, and suggested to further discuss how to increase the use of this Article. DHS suggested addressing this as part of a wider discussion on passenger data, travel trends and travelling threats. DHS underlined that both DHS and CBP maintain dialogues on potential cooperation with Europol and EU Member States interested in using advance traveller information.[50]

The EU team suggested organising a workshop with EU Member States, Europol and other stakeholders to discuss this issue in more detail in order to identify what is needed to increase the sharing of individual PNR and analytical information derived therefrom. DHS welcomed this idea.

Recommendation: The EU team welcomes the DHS Privacy Office recommendation to improve the procedure aimed at notifying to EU Member States in case sharing of EU PNRs between DHS and third countries occurs.

The EU team notes that the level of law enforcement cooperation in the area of sharing of advance traveller information requires more attention. DHS is thus requested to respect its commitment to ensure reciprocity and pro-actively share individual PNRs and analytical information flowing from PNR data with EU Member States and where appropriate with Europol and Eurojust. The EU team suggested organising a workshop to explore ways on how to improve this cooperation

2.2.4. Redress – transparency on redress mechanisms (Article 13)

It is explained under 3.1.3 that the use and analysis of PNR data, in particular under the Immigration Advisory Program and the Regional Carriers Liaison Groups Program, may contribute to a recommendation to deny boarding. It is also noted the Secure Flight Program and the No-Fly List as its essential part are not covered by the Agreement. The different programmes and different DHS agencies' involved may make it difficult for those denied boarding to understand how to challenge this decision.

Recommendation: Taking into account the complex interaction between the different programs using PNR data, the EU team sees a need to provide more transparency on the

[49] DHS Privacy Office internal review report, Chapter 5, page 18.

[50] Joint Review Discussion July 8 & 9, 2013.

possible interrelation of the various programs and in particular on the redress mechanisms available under U.S. law. Such transparency should allow passengers who are not U.S. citizens or legal residents to challenge DHS decisions related to the use of PNR data, in particular when the use of such data has led to a decision to recommend the denial of boarding by carriers.

3. CONCLUSIONS

The EU team finds that the joint review mechanism is a valuable tool for the assessment of the compliance of DHS with the Agreement. It enabled the EU team to witness how the data is used in practice and to have some direct exchanges with targeters, analysts and other officials who use PNR data.

The EU team also finds that DHS implements the Agreement in accordance with the terms of the Agreement. DHS respects its obligations as regards the access rights of passengers and has a regular oversight mechanism in place to guard against unlawful non-discrimination. It is especially important to note that the U.S. has transposed its commitments towards the EU into domestic rules through the publication of a System of Records Notice in the U.S. Federal Register.

While it is acknowledged that the implementation of some commitments is technically and operationally challenging, especially as regards the implementation of the push method, DHS should intensify its efforts to ensure that all carriers use the push method by 1 July 2014 and continue to actively working in international fora for an overall resolution of this issue, including finding a common standard for ad hoc “push”.

A number of recommendations are made to DHS which appear in Chapter 3 above. They relate to the start of the depersonalisation mechanism, the use of the ad hoc “pull” method, the redress mechanisms and the need to further improve implementation of the reciprocity commitment on sharing individual PNRs and analytical information flowing from PNR data with Members States, Europol and Eurojust.

It is proposed to organise the next joint review of the Agreement during the first half of 2015.

ANNEX A
EU QUESTIONNAIRE AND DHS REPLIES

A. QUESTIONS OF A GENERAL NATURE

Because the current Agreement replaced the Agreement of 2007, a number of questions were raised in connection to the transition from the old to the new Agreement.

Question: *Has the transition from the 2007 Agreement to the 2012 Agreement given rise to any particular difficulties?*

Response: No.

Question: *Are all mechanisms required to properly implement the Agreement, in particular those aimed at implementing the safeguards, in place and operating satisfactorily*?

Response: As of June 18, 2013, all technological, legal, procedural and policy mechanisms are in place to secure and appropriately process the data currently held consistent with the agreement. By July 1, 2017, a means for transferring data from active to dormant storage will be added. Pursuant to the agreement data acquired on the first day of operation of the agreement, July 1, 2012, is scheduled to transfer to a dormant state.

Question: *Have any specific incidents occurred during the first year of implementation of the Agreement?*

Response: No privacy incidents pursuant to Article 5, paragraphs 3 and 4 occurred during the first year of implementation.

B. SCOPE

B.1. The relevant Commitment of the U.S.

The scope of the Agreement is expressed in Article 2 of the Agreement. It states that:

'*1. PNR, as set forth in the Giudelines of the International Civil Aviation Organisation, shall mean the record created by air carriers or their authorised agents for each journey by on or behalf of any passenger and contained in carriers' reservation systesm, departure control systems, or equivalent systems providing similar functionality (collectively referred to in this Agreement as 'reservations systems'). Specifically, as used in this Agreement, PNR consists of the data types set forth in the Annex to this Agreement ('Annex').'*

'2. This Agreement shall apply to carriers operating passenger flights between the European Union and the United States.'

'3. This Agreement shall also apply to carriers incorporated or storing data in the European Union and operating passenger flights to or from the United States.'

B.2. The relevant written reply of DHS

Question*: Is the mechanism to filter out flights with no U.S. nexus still in place to ensure that the PNR data received regards solely flights with an U.S. nexus? Has this mechanism been audited and if so, which conclusions have been drawn?*

Response: Yes, the filter mechanism is still in place. This mechanism was reviewed by DHS Privacy during an internal review in May 2013; a report of that review was completed in July 2013.

Question: *Is the overriding functionality (operational since October 2009) still in place? If so, has it been audited and if so, how many audits have taken place and which conclusions have been drawn?*

Response: Yes, the overriding functionality is still in place. This functionality was reviewed by DHS Privacy during an internal review in May 2013; a report of that review was completed in July 2013. Each override is reviewed the day after the override occurs at CBP Headquarters to determine the validity for each occurrence.

Question: *How is access to this functionality regulated?*

Response: This functionality is limited by user access controls. Users seeking access to perform overrides must first be sponsored by a manager, who validates the user's need to access the override functionality prior to granting access to the user's account.

Question: *Is the override functionality still an exclusive pull mechanism? How does it relate to the agreed push method under Article 15?*

Response: Airline service providers have not provided an override push alternative that meets DHS/CBP's operational needs, as a result, all overrides continue to be via a pull of specific flight data.

B.3. DHS Privacy Office review report

The Privacy Office interviewed staff of the National Targeting Center and saw live demonstrations of how CBP has programmed ATS-P to use flight numbers and airport codes to identify flights with a U.S. nexus as requested under Articles 2(2) and (3).

The report further mentions that in case a system user seeks to use the override mechanism to get access to a flight without a clear U.S. nexus, a warning box appears informing that person (i) that s/he has to provide a justification for the request, (ii) affirm that s/he is authorized to access the PNR in question and (iii) that s/he understands CBP policies regarding the override mechanism. In addition, the report signals that the day following the use of the override mechanism, an email notice is sent to a group of managers to ensure appropriate use of this mechanism, allowing to identify any misuse of PNR and to recommend remedial training and/or suspension of system access.

The report mentions that during the review period (1 July 2012-31 March 2013), a total of 192 overrides were implemented. In three cases CBP managers could not readily determine the justification for the use of the override mechanism, in which case they sought clarification from the users and found that each of the three overrides were justified. Each officer received a reminder of the policy on PNR access and use.

C.PROVISION OF PNR

C.1. The relevant Commitment of the U.S.

The provision of PNR is regulated in Article 3 of the Agreement. It states that:

'*The Parties agree that carriers shall provide PNR contained in their reservation systems to DHS as required by and in accordance with DHS standards and consistent with this Agreement. Should PNR transferred by carriers include data beyond those listed in the Annex, DHS shall delete such data upon receipt.'*

C.2. The relevant written reply of DHS

Question: *Is the mechanism to filter out PNR data beyond those listed in the Annex to the Agreement still in place? Has this mechanism been audited and if so, which conclusions have been drawn?*

Response: Yes, the filter mechanism is still in place. This mechanism was most recently reviewed by DHS Privacy during an internal review in May 2013; a report of that review was completed in July 2013.

Question: *Has DHS become aware of any additional type of PNR information that may be available and required for the purposes set out in Article 4 and if so, which?*

Response: No.

Question: *Has DHS become aware of any type of PNR information that is no longer required for the same purposes and if so, which?*

Response: No.

Question: *Has DHS ever used information held in PNR beyond those listed in the Annex, including sensitive information, and if so, how many times and for what reasons?*

Response: No.

C.3. DHS Privacy Office review report

Based on the review of a randomly selected PNR, the DHS Privacy Office determined that *"no PNR data outside of the 19 PNR types listed in the Annex to the 2011 Agreement was received"*[51].

D.PURPOSE LIMITATION

D.1. The relevant Commitment of the U.S.

The purpose limitation of the use of PNR data by DHS is expressed in Article 4 of the Agreement. It states that:

'1. The United States collects, uses and processes PNR for the purposes of preventing, detecting, investigating, and prosecuting:

(a) Terrorist offences and related crimes, including:

(i) Conduct that —

1. involves a violent act or an act dangerous to human life, property, or infrastructure; and

2. appears to be intended to —

a. intimidate or coerce a civilian population;

b. influence the policy of a government by intimidation or coercion; or

c. affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking;

(ii) Activities constituting an offence within the scope of and as defined in applicable international conventions and protocols relating to terrorism;

(iii) Providing or collecting funds, by any means, directly or indirectly, with the intention that

[51] DHS Privacy Office review report, Chapter 4, page 16.

they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the acts described in subparagraphs (i) or (ii);

(iv) Attempting to commit any of the acts described in subparagraphs (i), (ii), or (iii);

(v) Participating as an accomplice in the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

(vi) Organising or directing others to commit any of the acts described in subparagraphs (i), (ii), or (iii);

(vii) Contributing in any other way to the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

(viii) Threatening to commit an act described in subparagraph (i) under circumstances which indicate that the threat is credible;

(b) Other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature.

A crime is considered as transnational in nature in particular if:

(i) it is committed in more than one country;

(ii) it is committed in one country but a substantial part of its preparation, planning, direction or control takes place in another country;

(iii) it is committed in one country but involves an organised criminal group that engages in criminal activities in more than one country;

(iv) it is committed in one country but has substantial effects in another country; or

(v) it is committed in one country and the offender is in or intends to travel to another country.

2. PNR may be used and processed on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court.

3. PNR may be used and processed by DHS to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination.

4. Paragraphs 1, 2, and 3 shall be without prejudice to domestic law enforcement, judicial powers, or proceedings, where other violations of law or indications thereof are detected in the course of the use and processing of PNR.'

D.2. The relevant written reply of DHS

Question: *Have PNR data been used also under the Regional Carriers Liaison Groups Program and if so, for what purposes? Has this Program been audited and if so, which conclusions have been drawn? What are the differences between the Secure Flight Program and this Program?*

Response: DHS Regional Carrier Liaison Groups (RCLGs) fall under the National Targeting Center-Passenger (NTC-P) Pre-Departure (PD) program and serve as liaisons between NTC-P and carriers serving the U.S. They have a working relationship with the carriers and have been given the responsibility of covering each airport not currently serving as an Immigration Advisory Program (IAP) location. Persons warranting further scrutiny are identified by NTC-P using the Automated Targeting System-Passenger (ATS-P), which leverages both PNR and Advance Passenger Information System (APIS) information to generate referrals for RCLGs

to investigate. The RCLGs will send carriers requests for denial of boarding, additional information to further assist in vetting a traveler, document validation, and enhanced screening of the traveler by airline security prior to boarding the flight. The RCLGs' targeting focus is mainly on alien smuggling and criminal fraud detection.

Secure Flight is a Transportation Security Administration (TSA) run program that identifies domestic and international travellers on terrorist watch lists and designates them for denial of boarding or additional physical screening prior to boarding depending on the specific circumstances of the background case. While CBP and TSA coordinate for identity resolution when appropriate, CBP and TSA systems are separate and work on two different platforms. The Secure Flight system does not have access to the PNR and instead, airlines send UN/EDIFACT PAXLIST messages to Secure Flight via a DHS server with a very limited and some very limited itinerary information. Under the system of records notice (SORN) titled Department of Homeland Security/Transportation Security Administration 019 (DHS/TSA–019), Secure Flight Records, for the passenger and non-traveler screening program known as Secure Flight, the data is stored in the Secure Flight database for no more than seven days after completion of the last leg of the individual's directional travel itinerary, if there are no positive results with the automated matching process. Potential matches are stored for seven years and confirmed matches are stored for 99 years in accordance with current retention schedules.

RCLG and Secure Flight differ in their scope. Secure Flight is limited to identifying and mitigating the risk associated with terrorist travel. As noted in the May 31, 2010 letter from former DHS Chief Privacy Officer Mary Ellen Callahan to Reinhard Priebe, the RCLG covers all security and admissibility issues, which can include terrorism, crime, immigration, health and other issues – although PNR supports this initiative solely for the purposes of preventing and detecting terrorism and crime that is transnational in nature.

RCLG members with access to PNR are subject to the same use audits as any other PNR user.

Question: *Have PNR data been used also under the Immigration Advisory Program and if so, for what purposes? Has this Program been audited and if so, which conclusions have been drawn? What are the differences between the Regional Carriers Liaison Groups Program, the Secure Flight Program and this Program?*

Response: CBP Officers deployed at foreign airports as part of the Immigration Advisory Program (IAP) rely on the centralized analysis of PNR by ATS-P to identify travellers to interview prior to departure and have similar access to raw PNR as other CBP officers. Similar to its support of port of entry operations, NTC-P uses ATS-P, which leverages both PNR and APIS information, to generate lists of passengers warranting further scrutiny (usually in the form of an interview prior to departure) for each IAP team, each day. IAP Officers responding to the NTC-P generated list may access the underlying PNR as part of the case adjudication.

IAP, RCLG and Secure Flight share similar goals of identifying the proper handling of travelers who are more likely to pose a risk to the aircraft or United States, but each functions separately and with unique goals. The primary difference between IAP and RCLG is the method of human intervention. Both IAP and RCLG support all admissibility operations, although as in the previous question PNR only supports counterterrorism operations and to identify crime that is transnational in nature. At IAP locations, a CBP Officer may personally interview the traveller prior to boarding whereas the RCLG provides similar benefits through liaison with the airlines as described in the previous question. Secure Flight is a Transportation Security Administration (TSA) program that identifies domestic and

international travellers on terrorist watchlists that either require additional physical screening by airport security personnel prior to boarding or who are banned from boarding aircraft in U.S. airspace. In Secure Flight, human intervention generally occurs prior to the issuance of a boarding pass at the time of check-in for potential matches to the watchlist, the results of which are communicated to the carrier through automated means within the Secure Flight system. CBP and TSA coordinate for identity resolution when appropriate, CBP and TSA systems are separate and work on two different platforms.

IAP has been audited through the Government Accountability Office (GAO) and CBP Headquarters site visits of overseas locations. IAP managers at CBP Headquarters conduct a daily review of advance target confirmation and boarding recommendations issued to carriers. Joint reviews are also conducted periodically with host governments, airline security officials and/or the U.S. Embassy to assess relationships and operational practices. The Secure Flight Program has been audited by both the GAO and the DHS Inspector General.

***Question**: In case the override functionality mentioned under Article 2 has been audited, which conclusions have been drawn in particular as regards accessing PNR data from offloaded passengers that have not boarded an air craft towards the U.S. as they have been identified by DHS to be inadmissible prior to boarding through its Immigration Advisory Program (see also the question under Article 4.3)?*

Response: DHS/CBP can begin receiving PNR for passengers 96 hours before the flight, well in advance of an admissibility recommendation by IAP, which generally occurs 24 hours before a flight.

***Question**: Are the data collected for the purposes of the Secure Flight Program still retained in the SFP database? If so, does DHS consider the possibility to retain the data only once, i.e. in the ATS-P database?*

Response: Data that is collected for the purposes of the Secure Flight Program is still retained in the Secure Flight database. However, the Secure Flight system does not utilize PNR, instead airlines send UN/EDIFACT PAXLIST messages to Secure Flight with a very limited amount of passenger data to include name, date of birth, gender, passport information, and some very limited itinerary information via DHS router. This data is specifically enumerated in the pplicable regulation (referred to as “Secure Flight Passenger Data”). Under the system of records notice (SORN) titled Department of Homeland Security/Transportation Security Administration 019 (DHS/TSA–019), Secure Flight Records, for the passenger and nontraveler screening program known as Secure Flight, the data is stored in the Secure Flight database for no more than seven days after completion of the last leg of the individual’s directional travel itinerary, if there are no positive results with the automated matching process. Potential matches are stored for seven years and confirmed matches are stored for 99 years in accordance with current retention schedules.
DHS notes that in its February 2010 report form the 2010 Joint Review the Commission recommended DHS consider whether it is necessary to “duplicate” data in ATS-P and Secure Flight. DHS does not consider the retention of Secure Flight Passenger Data to be the “duplication” of data, but a unique collection that is processed pursuant to the needs of the Secure Flight Programs. Neither ATS-P or Secure Flight repurposed data for objectives outside of their given legal and regulatory basis (see the applicable System of Records Notices and Privacy Impact Assessments at www.DHS.gov/privacy).

Further, because of the seven day retention period associated with Secure Flight, DHS believes the risk associated with storing basic identifiers in multiple databases to be minimal in comparison to the cost and operational disruption of reengineering operations across

multiple operational agencies of the Department. DHS notes, its structure is not fundamentally different than the European Union's own IT infrastructure where common data elements are processed by the Schengen Information System, Visa Information System and eventually the proposed Entry Exit System and Registered Traveller Program. Further, DHS has worked to minimize any impact on carrier operations of separated storage. As a result, DHS is not currently considering limiting retention to one database.

Secure Flight is outside the scope of the 2011 PNR Agreement.

***Question**: For how many case-by-case situations PNR data have been used?*

Response: DHS has disclosed PNR for case-by-case situations under Article 4, Paragraph 2 seven times since July 1, 2012.

***Question**: How does this provision relate to the use of PNR data from passengers that have not boarded an air craft towards the U.S. as they have been identified by DHS to be inadmissible prior to boarding through its Immigration Advisory Program?*

Response: This provision supports the operations of the IAP by acknowledging that at locations where it is present many of the actions that would occur at the border may occur prior to departure at the foreign airport where IAP is stationed. As noted in response to previous questions, CBP receives the PNR upwards of 96 hours in advance of the IAP officer interaction with the traveller, the NTC-P determines which travellers IAP team members should interview and provides the IAP team a list 24 hours in advance. When a hit is received by NTC-P and deemed worthy of a referral to IAP, it is placed in the system and added to a referral spread sheet. Prior to the start of the day, the IAP officers review these referral sheets and work through the targets to determine their workload. Much of the admissibility opinions being given by the IAP officers are based on the information provided by NTC-P and are not directly related to PNR.

D.3. DHS Privacy Office review report

The report mentions that "*between July 1, 2012 and April 30, 2013, 0.002 percent of individuals traveling to the U.S. were identified by ATS for additional attention based primarily on analysis of their PNR. These individuals were identified during an investigation related to terrorism or other serious crime as defined in Article 4 of the 2011 Agreement.*"[52]

The Report also mentions that the Privacy Office reviewed a random sample of 13 disclosures of PNR provided by DHS (CBP) to other U.S. government agencies between 1 July 2012 and 31 March 2013, of which seven concerned the sharing of PNR with the U.S Center for Disease Control "*to coordinate appropriate responses to health concerns associated with international air transportation*". According to the Privacy Office these disclosures are within the scope of the purposes defined in Article 4 of the Agreement[53]. Article 4(2) allows the use and processing of PNR "*on a case-by-case basis where necessary [….] for the protection of vital interests of any individual [….]*".

Following a question by the EU team if the Privacy Office had seen any use of Article 4(4) of the Agreement during this period, the Privacy Office replied that it had not seen such use.

52 Ibid., Chapter 2, pages 11-12.

53 Ibid., Chapter 3, page 14.

E. DATA SECURITY

E.1. The relevant Commitment of the U.S.

The data security safeguards are laid down in Article 5 of the Agreement. It states that:

'1. DHS shall ensure that appropriate technical measures and organisational arrangements are implemented to protect personal data and personal information contained in PNR against accidental, unlawful, or unauthorised destruction, loss, disclosure, alteration, access, processing or use.

2. DHS shall make appropriate use of technology to ensure data protection, security, confidentiality and integrity. In particular, DHS shall ensure that :

(a) encryption, authorisation and documentation procedures recognised by competent authorities are applied. In particular, access to PNR shall be secured and limited to specifically authorised officials;

(b) PNR shall be held in a secure physical environment and protected with physical intrusion controls; and

(c) a mechanism exists to ensure that PNR queries are conducted consistent with Article 4.

3. In the event of a privacy incident (including unauthorised access or disclosure), DHS shall take reasonable measures to notify affected individuals as appropriate, to mitigate the risk of harm of unauthorised disclosures of personal data and information, and to institute remedial measures as may be technical practicable.

4. Within the scope of this Agreement, DHS shall inform without undue delay the relevant European authorities about cases of significant privacy incidents involving PNR of EU citizens or residents resulting from accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, or any unlawful forms of processing or use.

5. The United States confirms that effetcive administrative, civil, and criminal enforcement measures are available under U.S. law for privacy incidents. DHS may take disciplinary action against persons responsible for any such proivacy incident, as appropriate, to include denial of system access, formal reprimands, suspenion, demotion, or removal from duty.

6. All access to PNR, as well as its processing and use, shall be logged or documented by DHS. Logs or documentation shall be used only for oversight, auditing, and system maintenance purposes or as otherwise required by law.'

E.2. The relevant written reply of DHS

***Question**: Which appropriate technical and organisational measures have been implemented to protect personal data and personal information contained in PNR?*

Response: Physical and procedural safeguards are in place in ATS, including physical security, access controls, data separation and encryption, audit capabilities, and accountability measures.

Additionally, all PNR users must undergo privacy training and obtain approval from their supervisor and the ATS system owner before gaining role-based access to ATS. Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. Notices upon sign-on remind users that they are accessing a law enforcement sensitive database for official use only and that an improper disclosure of PII contained in the system could constitute a violation of the Privacy Act. The notice also states that information contained in the system is subject to the third party rule and may not be disclosed to other

government agencies without the express permission of CBP. Access to ATS-P and PNR is limited to those individuals with a need to know the information in order to carry out their official duties. Furthermore, access to PNR is further controlled by providing each user only those accesses required to perform his or her job. Within the ATS-P database, audit trails of what information has been accessed by whom are maintained and used to support internal audits to ensure compliance with the stated purposes of the system. All ATS-P users are required to undergo regular training, including annual privacy training, to maintain their system access.

A system security plan for ATS was completed and an Authority to Operate (ATO) was granted to ATS for three years, on January 21, 2011.

***Question**: Which encryption, authorisation, logging and documentation procedures are applied by DHS?*

Response: Users may only access PNR through ATS-P, which can only be accessed through a webbased user interface over the DHS infrastructure or remotely through secure-encrypted mobile devices for certain CBP officers in foreign locations and at Ports of Entry. Within the ATS-P database, audit trails of what information has been accessed by whom are maintained and used to support internal audits to ensure compliance with the stated purposes of the system.

***Question**: Which measures are in place to ensure limited access to specifically authorised officials?*

Response: Each user's access to PNR is reviewed twice per year by the supervisor who authorized the role, and validated by a CBP Headquarters Manager.

***Question**: In what secure physical environment is PNR being held and which physical intrusion controls are implemented to protect PNR?*

Response: PNR records are stored electronically in an encrypted system or on paper in secure facilities in a locked drawer behind a locked door.

***Question**: Which mechanism exists to ensure that PNR queries are conducted consistent with Article 4?*

Response: The mechanism that exists to ensure that PNR queries are conducted consistent with the PNR uses permitted under Article 4 of the 2011 Agreement is the CBP Directive regarding use and disclosure of PNR data. The updated Directive reflecting the 2011 Agreement is currently available under the Help tab in ATS-P and outlines the appropriate use, handling, and disclosure of PNR data and provides a framework for granting access to PNR to authorized personnel within DHS and for sharing PNR with DHS's domestic and international mission partners, as appropriate. The updated Directive has been distributed throughout CBP and to other DHS PNR users with updated field guidance.

CBP has developed policy, in the form of this directive, outlining the purposes for which PNR may be used. CBP also maintains a process of user access control, by which a user requiring access to PNR for his or her official duties must obtain prior supervisory approval before receiving access. Each user's level of access is also validated twice per year by supervisory and management review. CBP's use of PNR in scenario-based targeting rules is also reviewed on a quarterly basis by DHS oversight offices, including the Chief Privacy Officer, the Civil Rights/Civil Liberties Officer, and the Office of General Counsel.

***Question**: Which reasonable measures are taken to notify affected individuals in the event of a privacy incident? Have any such incidents occurred and if so, how many and what was their*

nature (unauthorised access, unauthorised disclosure, any other form of privacy incident)? Which remedial measures have been taken?

Response: There have been no significant privacy incidents since the entry into force of the 2011 PNR Agreement.

***Question**: How many cases of significant privacy incidents were reported by DHS to EU authorities involving PNR of EU citizens or residents? Has any such incident occurred without such reporting?*

Response: No incidents have been reported by DHS to EU authorities because there have been no significant privacy incidents and no unauthorized access or disclosure.

***Question**: What effective administrative, civil and criminal enforcement measures are implemented under U.S. law for privacy incidents?*

Response: Administrative, civil, and criminal enforcement measures are available under U.S. law for unauthorized disclosure of U.S. records, including PNR. Relevant provisions include but are not limited to:

- The Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030) allows individuals to bring a civil action in court for actual damages, and in some cases punitive damages plus attorney fees, when that individual's personal information held on a U.S. government computer system, including the Automated Targeting System-Passenger (ATS-P) that holds PNR, has been improperly accessed, causing a certain type of harm.
- The Electronic Communications Privacy Act (18 U.S.C. 2710 et seq. and 18 U.S.C. 2510 et seq.) allows any person to bring a civil action in court for actual damages, and in some cases punitive damages plus attorney fees, when that person's stored wire or electronic communications are improperly accessed or disclosed, or when that person's wire, oral, or electronic communications are improperly intercepted or disclosed.
- 18 U.S.C. § 641 – Public money, property or records provides for criminal fines and imprisonment of persons convicted of stealing or conversion of U.S. government records to his or her use, or the sale or disposal of such record without authority.
- 18 U.S.C. § 1030 – provides for criminal fines and imprisonment for fraud and related activity involving unauthorized access to a U.S. government computer.
- 19 C.F.R. § 103.34 – Provides for sanctions (including administrative and criminal, where appropriate) for improper disclosure of confidential information contained in Customs documents.

E.3.DHS Privacy Office review report

Article 5(2) requires DHS to make appropriate use of technology to ensure data protection, security, confidentiality and integrity. The report indicates that, in order to promote data integrity, "*DHS provides individuals with the means to seek correction or rectification of their PNR*".[54]

With regards to accountability measures, the report outlines in more detail the layers of oversight ensuring compliance with data security requirements. The report mentions that with regard to the risk of unauthorized access or use of PNR, "*CBP's Office of Internal Affairs*

[54] Ibid., Chapter 5, page 17.

audits the use of ATS and the CBP Office of Intelligence and Investigation Liaison (OIIL) verifies that users with PNR access are authorized to retain that access. To guard against unintended or inappropriate disclosure of PNR data, OIIL conducts audits of al disclosures within and outside DHS. The CBP Privacy Office oversees the results of these audits and takes appropriate corrective action if warranted. OIIL, in coordination with CBP's Office of Field Operations (OFO) and Office of Information and Technology (OIT), is responsible for maintaining updated technical/security procedures by which PNR is accessed by DHS and Non-DHS Users. CBP completed a security Plan for ATS and in 2011 received its certification and accreditation (C&A) under the Federal Information Security Management Act (FISMA) and Authority to Operate ATS for three years."[55]

The report also mentions that between 1 July 2012 and 31 March 2013 the DHS Privacy Office did not receive reports of the loss or compromise of EU PNR.[56]

F. USE OF SENSITIVE DATA

F.1. The relevant Commitment of the U.S.

The use of sensitive data is regulated in Article 6 of the Agreement. It states that:

'1. To the extent that PNR of a passenger as collected includes sensitive data (i.e. personal data and information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning the health or sex life of the individual), DHS shall employ automated systems to filter and mask out sensitive data from PNR. In addition, DHS shall not further process or use such data, except in accordance with paragraphs 3 and 4.

2. DHS shall provide to the European Commission within 90 days of the entry into force of this Agreement a list of codes and terms identifying sensitive data that shall be filtered out.

3. Access to, as well as processing and use of, sensitive data shall be permitted in exceptional circumstances where the life of an individual could be imperilled or seriously impaired. Such data may be exclusively accessed using restrictive processes on a case-by-case basis with the approval of a DHS senior manager.

4. Sensitive data shall be permanently deleted not later than 30 days from the last receipt of PNR containing such data by DHS. However, sensitive data may be retained for the time specified in U.S. law for the purpose of a specific investigation, prosecution or enforcement action.'

F.2. The relevant written reply of DHS

***Question**: Which automated systems does DHS employ to filter and mask out sensitive data from PNR?*

Response: DHS/CBP has developed automated processes within the ATS-P database to filter, mask out, and delete sensitive data from PNR.

***Question**: How many times DHS staff accessed, used and/or processed sensitive data and for which type of circumstances?*

Response: Three; all were conducted solely for the purpose of ensuring the proper functionality of accessing sensitive data in the production system.

---

55 Ibid, Chapter 7, pages 20-21.

56 Ibid., Chapter 7, page 21.

***Question**: In case such data were used, how useful have they been in preventing the life of an individual to become imperilled or seriously impaired?*

Response: Not applicable; please see response above.

***Question**: Which restrictive processes are applied by DHS, and what are the experiences with the role of the DHS senior manager providing approval?*

Response: The only cases of access to sensitive data to date were solely for the purpose of ensuring the proper functionality of accessing sensitive data in the production system.

***Question**: Which measures have been taken by DHS to ensure that the data are permanently deleted after no more than 30 days from the last receipt of PNR containing such data?*

Response: DHS/CBP has developed automated processes within the ATS-P database to delete sensitive data from PNR in accordance with the terms of the agreement.

***Question**: In how many cases sensitive data have been retained for a time specified in U.S. law for specific investigation, prosecution or enforcement actions?*

Response: No sensitive data has been retained for investigation, prosecution or enforcement actions.

F.3. DHS Privacy Office review report

The report indicates that the Privacy Office observed that sensitive terms within the 19 PNR data elements were appropriately masked. DHS also demonstrated to the Privacy Office that "*certain codes and terms that may appear in a PNR have been identified as "sensitive" and are masked by ATS-P to prevent routine viewing*".[57] The report also mentions that "*Any retrieval of sensitive PNR through ATS-P is recorded by the system and ATS generates a daily email informing CBP management whether or not any sensitive data elements have been accessed*".[58]

In relation to the automatic filtering by ATS of sensitive PNR codes and terms, the Privacy Office reviewed samples of raw PNR from seven randomly-selected cases. The report states that "*Each PNR showed blocked data fields where a sensitive term that may have been included in an air carrier's record was hidden from DHS view*".[59]

G. AUTOMATED INDIVIDUAL DECISIONS

Article 7 of the Agreement

The EU team did not raise questions as regards Article 7 of the Agreement on "automated individual decision", as it is clear from the explanations of how the ATS-P functions as outlined in the SORN and the PIA that DHS does not take decisions producing significant adverse actions affecting the legal interests of individuals on the sole basis of an automated processing and use of PNR.

The DHS Privacy Office review report mentions that it received statistics from CBP (DHS) showing its use of PNR. The report mentions that the CBP Directive "*requires that no decisions concerning travelers are to be based solely on the automated processing and use of PNR*".[60]

---

57 Ibid., Chapter 4, page 16.
58 Ibid.
59 Ibid.
60 Ibid., Chapter 3, page 13.

Article 7 seems to be fully respected and implemented.

H. DATA RETENTION

H.1. The relevant Commitment of the U.S.

The periods of data retention is expressed in Article 8 of the Agreement. It states that:

'1. DHS retains PNR in an active database for up to five years. After the initial six months of this period, PNR shall be depersonalised and masked in accordance with paragraph 2 of this Article. Access to this active database shall, unless otherwise permitted by this Agreement, be restricted to a limited number of specifically authorised officials.

2. To achieve depersonalisation, personally identifiable information contained in the following PNR data types shall be masked out:

(a) name(s);

(b) other names on PNR;

(c) all available contact information (including originator information);

(d) general remarks, including other supplementary information (OSI), special service information (SSI), and special service request (SSR); and

(e) any collected Advance Passenger Information System (APIS) information.

3. After this active period, PNR shall be transferred to a dormant database for a period of up to ten years. This dormant database shall be subject to additional controls, including a more restricted number of authorised personnel, as well as a higher level of supervisory approval required before access. In this dormant database, PNR shall not be repersonalised except in connection with law enforcement operations and then only in connection with an identifiable case, threat or risk. As regards the purposes as set out in Article 4(1)(b), PNR in this dormant database may only be repersonalised for a period of up to five years.

4. Following the dormant period, data retained must be rendered fully anonymised by deleting all data types which could serve to identify the passenger to whom PNR relate without the possibility of repersonalisation.

5. Data that are related to a specific case or investigation may be retained in an active PNR database until the case or investigation is archived. This paragraph is without prejudice to data retention requirements for individual investigation or prosecution files.

6. The Parties agree that, within the framework of the evaluation as provided for in Article 23(1), the necessity of a 10-year dormant period of retention will be considered.'

H.2. The relevant written reply of DHS

***Question**: Which measures are in place to ensure the depersonalising and masking of the data sets listed under paragraph 2?*

Response: DHS/CBP has developed automated processes within the ATS-P database to depersonalize PNR, and has also developed manual processes to allow designated users to request permission to repersonalize PNR.

***Question**: What is the number of officials specifically authorised to access the active database?*

Response: As of May 1, 2013, there were 12,448 users with access to the active PNR database. This figure is roughly one quarter (25%) of all ATS-P users (approximately 40,000).

***Question**: Has paragraph 5 been applied in practice yet?*

Response: DHS/CBP has developed automated processes within the ATS-P database to identify PNR linked to law enforcement cases or investigations. No data is scheduled to be transferred to a dormant database until July 1, 2017.

***Question**: What are the data retention requirements under U.S. law that apply to this paragraph?*

Response: This paragraph is codified in the System of Records Notice for the Automated Targeting System (DHS/CBP-006 - Automated Targeting System May 22, 2012 (77 FR 30297)), as follows:

Information maintained only in ATS that is linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (i.e., threats; flights, individuals, and routes of concern; or other defined sets of circumstances) will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

The specific retention period in the active system for any data tied to a specific case or investigation would need to be determined upon its identification. However, this provision does not become relevant until data must start being transferred to a dormant database on July 1, 2017.

H.3. DHS Privacy Office review report

The report mentions that the Privacy Office has reviewed depersonalized records stored between 1 July and 1 September 2012 and the process to repersonalise those records. The report indicates that the ATS-P is programmed to "*automatically depersonalize PNR six months from its last use. Records older than six months reviewed by the Privacy Office showed only the record locator, reservation system, date record was created, load and update dates, and the itinerary. An affirmation of depersonalization and the date of depersonalization are also included in the depersonalized record*".[61]

The report further mentions that "*any use of repersonalized PNR is with supervisory approval and only in connection with law enforcement operations that include an identifiable case, threat, or risk*".[62]

In relation to the requirement in Article 8(1) to restrict access to the active database to a limited number of specifically authorised officials, the report signals that "*each user's level of access is validated twice a year by supervisory and management review. This process includes seeking supervisors' verification that users have continued need for access*". In case the user is a DHS official working for another DHS component than CBP, the report mentions that CBP receives "*written confirmation from that other DHS component that a DHS employee requires access to PNR to perform his or her official duties*". The Privacy Office reviewed the sharing and use of PNR within DHS and found that this is done "*on a need-to-know basis and for the purposes specified in Article 4 of the Agreement*".[63]

61 Ibid., Chapter 4, page 16.
62 Ibid., Chapter 3, page 13.
63 Ibid., Chapter 3, page 14.

The Privacy Office also reviewed biannual reports of CBP's ATS-P User Access Verification audits from July 2010 to September 2012. According to the DHS Privacy Office, these audits demonstrated that "*CBP has modified user access to ATS-P, adjusted user roles, and even withdrawn user access completely, as appropriate, depending on the results of field and headquarters review*".[64]

I. NON-DISCRIMINATION

I.1. The relevant Commitment of the U.S.

A non-discrimination clause is laid down in Article 9 of the Agreement. It states that:

'The United States shall ensure that the safeguards applicable to processing and use of PNR under this Agreement apply to all passengers on an equal basis without unlawful discrimination.'

I.2. The relevant written reply of DHS

***Question**: What measures are implemented to ensure that the safeguards to process and use PNR are applied to all passengers?*

Response: CBP issued an updated Directive in June 2013 that governs the processing and use of all PNR it receives. To ensure that the Department does not use PNR to unlawfully discriminate against individuals, the Privacy Office, Office of Civil Rights and Civil Liberties, the Office of the General Counsel, and relevant program staff conduct quarterly reviews to oversee implementation of ATS and to assess whether privacy and civil liberties protections are adequate and consistently implemented. All travel targeting scenarios, analysis, and rules are reviewed to ensure that they are appropriately tailored to minimize the impact upon bona fide travelers' civil rights, civil liberties, and privacy, and are in compliance with relevant legal authorities, regulations, and DHS policies.

I.3. DHS Privacy Office review report

The report further specifies that as part of the quarterly reviews, not only the targeting rules, but also all travel targeting scenarios and analysis are reviewed to minimize the impact upon bona fide travellers' civil rights, civil liberties and privacy.[65]

J. TRANSPARENCY

J.1. The relevant Commitment of the U.S.

A transparency clause is laid down in Article 10 of the Agreement. It states that:

'1. DHS shall provide information to the travelling public regarding its use and processing of PNR through:

(a) publications in the Federal Register;

(b) publications on its website;

(c) notices that may be incorporated by the carriers into contracts of carriage;

(d) statutorily required reporting to Congress; and

(e) other appropriate measures as may be developed.

---

64 Ibid., Chapter 3, page 13.

65 Ibid., Chapter 2, page 12.

2. DHS shall publish and provide to the EU for possible publication its procedures and modalities regarding access, correction or rectification, and redress procedures.

3. The Parties shall work with the aviation industry to encourage greater visibility to passengers at the time of booking on the purpose of the collection, processing and use of PNR by DHS, and on how to request access, correction and redress.'

J.2. The relevant written reply of DHS

***Question**: Has information to travelling public been provided through the channels mentioned under (a) – (e)?*

Response: A PNR Frequently Asked Questions (FAQs) document and a Privacy Policy Document are posted on the CBP website 3. Both documents were updated in June 2013 to reflect the 2011 Agreement, corresponding revised SORN, technical revisions to implement the agreement and internal DHS implementing guidance.

The 2011 U.S.-EU PNR Agreement and previous reports of DHS Privacy Office and joint reviews are posted on the DHS website http://www.dhs.gov/privacy-foia-reports. For a comprehensive explanation of the manner in which DHS/CBP generally handles PNR data, the travelling public can refer to the Automated Targeting System (ATS) System of Records

Notice (SORN) (May 22, 2012) at: http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm, and the Privacy Impact Assessment (PIA) for ATS (June 1, 2012) at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.

CBP's interim regulation regarding PNR is located in title 19, Code of Federal Regulations, section 122.49d, which is publicly available through multiple sources.

In addition to the above, CBP updated its "DHS/CBP Procedures for Access, Correction or Rectification, and Redress for Passenger Name Records (PNR)" with new contact information in June 2013. An earlier version of this document was available on DHS's website from July 2012 through the update.

***Question**: Has DHS published its procedures and modalities regarding access, correction or rectification and redress procedures and has it provided the EU with such information for possible publication by the EU?*

Response: CBP has taken steps to work with the aviation industry to encourage greater visibility to passengers at the time of booking about the purpose of the collection, processing, and use of PNR and how to request access, correction, and redress by providing the FAQs and Privacy Policy documents on the CBP website. The updated FAQs and Privacy Policy documents on the CBP website will be shared with the carriers and with the EU for possible publication. The guidance that has previously been provided to all carriers affected by the 2011 U.S.-EU PNR Agreement has a link to the DHS Traveler Redress Inquiry Program (DHS TRIP) listed for the carriers to provide to passengers. Information about DHS TRIP is located at http://www.dhs.gov/dhs-trip.

In addition to the above, CBP updated and posted its "DHS/CBP Procedures for Access, Correction or Rectification, and Redress for Passenger Name Records (PNR)" with new contact information in June 2013. An earlier version of this document was available on DHS's website from July 2012 through the update. On July 30, 2012, former DHS Chief Privacy Officer Mary Ellen Callahan sent a letter to Director Richard Priebe with a copy of original *DHS Procedures for Access, Correction or Rectification, and Redress for Passenger Name Record (PNR),* informing him that DHS would post the document on both the CBP and

Privacy Office websites and encouraging the European Commission to also post this information publicly, so as to refer travelers to EC resources as well.

***Question**: What measures are implemented together with the aviation industry to encourage greater visibility to the public?*

Response: In addition to the information provided in response to the above question, the guidance provided to air carriers also encouraged them to provide information to passengers at the time of booking regarding the purpose of the collection, processing and use of PNR by DHS, and many carriers have posted information on their websites with links to the government sites provided.

J.3. DHS Privacy Office review report

The report mentions the Privacy Office's finding that CBP's Frequently Asked Questions and PNR Privacy Policy "*reflected the 2007 PNR Agreement rather than the 2011 Agreement*". It recommended to promptly amend these documents to provide full transparency. [66] The report mentions that information on the Agreement (additional to the ones mentioned in the DHS reply) can be found under the Reports section of its website[67].

The report further signals (in relation to Article 11 on access) that information on a number of programs providing passengers with information about travelling to the U.S is available online.[68]

K. ACCESS FOR INDIVIDUALS

K.1. The relevant Commitment of the U.S.

Rules on access for individuals to their PNR data are laid down in Article 11 of the Agreement. It states that:

1. In accordance with the provisions of the Freedom of Information Act, any individual, regardless of nationality, country of origin, or place of residence is entitled to request his or her PNR from DHS. DHS shall timely provide such PNR subject to the provisions of paragraphs 2 and 3 of this Article.

2. Disclosure of information contained in PNR may be subject to reasonable legal limitations, applicable under U.S. law, including any such limitations as may be necessary to safeguard privacy-protected, national security, and law enforcement sensitive information.

3. Any refusal or restriction of access shall be set forth in writing and provided to the requesting individual on a timely basis. Such notification shall include the legal basis on which information was withheld and shall inform the individual of the options available under U.S. law for seeking redress.

4. DHS shall not disclose PNR to the public, except to the individual whose PNR has been processed and used or his or her representative, or as required by U.S. law.'

K.2. The relevant written reply of DHS

***Question**: Does the tracking system deployed by DHS allow identifying requests for access to PNR data, including EU-originating PNR data? How many requests for PNR have been received from individuals? What was the average response time by DHS?*

---

66 Ibid., Overview, page 5.

67 http://www.dhs.gov/privacy-foia-reports, DHS Privacy Office review report, Chapter 1, page 10.

68 DHS Privacy Office review report, Chapter 6, page 18.

Response: Yes, DHS identifies and tracks all requests for access to PNR, including requests from individuals that provide an EU place of birth, citizenship, or mailing address. DHS has received 27 requests for PNR since July 1, 2012, none of which came from an individual with an EU place of birth, citizenship, or mailing address. The average response time was 38 days.

***Question**: In how many cases has disclosure of information been limited and for which reasons?*

Response: Under the terms of the System of Records Notice for ATS, which maintains PNR data, and the DHS Privacy Policy Guidance Memorandum 2008-01, CBP provides access to all persons requesting their own PNR. CBP has not limited disclosure of PNR to a requestor seeking access to her or his own PNR data.

***Question**: How many refusals or restrictions of access have been set forth in writing and provided to requesting individuals? What was the average response time by DHS?*

Response: DHS has not refused or restricted access by an individual to his/her own PNR data.

***Question**: How many times PNR has been disclosed to other persons than the requesting individual?*

Response: In the course of the Privacy Office review we found that one PNR-related FOIA response included PNR on other than the requesting individual. The PNR released was of a family member and was not EU related. CBP FOIA took corrective measures and now includes an additional layer of supervisory oversight before any FOIA responses are released. There were no complaints as a result of this FOIA response and no incident was reported.

K.3. DHS Privacy Office review report

The Privacy Office reviewed the activities of the CBP Customer Service Center, the CBP FOIA/Privacy Act Program and DHS TRIP, because these programs accept requests for access to PNR from individuals regardless of the their status within the U.S. Information on how to submit an access request under these programs is available online.[69] The report mentions that during the review period (1 July 2012 to 31 March 2013), the CBP Customer Service Centre did not receive specific requests related to PNR. It also indicates that in case a traveller would submit a PNR access request to the CBP Customer Service Centre, the latter would direct the requester to submit a Freedom of Information Act (or FOIA) request or a Privacy Act request.[70]

The report signals that PNR-specific FOIA requests were handled on average within 38 days, which is also the average response time for all CBP FOIA requests. In this respect the report highlights that this is a significant improvement compared to the situation reported on in tis 2008 Privacy Report, which signalled that some PNR requests took more than a year to be handled.

Following recommendations made by the Privacy Office in 2008 and 2010, CBP developed "*Processing Instructions for PNR*", including instructions on how to conduct searches in the ATS database in response to a FOIA request for access to PNR. The review of these instructions by the Privacy Office revealed that none of the 27 PNR-related access requests were EU related within the definition used by CBP (i.e. a request is EU-related if the requester claims citizenship, a mailing address, or place of birth in the EU). The review also revealed that in one instance, personal information of another person was made available to a

---

69 Http://www.cbp.gov/xp/cgov/travel/customerservice; http://foia.cbp.gov/palMain.aspx; http://www.dhs.gov/dhs-trip.

70 DHS Privacy Office review report, Chapter 6, page 18.

requester. This finding has led to a new rule to double check all FOIA responses before they are send.[71]

The Privacy Office did not find any cases where access to PNR following a FOIA request was refused or restricted.[72]

L. CORRECTION OR RECTIFICATION FOR INDIVIDUALS

L.1. The relevant Commitment of the U.S.

Rules on correction or rectification for individuals of their PNR data are laid down in Article 12 of the Agreement. It states that:

'1. Any individual regardless of nationality, country of origin, or place of residence may seek the correction or rectification, including the possibility of erasure or blocking, of his or her PNR by DHS pursuant to the processes described in this Agreement.

2. DHS shall inform, without undue delay, the requesting individual in writing of its decision whether to correct or rectify the PNR at issue.

3. Any refusal or restriction of correction or rectification shall be set forth in writing and provided to the requesting individual on a timely basis. Such notification shall include the legal basis of such refusal or restriction and shall inform the individual of the options available under U.S. law for seeking redress.'

L.2. The relevant written reply of DHS

***Question**: How many requests from individuals seeking for correction or rectification, erasure or blocking their PNR have been received by DHS?*

Response: DHS has not received any requests to correct, rectify, erase, or block PNR.

***Question:** In how many cases individuals were informed of DHS' decision to correct or rectify their PNR? What was the average response time by DHS?*

Response: Not applicable. CBP received no requests to refer to DHS PRIV.

***Question:** How many refusals or restrictions of correction or rectification have been set forth in writing and provided to requesting individuals? What was the average response time by DHS?*

Response: Not applicable (see, response to 12.2 above).

L.3. DHS Privacy Office review report

The report mentions that several options are available to those who want to seek correction of personal information (such as PNR) held by DHS. In case a traveller is not an U.S. citizen or a lawful permanent resident, s/he may request a correction of his or her PNR by filing a Privacy Act Amendment Request through the CBP FOIA Headquarters Office, either online or by mail. A traveller may also file a request for correction by contacting the Assistant Commissioner, CBP Office of Field Operations. Alternatively a traveller may also address him or herself directly to the office of the DHS Chief Privacy Officer by email or in writing.[73]

---

71 Ibid., Overview, page 6 and Chapter 6, page 19.

72 Ibid., Chapter 6, page 19.

73 Ibid., Chapter 6, page 19.

M. REDRESS FOR INDIVIDUALS

M.1. The relevant Commitment of the U.S.

Rules on redress for individuals are laid down in Article 13 of the Agreement. It states that:

'1. Any individual regardless of nationality, country of origin, or place of residence whose personal data and personal information has been processed and used in a manner inconsistent with this Agreement may seek effective administrative and judicial redress in accordance with U.S. law.

2. Any individual is entitled to seek to administratively challenge DHS decisions related to the use and processing of PNR.

3. Under the provisions of the Administrative Procedure Act and other applicable law, any individual is entitled to petition for judicial review in U.S. federal court of any final agency action by DHS. Further, any individual is entitled to petition for judicial review in accordance with applicable law and relevant provisions of:

(a) the Freedom of Information Act;

(b) the Computer Fraud and Abuse Act;

(c) the Electronic Communications Privacy Act; and

(d) other applicable provisions of U.S. law.

4. In particular, DHS provides all individuals an administrative means (currently the DHS Traveller Redress Inquiry Program (DHS TRIP)) to resolve travel-related inquiries including those related to the use of PNR. DHS TRIP provides a redress process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat. Pursuant to the Administrative Procedure Act and Title 49, United States Code, Section 46110, any such aggrieved individual is entitled to petition for judicial review in U.S. federal court from any final agency action by DHS relating to such concerns.'

M.2. The relevant written reply of DHS

Question: *How many individuals sought administrative or judicial redress in accordance with U.S. law? What was the outcome of this procedure?*

Response: No individual has sought administrative or judicial redress from the United States Government in connection with DHS's collection and use of their PNR.

Of note, DHS TRIP received over 13,000 inquires since July 1, 2012. Of these inquiries, there were 1,834 with an EU address (DHS TRIP does not collect information on citizenship or residency). There were no EU inquires specifically naming PNR. There were two mentions of "PNR" in the aggregate inquires but neither related EU nor to issues surrounding the use of PNR data. Of all inquiries received since July 1, 2012, DHS has addressed 68 percent and provided the individuals with a response. The average response time for all inquiries is 30 days, with the average response time for EU inquires at 42 days.

Question: *In how many cases individuals sought to administratively challenge a DHS decision related to the use or processing of PNR? What was the outcome of this procedure?*

Response: None.

Question*: In how many cases an individual decided to petition for judicial review in a U.S. federal court of any final agency action by DHS? What was the outcome of this procedure?*

Response: No individual has petitioned for judicial review in connection with a final agency action based on the use of PNR.

M.3. DHS Privacy Office review report

The Privacy Office reviewed the DHS TRIP program and found that during the review period (1 July 2012 to 31 March 2013) this program had received over 13 000 inquiries, of which two specifically related to PNR but did not involve inquiries from EU individuals.[74]

With regard to the redress process provided under DHS TRIP for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat, the Privacy Office also reviewed redress applications from travellers living in or holding a passport from an EU Member State and who raised a potential privacy issue. The Privacy Office found that none of these travellers claimed that their PNR was abused. The Privacy Office also found that the average processing time for an EU-originated DHS TRIP request was comparable to the average processing time for all DHS TRIP requests.[75]

M.5. Comments

Of the 13 000 TRIP inquiries received between 1 July 2012 and 31 March 2013, DHS dealt with two inquiries specifically related to PNR but these did not involve inquiries from EU individuals.

N. OVERSIGHT

N.1. The relevant Commitment of the U.S.

Rules on oversight are laid down in Article 14 of the Agreement. It states that:

'1. Compliance with the privacy safeguards in this Agreement shall be subject to independent review and oversight by Department Privacy Officers, such as the DHS Chief Privacy Officer, who:

(a) have a proven record of autonomy;

(b) exercise effective powers of oversight, investigation, intervention, and review; and

(c) have the power to refer violations of law related to this Agreement for prosecution or disciplinary action, when appropriate.

They shall, in particular, ensure that complaints relating to non- compliance with this Agreement are received, investigated, responded to, and appropriately redressed. These complaints may be brought by any individual, regardless of nationality, country of origin, or place of residence.

2. In addition, application of this Agreement by the United States shall be subject to independent review and oversight by one or more of the following entities:

(a) the DHS Office of Inspector General;

(b) the Government Accountability Office as established by Congress; and

(c) the U.S. Congress.

Such oversight may be manifested in the findings and recommendations of public reports, public hearings, and analyses.'

---

74 Ibid., Chapter 6, page 19.

75 Ibid., Chapter 6, pages 19-20.

N.2. The relevant written reply of DHS

Question*: How many complaints have been lodged with the DHS Chief Privacy Officer since the agreement entered into force? What were the issues raised and what was the outcome of these complaints? What was the average response time by the DHS Privacy Office to such complaints?*

Response: There were no complaints lodged with the DHS Privacy Office since the agreement entered into force.

Question*: How many independent reviews were conducted by the DHS Office of Inspector General, the Government Accountability Office and the U.S. Congress since the agreement entered into force? If so, what were the outcomes of such reviews?*

Response: The DHS is not aware of any reviews of the agreement or the Department's use of PNR from OIG, GAO or other Congressional oversight committees during the time in question.

N.3. DHS Privacy Office review report

The report refers to the DHS Privacy Office authority to investigate and review all programs, such as ATS, and policies for their privacy impact. It also mentions that the Privacy Office "*conducts ongoing oversight of ATS and has conducted formal reviews of the system many times, including PIA and SORN updates and previous PNR Reports*".

The report highlights the central role in relation to oversight of the CBP Directive (regarding use and disclosure of PNR data), which outlines the use, handling, and disclosure of PNR data and provides a framework for granting access to PNR to authorized personnel within DHS and for sharing PNR with DHS's domestic and international mission partners. Because of its rules on issues such as maintaining records of access to PNR and records on sharing PNR both within DHS and with Non-DHS users, the Directive provides the framework for auditing and oversight by CBP. The Privacy Office reviewed documents recording instances of sharing PNR with other U.S. agencies.

The report observes that during the reporting period the DHS privacy Office did not receive any complaints related to non-compliance with the current PNR Agreement or any complaints related to a misuse of PNR.[76]

Besides the Privacy Office, other DHS components, such as the CBP Privacy Officer and the CBP Office of Internal Affairs have oversight functions. The CBP Privacy Officer keeps copies of all requests for PNR by Non-DHS users and the correspondence regarding PNR disclosures for audit purposes and maintains a record of access determinations for oversight purposes. As mentioned earlier, the CBP Office of Internal Affairs audits the use of ATS-P to guard against unauthorized use.

In view of the multi-faceted approach to oversight within CBP, the DHS Privacy Office recommends that "*CBP should consider consolidating the results of its various audits into comprehensive reports for review by the CBP Privacy Office*" in order to enhance accountability and ensure efficient oversight, a recommendation with which CBP agrees.[77]

[76] Ibid., Chapter 8, page 21.

[77] Ibid., Overview, page 7 and Chapter 8, page 23.

O. METHOD OF PNR TRANSMISSION

O.1. The relevant Commitment of the U.S.

Rules on the method of transmission of PNR are laid down in Article 15 of the Agreement. It states that:

'For the purposes of this Agreement, carriers shall be required to transfer PNR to DHS using the 'push' method, in furtherance of the need for accuracy, timeliness and completeness of PNR.

2. Carriers shall be required to transfer PNR to DHS by secure electronic means in compliance with the technical requirements of DHS.

3. Carriers shall be required to transfer PNR to DHS in accordance with paragraphs 1 and 2, initially at 96 hours before the scheduled flight departure and additionally either in real time or for a fixed number of routine and scheduled transfers as specified by DHS.

4. In any case, the Parties agree that all carriers shall be required to acquire the technical ability to use the 'push' method not later than 24 months following entry into force of this Agreement.

5. DHS may, where necessary, on a case-by-case basis, require a carrier to provide PNR between or after the regular transfers described in paragraph 3. Wherever carriers are unable, for technical reasons, to respond timely to requests under this Article in accordance with DHS standards, or, in exceptional circumstances in order to respond to a specific, urgent, and serious threat, DHS may require carriers to otherwise provide access.'

O.2. The relevant written reply of DHS

***Question**: All carriers should have acquired the technical ability to use the push method not later than 1 July 2014. What is the state of play? How many carriers operating flights from the EU do not yet have a push system in place?*

Response: CBP is working with both the affected carriers and service providers to 'push" prior to July 1, 2014.

CBP has reached out, individually via email and telephone, to all affected air carriers that are required to change to the push method. DHS/CBP has posted the 2011 Agreement on the DHS site and CBP has provided the link to the Agreement to carriers and service providers.

So affected carriers can better understand their obligations, CBP has also provided guidance, which highlights the changes that are to be implemented, and specifically stated that within 24 months from July 1, 2012, air carriers covered by the new Agreement are required to utilize the PNR push process when providing PNR data to DHS/CBP and that the pull process will only be utilized under limited circumstances.

CBP hosted a conference call with a trade association to discuss the Agreement and the impact on carriers.

In addition, CBP is also contacting service providers that will need to make system changes for their carriers to push data.

CBP will make CBP's Office of Information and Technology available to answer questions from carriers' service providers individually and has offered to have a technical meeting with carriers.

The following list represents the number of affected carriers using each method, as of June 1, 2013:

- 47- Total carriers affected by the Agreement:
- 32- Of the carriers affected, the number of carriers that already use the "push" method;
- 15- Of the carriers affected, the number of carriers that use the "pull" method;
- 5 utilize the services of the same service provider that we are working with;
- 2 utilize the services of a service provider that "push" for other carriers
- 4 utilize different service providers;
- 4 large carriers have their own system.

***Question**: In how many cases DHS required carriers to provide PNR between or after the regular transfers described in paragraph 3? Which method of transmission was used?*

Response: Total number of PNRs received (push + pull) in calendar year 2012: 81,252,544

Total number of ad hoc PNRs pulled in calendar year 2012: 243,120 (or 0.30% of total PNR)

Total number of PNRs received (push + pull) in calendar year 2011: 79,005,866

Total number of ad hoc PNRs pulled in calendar year 2011: 570,401 (or 0.72% of total PNR)

***Question**: Has DHS assessed its way of using the ad hoc functionality and if so, what were the findings?*

Response: Yes. The mechanism was reviewed by DHS Privacy during an internal review in May 2013; a report of that review was completed in July 2013.

***Question**: Has DHS resumed talks with the air carriers for finding an acceptable ad hoc push functionality? If so, what is the state of play of such talks? If not, what are the reasons for not having pursued such talks?*

Response: As part of the new PNRGOV International Standard, CBP is working with the International Air Transport Association (IATA), air carriers and service providers, along with other government representatives to include ad hoc push functionality as part of the standard.

***Question**: Although the Agreement does not explicitly require limiting access to the ad hoc functionality to specifically authorised DHS officials, in order to assess the way in which it is used, it is useful to understand how DHS has organised access to this functionality.*

Response: Each user's access to the PNR ad hoc functionality is reviewed twice per year by the supervisor who authorized the role, and validated by a CBP Headquarters Manager.

O.3. DHS Privacy Office review report

The report mentions that DHS (CBP) has made significant progress to ensure that airlines "push" PNR to CBP and that as of 22 April 2013 68% of air carriers operating flights between the U.S and the EU has moved to the "push" method, an increase of 20 air carriers since the 2010 review report of the DHS Privacy Office.[78]

The report signals that CBP has promoted awareness with air carriers that are required to change to the "push" method. The guidance given focused on four key issues: the time intervals for PNR transfers; the requirement to move to a PNR "push"; the need to provide passengers with information about DHS' collection, processing and use of PNR; and

[78] Ibid., Overview, page 5.

information on how passengers can request access to or correction of their PNR or redress for an action taken that resulted from use of PNR.[79]

The report notes[80] that DHS (CBP) had not yet begun to require air carriers to transfer PNR to DHS at 96 hours before the scheduled flight departure as allowed under the new Agreement, and continued to operate using the 72–hour interval as laid down in the previous PNR Agreement of 2007. The report also mentions that CBP is informing those air carriers using the "push" method that it seeks to receive PNR at 96 hours before scheduled flight departure. DHS confirmed that it has started preparations to allow transfer of PNR data starting at 96 hours prior to scheduled departure.

In relation to the ad hoc "pulls", the report indicates[81] that on one occasion, DHS (CBP) requested one retransmission of PNR by an EU-based service provider as the PNR had not been provided timely.

The report further mentions in relation to Articles 5 and 15 of the Agreement that when information is transferred from the IT system (probably what is meant is the system holding the PNR data, the ATS-P system), ATS logs the external sharing[82].

P. DOMESTIC SHARING

P.1. The relevant Commitment of the U.S.

Rules on domestic sharing of PNR are laid down in Article 16 of the Agreement. It states that:

'1. DHS may share PNR only pursuant to a careful assessment of the following safeguards:

(a) Exclusively as consistent with Article 4;

(b) Only with domestic government authorities when acting in furtherance of the uses outlined in Article 4;

(c) Receiving authorities shall afford to PNR equivalent or comparable safeguards as set out in this Agreement; and

(d) PNR shall be shared only in support of those cases under examination or investigation and pursuant to written understandings and U.S. law on the exchange of information between domestic government authorities.

2. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraph 1 of this Article shall be respected.'

P.2. The relevant written reply of DHS

***Question**: How does DHS guarantee that receiving authorities afford to PNR equivalent or comparable safeguards as set out in the agreement?*

Response: CBP issued an updated Directive governing the processing and use of all PNR it receives.

In addition, all EU PNR shared within the U.S. government includes the following caveat:

"This document is provided by the U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)/U.S. CUSTOMS AND BORDER PROTECTION (CBP) to [insert authorized agency]

79 Ibid., Chapter 1, page 11.
80 Ibid., Chapter 5, page 17.
81 Ibid., Chapter 5, page 18.
82 Ibid., Chapter 7, page 21.

for its official use only. This document contains confidential personal information of the data subject, including Passenger Name Record data ("Official Use Only"), which is governed by the Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security. Such data must receive equivalent and comparable safeguards and be used only for the purposes outlined in the Agreement. This document may also contain confidential commercial information. The data is this document may only be used for authorized purposes and shall not be disclosed to any third party without the express prior written authorization of DHS/CBP."

P.3. DHS Privacy Office review report

The report indicates that domestic sharing "*only takes place for specific cases after DHS determines that the recipient has a need to know the information to carry out functions consistent with the routine uses set forth in the ATS SORN*". The report also mentions that the recipient has to provide a written confirmation to handle PNR with safeguards equivalent or comparable to those required by the Agreement and also should be consistent with U.S. law on the exchange of information between domestic government authorities. As part of an express understanding, the recipient domestic authority also has to treat PNR as sensitive and confidential and is prohibited from providing PNR to any other third party without prior written authorization of DHS.[83]

The report mentions in relation to Articles 5 and 15 of the Agreement that when information is transferred from the IT system (probably what is meant is the system holding the PNR data, the ATS-P system), ATS logs the external sharing.[84] This observation is also relevant in relation to Article 16.

Q. ONWARD TRANSFER

Q.1. The relevant Commitment of the U.S.

Rules on onward transfer of PNR are laid down in Article 17 of the Agreement. It states that:

'1. The United States may transfer PNR to competent government authorities of third countries only under terms consistent with this Agreement and only upon ascertaining that the recipient's intended use is consistent with those terms.

2. Apart from emergency circumstances, any such transfer of data shall occur pursuant to express understandings that incorporate data privacy protections comparable to those applied to PNR by DHS as set out in this Agreement.

3. PNR shall be shared only in support of those cases under examination or investigation.

4. Where DHS is aware that PNR of a citizen or a resident of an EU Member State is transferred, the competent authorities of the concerned Member State shall be informed of the matter at the earliest appropriate opportunity.

5. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraphs 1 to 4 shall be respected.'

This provision is accompanied by a specific recital in the Agreement stating that '*NOTING the interest of the Parties, as well as EU Member States, in exchanging information regarding the method of transmission of PNR as well as the onward transfer of PNR as set forth in the*

[83] Ibid., Chapter 3, page 14.
[84] Ibid., Chapter 7, page 21.

relevant articles of this Agreement, and further noting the EU's interest in having this addressed in the context of the consultation and review mechanism set forth in this Agreement;'.

Q.2. The relevant written reply of DHS

***Question**: According to paragraph 2, the U.S. will fulfil the conditions of paragraph 1 by way of express understandings that incorporate data privacy protections comparable to those applied to PNR by DHS under the Agreement. How many such understandings have been entered into by the U.S.?*

Response: DHS/CBP has a pre-existing arrangement to exchange PNR data with the Canada Border Services Agency on high-risk travelers. The arrangement was last updated to reflect the provisions of the 2007 EU-U.S. PNR agreement, and discussions with CBSA on any further updates will commence after the entry into force of the PNR agreement currently in negotiations between Canada and the EU.

***Question**: Have any 'emergency circumstances' occurred since the entry into force of the Agreement? If so, how many times and what type of emergency had to be faced?*

Response: CBP is not aware of any such emergency circumstances.

Question: How many times DHS informed an EU Member State that the U.S. shared PNR of one of its citizens or residents with a third country? Did the Member State react to this sharing of information? Have there been situations in which a Member State was not informed and if so, why?

Response: CBP is not aware of any sharing of EU PNR with third countries, other than PNR data on high-risk travellers exchanged under the agreement with Canada described above.

Q.3. DHS Privacy Office review report

The report mentions that also in the case of the sharing of PNR with foreign or international government agencies, DHS requires an express understanding that the recipient will treat PNR as sensitive and confidential and that it will not provide PNR to any other third party without DHS' prior written authorization. The report specifies that "*sharing takes place for specific cases and only after DHS determines that the recipient has a need to know the information to carry out functions consistent with the routine uses set forth in the ATS SORN"*. The report underlines that the Privacy Office and CBP review each international access arrangement "*to ensure that the terms are observed and that continued sharing of PNR with a non-U.S. user is appropriate*". [85]

The report mentions that in one case, EU PNR data were shared with an EU Member State. The Privacy Office reviewed this case and found that '*the PNR was shared for the authorized purpose and pursuant to an agreement or arrangement that included specific language governing the use and protection of the PNR shared'*[86].

The report also mentions that DHS (CBP) shared PNR with one international partner on the basis of an information sharing agreement in place since 2006 and updated in 2009 so as '*to ensure that only PNR with a nexus to terrorism or serious transnational crime are transmitted'*. As shown by the reply of DHS to the questionnaire mentioned above, this relates to an information sharing agreement with the Canadian authorities. In relation to this U.S.-Canadian arrangement and this specific PNR transfer, the Privacy Office found also that '*the*

[85] Ibid., Chapter 3, page 14.
[86] Ibid., Chapter 3, page 15.

PNR was shared for the authorized purpose and pursuant to an agreement or arrangement that included specific language governing the use and protection of the PNR shared' yet notes that the notification to EU Member States was not provided.[87] The Privacy Office thus recommends in its report that '*CBP should provide the DHS Office of International Affairs (OIA) with notification about disclosures and, in turn, OIA should notify EU Member States, as appropriate, in a timely manner and develop a consistent approach moving forward for notifications."*[88] In its response to this recommendation, DHS (CBP) indicated it agrees with the Privacy Office's findings. The report also mentions that CBP and the OIA *"are working to develop a consistent process for notification to the EU Member States. CBP will work with OIA to notify the EU Member States in a timely fashion, as appropriate."*[89]

The DHS Privacy Office review report further mentions in relation to Articles 5 and 15 of the Agreement that when information is transferred from the IT system (probably what is meant is the system holding the PNR data, the ATS-P system), ATS logs the external sharing. This observation is also relevant in relation to Article 17.[90]

R. LAW ENFORCEMENT COOPERATION

R.1. The relevant Commitment of the U.S.

Rules on police, law enforcement and judicial cooperation are laid down in Article 18 of the Agreement. It states that:

"1. Consistent with existing law enforcement or other information-sharing agreements or arrangements between the United States and any EU Member State or Europol and Eurojust, DHS shall provide to competent police, other specialised law enforcement or judicial authorities of the EU Member States and Europol and Eurojust within the remit of their respective mandates, as soon as practicable, relevant, and appropriate, analytical information obtained from PNR in those cases under examination or investigation to prevent, detect, investigate, or prosecute within the European Union terrorist offences and related crimes or transnational crime as described in Article 4(1)(b).

2. A police or judicial authority of an EU Member State, or Europol or Eurojust, may request, within its mandate, access to PNR or relevant analytical information obtained from PNR that are necessary in a specific case to prevent, detect, investigate, or prosecute within the European Union terrorist offences and related crimes or transnational crime as described in Article 4(1)(b). DHS shall, subject to the agreements and arrangements noted in paragraph 1 of this Article, provide such information.

3. Pursuant to paragraphs 1 and 2 of this Article, DHS shall share PNR only following a careful assessment of the following safeguards:

(a) Exclusively as consistent with Article 4;

(b) Only when acting in furtherance of the uses outlined in Article 4; and

(c) Receiving authorities shall afford to PNR equivalent or comparable safeguards as set out in this Agreement.

4. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraphs 1 to 3 of this Article shall be respected."

---

87 Ibid.

88 Ibid., Overview, pages 5-6.

89 Ibid., Overview, page 6.

90 Ibid., Chapter 7, page 21.

R.2. The relevant written reply of DHS

***Question**: In how many cases did DHS provide analytical information obtained from PNR to relevant EU Member States authorities, Europol or Eurojust?*

Response: CBP is not aware of any provision of analytical data obtained from PNR that has been provided to relevant EU authorities. However, warnings derived from DHS's analysis of PNR and/or API have been provided to EU Member States. The specific accounting and details of these exchanges are law enforcement sensitive and may be discussed further during the Joint Review.

***Question**: What criteria does DHS use to define 'as soon as practicable, relevant and appropriate' in order to provide analytical information obtained from PNR?*

Response: DHS views "as soon as practicable, relevant and appropriate" to be directly tied to how the receiving EU Member State will utilize the data upon receipt of it. As such, a specialized decision based on the unique counterterrorism and law enforcement interests and capabilities of each Member State must be compared to the terms of the agreement. DHS will not release information that cannot be operationally utilized consistent with the agreement, including to EU Member States.

***Question**: How many requests did DHS receive from relevant EU Member States authorities, Europol or Eurojust for access to PNR or relevant analytical information obtained from PNR? If so, what was the nature of the specific investigation for which the data were requested, i.e. to combat terrorism and related crimes, or to combat transnational crime as described in Article 4?*

Response: CBP is not aware of any such requests.

***Question**: How does DHS guarantee that the transfers respect the Agreement's safeguards and that equivalent or comparable safeguards are guaranteed by the receiving authorities?*

Response: Because the agreement is binding on all Member States they should be legally bound to provide such protections under EU law pursuant to 18.3(c), subject to the full scope of sanctions available to the European Commission should they fail to adhere to meet such a standard. Nonetheless, DHS will provide appropriate markings on any data transferred under Article 18 under an existing authority to remind the recipient of this obligation. Such markings state:

"This document is provided by the U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)/U.S. CUSTOMS AND BORDER PROTECTION (CBP) to [insert authorized agency] for its official use only. This document contains confidential personal information of the data subject, including Passenger Name Record data ("Official Use Only"), which is governed by the Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security. Such data must receive equivalent and comparable safeguards and be used only for the purposes outlined in the Agreement. This document may also contain confidential commercial information. The data is this document may only be used for authorized purposes and shall not be disclosed to any third party without the express prior written authorization of DHS/CBP."

R.3. DHS Privacy Office review report

In reviewing the sharing of PNR with foreign agencies, the Privacy Office observed that in one case the sharing of EU PNR data with a third country was not notified to EU Member

States as required under the Agreement.[91] The DHS Privacy Office thus recommends that CBP should provide the DHS Office of International Affairs with notification about such disclosures, and that in turn this DHS Office should notify EU Member States as appropriate, in a timely manner and develop a consistent approach on notifications. [92]

S. IMPLEMENTING AND FINAL PROVISIONS

Articles 19-21, Articles 23- 27 of the Agreement

The EU team did not raise questions as regards these Articles and they were not discussed either during the review meeting or addressed in the review report of the DHS Privacy Office.

T. NOTIFICATION OF CHANGES IN DOMESTIC LAW

Article 22 of the Agreement

The EU team did not raise questions as regards this Article. DHS informed the EU team that no changes in U.S law occurred that materially would affect the implementation of the Agreement.

91 Ibid., Overview, page 5 and Chapter 3, page 15.

92 Ibid., Overview, pages 5-6.

ANNEX B
COMPOSITION OF THE REVIEW TEAMS

The members of the EU team were:

- Reinhard Priebe, Director, European Commission, DG Home Affairs – Head of the EU delegation
- Cecilia Verkleij, European Commission, DG Home Affairs
- Julian Siegl, European Commission, DG Home Affairs
- Liene Balta, European Commission, DG Justice
- Karsten Behn, expert on data protection in the law enforcement area from the German Federal data protection authority
- Muriel Sylvan, PNR expert from the French Ministry of the Interior
- Jose Maria Muriel from the EU delegation in Washington.

The members of the U.S. team were:

- Jonathan Cantor, Acting Chief Privacy Officer, Privacy Office, DHS
- Rebecca Richards, Acting Deputy Chief Privacy Officer and Senior Director for Privacy Compliance, Privacy Office, DHS
- Shannon Ballard, Director, International Privacy Programs, Privacy Office, DHS
- Kelli Ann Walther, Deputy Assistant Secretary, Screening Coordination Office, DHS
- Michael Scardaville, Director, European and Multilateral Affairs, Office of International Affairs, DHS
- Regina Hart, Senior Counsel, Office of the General Counsel, DHS
- David Harding, Secure Flight Program, Transportation Security Administration (TSA), DHS
- Peter Pietra, Privacy Office, TSA, DHS
- Carey Davis, Acting Executive Director, Office of filed Operations, CBP, DHS
- Donald Conroy, Director, National Targeting Center-Passenger, CBP, DHS
- Franklin Jones, Executive Director, Diversity and Civil Rights, CBP, DHS
- Laurence Castelli, Privacy Officer, CBP, DHS
- Kristin Dubelier, Deputy Associate Chief Counsel (Enforcement), CBP, DHS
- Robert M. Neumann, Acting director, Travel Entry Programs, Office of Field Operations, CBP, DHS
- Jeannine Perniciaro, Program Manager, Travel Entry Programs, CBP, DHS
- Akbar Siddiqui, Attorney Advisor, CBP, DHS

- Emily Rohde, Attorney, CBP, DHSThomas Burrows, Assocaite Director, Office of intrenatinal Afairs, U.S. Department of Justice
- Leslie Freriksen, Auropean Union Affairs, U.S. Department of State (DoS)
- Kathlen Wilson, Office of the Legal Advisor, DoS
- Elaijne Morris-Moxnes, Program Manager, Targeting and Analysis Systems Program Office, CBP, DHS