EUROPEAN
COMMISSION

Brussels, 12.1.2021
SWD(2021) 4 final

COMMISSION STAFF WORKING DOCUMENT
Accompanying the document

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the joint evaluation of 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

{COM(2021) 18 final}

CONTENTS

1. INTRODUCTION

The Agreement between the U.S. and the European Union (EU) on the use and transfer of Passenger Name Record (PNR) to the U.S. Department of Homeland Security (DHS) entered into force on 1 July 2012[1] (herein after "the Agreement"). It responds to the needs of U.S. law requirement for airlines operating flights to or from the United States of America (U.S.) to provide the DHS, U.S. Customs and Border Protection (CBP), with PNR data for purposes of preventing, detecting, investigating, and prosecuting terrorist offenses and related crimes and certain other crimes that are transnational in nature[2]. This information is collected in airline travel reservations and is transmitted to CBP prior to departure.

Accordingly, the Agreement allows for transfers of PNR data to the U.S. from the carriers operating passenger flights between the European Union and the U.S. and from carriers storing data in the EU and operating passenger flights to or from the U.S., subject to safeguards and controls included therein. According to Article 23(1) of the Agreement, "The Parties shall jointly review the implementation of this Agreement one year after its entry into force and regularly thereafter as jointly agreed. Further, the Parties shall jointly evaluate this Agreement four years after its entry into force". Two joint reviews of the Agreement[3] took place in 2013[4] and 2015[5] which examined the practical application of the Agreement. The second joint review was carried out in 2015, however, the report was published in 2017. At the time of agreeing on the aspects of the joint evaluation, considering that the report had been published quite recently, it was decided for the next joint review to take place after the finalisation of the joint evaluation. These reviews, which are publicly available online, found DHS in compliance with the Agreement's terms and proposed recommendations to further improve it.

---

1 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, OJ L 215, 11.8.2012, p. 5.

2 This information is collected in airline travel reservations and is transmitted to CBP prior to departure.

3 The 2013 and 2015 Joint Reviews are in addition to Joint Reviews completed in 2008 and 2005 on early versions of the U.S.-EU PNR Agreement.

4 Report on the joint review 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 {SEC(2013) 630 final}. Brussels, 27.11.2013, COM(2013) 844 final and SEC(2013) 630 final.

5 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 records to the United States Department of Homeland Security {SWD(2017) 14 final} {SWD(2017) 20 final}. Brussels, 19.1.2017, COM(2017) 29 final.

In January 2019, it was jointly agreed to launch the joint evaluation of the EU-U.S. PNR Agreement exercise as foreseen in Article 23 thereof. This document includes findings by the EU side and the result of the joint evaluation. Prior to its finalisation, it was shared with the U.S. authorities providing them with the opportunity to identify possible inaccuracies and comment on its content. Pursuant to the agreed terms of the evaluation the U.S. may issue its own report with its observations.

Due to the sensitive nature of the PNR programme, some information was provided to the EU team on the condition that it would be treated as classified up to the level of EU Secret. These limitations have not come in the way of a thorough and objective evaluation, as well as an open and frank exchange of views with the U.S. authorities in a very constructive spirit.

Background on PNR processing in the U.S.

PNR data are transmitted to DHS/CBP pursuant to its statutory authority, 49 USC. § 44909[6], as implemented by the Title 19 of the Code of Federal Regulation (CFR) 122.49d[7]. The U.S. provided the EU team with information about the implementation and use of the Automated Targeting System (ATS).

DHS/CBP operates the ATS, which is a decision support system using, inter alia, PNR data to facilitate legitimate travel while identifying potential threats to the U.S. posed by individuals so they can be referred for an in depth examination prior to entering or exiting the U.S.. ATS compares information about individuals travelling on flights to or from the U.S. against U.S. law enforcement databases[8] as well as redress records and travel history of the passengers. It compares existing information about individuals entering and exiting the country with patterns of known illicit activities ("targeting rules") identified through risk-based assessments and intelligence. It flags possible matches to these targeting rules. It allows users to search data to provide a consolidated view of data about a person or entity of interest. It also provides users with a consolidated view of data about a person entering or departing the U.S. so a decision about their admissibility can be rendered. As such, it allows DHS to focus law enforcement attention on those individuals most likely to pose a risk while facilitating the

6 Please see: https://www.govinfo.gov/content/pkg/USCODE-2018-title49/pdf/USCODE-2018-title49-subtitleVII-partA-subpartiii-chap449-subchapI-sec44909.pdf.

7 Please see: https://www.govinfo.gov/app/details/CFR-2012-title19-vol1/CFR-2012-title19-vol1-sec122-49d/summary.

8 Please see replies to the Questionnaire under "Automated processing".

entry of the overwhelming majority of legitimate travellers by reducing inspection requirements.

The U.S. approach to making admissibility determinations, shares some similarities with the techniques adopted by other law enforcement services whose data and expertise contribute to the conduct of that analysis. In addition, representatives from these services may be assigned to work at DHS facilities, or contribute from their own locations. ATS unifies this information to support decision making procedures and is used both by CBP officers at ports of entry, including dedicated Passenger Analytical Units at relevant points of entry and at the national level, including at CBP's National Targeting Center (NTC). This distinction between national and local operations is, in some respects different from that employed by individual EU Member States which rely on a single Passenger Information Unit (PIU) to conduct analysis at a national level.

As a result of the U.S. structure, DHS officials, including from CBP, Immigration and Customs Enforcement (ICE), U.S. Coast Guard, U.S. Citizen and Immigration Services (USCIS), the Transportation Security Administration (TSA) and the Office of Intelligence and Analysis (I&A) use the ATS, although their access to PNR data is limited to what is necessary to fulfil the individual's official responsibilities consistent with U.S. law, policy, and the Agreement. The U.S. team noted that DHS provides individual users with access to PNR data only to the extent that the users have an official need for the information to perform their duties and each user's access to specific PNR user groups or roles must be approved by the CBP Privacy Office and the CBP Office of Chief Counsel (OCC). DHS vets all of its employees before hiring them, and DHS trains them before and regularly after giving them access to the PNR needed to perform their duties.

To demonstrate the scale of the CBP airport operations, in fiscal year 2019 (1 October 2018 to 30 September 2019), there were 968,914 commercial aircraft arriving from approximately 280 points of departure airports outside the United States bringing to the United States more than 135.7 million travellers. This was increase in air passenger volume of 3.76% over the previous fiscal year. Most points of entry operate 24 hours per day, seven days a week, requiring three shifts of frontline officers and supervisory officers that, among other things, receive and evaluate PNR data to determine whether travellers should be further scrutinised prior to their admission into the United States.

2. METHODOLOGY

Although the Agreement does not state the scope and purpose of the joint evaluation, the Commission and DHS agreed it should take a wider approach than the joint reviews. Hence, unlike the joint reviews, whereby both parties assess together whether the Agreement is being implemented correctly, the joint evaluation consists of a more thorough examination of the Agreement. In particular, the joint evaluation explores the wider functioning and operationally added value and assess its results, impacts, effectiveness, necessity and proportionality. It also offers an opportunity to take stock of any impact caused by the evolution of the relevant legal framework and case law of both parties.

As a first step, the European Commission sent a detailed questionnaire to DHS covering relevant aspects (the questionnaire and the replies provided by the U.S. can be found in Annex B). The EU team visited DHS and CBP premises on 5-6 September 2019. In order for the EU to provide insight to the U.S. on the newly EU established system, the U.S. team visited Europol headquarters, the Dutch and the Belgian Passenger Information Units (PIU) on 22–23 October 2019.

The joint evaluation covers the entire period of application of the 2012 Agreement to 2019[9]. As was the case with the joint reviews, the European Union was represented by the European Commission. The Commission team was led by the Director for Security and included officials from the Directorate General for Migration and Home Affairs, the Directorate General for Justice and Consumers, Europol, as well as data protection and law enforcement experts from the EU Member States. The U.S. was represented by DHS with a team composed of officers from various units in charge of the PNR data collection and analysis as well as participants from its legal, policy and privacy officers, and the U.S. Departments of State and Justice. A full list of the members of both teams appears in Annex C (the composition of the teams).

The joint evaluation relied on the following elements:

- The questionnaire sent to the U.S. in advance of the joint evaluation and the replies to this questionnaire (Annex B);

[9] The health issues emerged during the 2020 Covid-19 pandemic will be assessed under the next Joint Review of the EU-US PNR Agreement.

- Visits to DHS headquarters, CBP, and the CBP NTC in Washington, D.C., and Virginia, U.S. on 5-6 September 2019;
- Visit of the U.S. team to the Belgian and Dutch Passenger Information Units and Europol on 22-23 October 2019;
- Exchanges with DHS personnel responsible for the PNR programme, including analysts who use and have access to PNR data;
- The information provided during the visits to the U.S. and discussions with representatives from DHS, U.S. Customs and Border Protection, the U.S. Department of Justice, and the U.S. Department of State;
- Documentation received from U.S. (including on the CBP's targeting programme and its privacy framework and oversight).
- The joint review reports of 2013 and 2015, where appropriate;
- Related legislation and case law; notably the Opinion 1/15 of the European Court of Justice of 26 July 2017 on envisaged EU-Canada PNR Agreement.[10]
- The evolution of the security environment in the EU, the U.S., and globally, including the adoption of an obligation for all States to collect and use PNR in the United Nations Security Council Resolution 2396 (2017).[11]

The present document has received the unanimous agreement of the members of the EU team. It has also been shared with DHS, providing the U.S. with the opportunity to comment on inaccuracies, identify information which cannot be disclosed to public audiences, and respond to conclusions by the European Commission. While the evaluation itself was conducted jointly, this is document is not a joint report of the EU and U.S. teams.

3. THE OUTCOME OF THE JOINT EVALUATION

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

3.1. The use and operational value of PNR data

The evaluation teams discussed different ways in which PNR data are used for purposes of preventing, detecting, investigating, and prosecuting terrorist offenses and related crimes and

[10] Opinion 1/15 of the Court (Grand Chamber), ECLI:EU:C:2017:592.
[11] Resolution 2396 (2017) - Adopted by the Security Council at its 8148th meeting, on 21 December 2017.

certain other crimes that are transnational in nature as defined in Article 4 of the Agreement, as well as other purposes addressed by Article 4 of the Agreement, to include the protection of vital interests of any individual. PNR data contains elements that are not available through other means and is used to assist in identifying high risk travellers who are not otherwise known to law enforcement agencies (examples of real cases are provided throughout the present document).

PNR data are used to help identify travellers to or from the U.S. who may be involved in terrorism or serious transnational crimes. This is done by comparing PNR data with relevant databases[12] and on the basis of targeting rules established on the basis of past investigations and intelligence showing how terrorists and criminals exploit air travel to identify passengers who may need additional scrutiny. If there is a match, CBP conducts additional research using other available information and databases. .

According to the U.S. authorities, the transfer, processing, and analysis of PNR data under the Agreement:

- Facilitates the expeditious entry of the overwhelming majority of travellers posing no threat to public safety.
- Contributes to the effective and accurate identification of individuals who should undergo further inspection upon arrival.
- Complements other information about a traveller and their journey such as Advance Passenger Information (API), visa applications, Electronic System for Travel Authorization (ESTA) applications, and biometrics to provide a complete and accurate picture of the traveller's identity and means of travel as relevant for border enforcement purposes.
- Helps DHS to limit inspections to travellers posing higher relative risk when processed and analysed along with other information in relevant databases, past enforcement actions and known or suspected illicit trends, thereby expediting the admission of all other travellers.
- Provides insight into the travel of the individual, at times including multiple legs of the journey, prior to and after arrival and/or boarding that is not available from other information that is relevant to border enforcement.

[12] The full list is included in the replies to the questionnaire.

- Illuminates the modus operandi of criminals and terrorists through the review of historical[13] PNR of newly identified suspects.
- Identifies previously unknown terrorists and criminals, both during routine border encounters and through the review of current and historical PNR during investigations.

Example:

In January 2015, DHS referred an individual for a secondary inspection, as the information in his PNR matched the modus operandi of known terrorists. During the secondary inspection, a review of the traveller's electronic device revealed images related to terrorist activities. The traveller could not explain why he had these images. Based on secondary inspection, DHS referred him to another law enforcement agency for further investigation.

In another example, in January 2019, an EU citizen sought to travel from the U.S. to the EU with weapons in his checked baggage. Through PNR, DHS was alerted that the individual had checked weapons in his luggage. DHS inspected the luggage and found several rifles. Processing of PNR data alerted DHS of the weapons. DHS reviewed additional information and determined that the individual had not obtained the required export licence. Because the illicit export of the rifles constituted a serious violation, DHS seized the items.

The U.S. explained that, without PNR data, DHS Officers would need to undertake much more intrusive and time-consuming interviews and inspections of each and every traveller, significantly delaying passengers and the operation of the international air transportation system. PNR data allows DHS to focus on high-risk individuals, thereby reducing passenger wait times and inspections at ports of entry for nearly all travellers to a few minutes or less.

3.2. Targeting Rules and use of historical PNR data

During the evaluation exercise, the U.S. Delegation provided additional information about PNR's contribution to security. The U.S. representatives stated that PNR data provides important historical information for investigations and thus assists with identification of previously unknown persons of interest, who have been linked to known or suspected terrorists, criminal networks, or other illegal activities. This was also the case regarding the investigations into several terrorist attacks in the EU. At the request of European national law

[13] Historical PNR data refers to the PNR data retained under the conditions and safeguards of the EU - U.S.. PNR Agreement.

enforcement agencies leading the investigations, DHS shared PNR and other records that aided European authorities in locating additional, previously unknown suspects. DHS's receipt and retention of PNR allowed it to support EU Member States directly or through EUROPOL following many of the EU-based terrorist attacks since at least 2012, including the Paris Bataclan, Barcelona, Brussels, Berlin Christmas Market, and Bastille Day attacks.

The U.S. authorities illustrated the operational added value of the processing of PNR data including historical PNR data on a number of case studies and examples available below and in Annex A and B.

Examples:

I. In August 2019, DHS identified a previously unknown associate of a known or suspected terrorist, based on matches to multiple historic PNR data belonging to the previously unknown associate. DHS's ability to validate the association between the two individuals over the course of many years was critical to establishing reasonable suspicion and the individual was referred to law enforcement for further investigation.

II. In January 2014, a U.S. law enforcement agency asked for DHS's assistance in locating a criminal fugitive wanted since 2004 and believed to have fled the country. Using historical PNR, DHS identified the probable residence of the subject in a foreign country. The U.S. law enforcement agency, with assistance from the foreign country, located the subject in the other country in June 2014, and successfully had the subject extradited back to the U.S.

III. In 2004, U.S. authorities detained a woman who had smuggled children into the U.S. A transnational criminal organisation recruited her to smuggle the children into the U.S. where the organisation's operatives sold them. Through information gained during her interview about the organisation's routine operations, DHS used historical and current PNR data to identify additional potential smugglers and victims previously unknown to U.S. law enforcement. The U.S. and a foreign government conducted joint law enforcement operations to shut down two transnational criminal organisations who used the same technique to smuggle children into the U.S. The joint operations resulted in the arrest of dozens of criminals and the return of dozens of children to their parents in foreign countries. The modus operandi discovered by this case supported law enforcement investigations and interdictions for many years, leading to additional arrests and rescued children.

IV. In 2012, the U.S. investigated an individual for child sex tourism. Similar allegations about the subject had been made since the 1970's, and he had been previously charged in the U.S., the UK, and Egypt. DHS provided certified copies of historical PNR data to the Assistant U.S. Attorney for use at trial. The historical PNR data showed the subject's travel, his use of aliases, and the identity of third parties who paid for his tickets. On 28 February 2013, a U.S. district court found the individual guilty of child sex tourism charges.

V. In the 1990s, an individual joined al Qaeda and fought in Afghanistan. When he returned to the U.S., U.S. authorities arrested him for planning to set off bombs in the U.S. and Europe. DHS provided U.S. prosecutors with historical PNR data of his travel to various countries with a significant terrorist presence, data which DHS retained at a time when the individual was not under suspicion of any criminal activity. The retained PNR contributed to his conviction and 15-year prison term for conspiring to use weapons of mass destruction and providing support to terrorists.

VI. In 2019, a U.S. citizen travelled to the United States from Europe. Because his historical PNR matched an illicit trend used by known or suspected terrorists, DHS/CBP referred him for secondary inspection. The subject claimed that he had been overseas for a few years attending school and working. When asked if he knew anyone involved in the Syrian conflict, he stated that he attended a mosque that was soliciting funds to support the conflict in Syria. During the secondary inspection, DHS discovered photos of weapons on his electronic device, of the subject aiming a gun at someone, and of a video of militants wearing ISIS patches. Based on this inspection, and the availability and use of historical PNR data, DHS was able to refer him to law enforcement for further investigation.

VII. In February 2010, a terrorist pleaded guilty to conspiring to conduct suicide attacks against the New York City subway system. The terrorist and two co-conspirators planned to travel from the U.S. to Afghanistan to join the Taliban and fight against the U.S. military and its allies. Another U.S. law enforcement agency requested immediate assistance from DHS in investigating the suspected terrorist due to his likely involvement in imminent attack planning. DHS's research indicated that he travelled to Pakistan with two other individuals, who were previously unidentified co-conspirators at the time DHS conducted the research and at the time of their travel. According to DHS, if DHS had deleted the suspect's and others' PNR data after their departure from the U.S.., DHS would not have been able to help

the U.S.. law enforcement agency to identify the co-conspirators and the full scope of the plot and the network supporting it.

VIII. In April 2017, a traveller arrived at a U.S. land port of entry. By reviewing the traveller's historical PNR data from 2012, DHS officers determined the individual had a connection to a recently identified known or suspected terrorist. The linkage between the two travellers was supported by information in the known or suspected terrorist's 2015 PNR. During inspection, DHS discovered that the traveller's phone contained several images of persons holding what appeared to be AK-47 assault rifles, and images of people bound and gagged who appeared to be dead. DHS officers also discovered several images of what appeared to be the traveller brandishing weapons while with a group of fighters. Further questioning confirmed the ties between the traveller and the known or suspected terrorist.

IX. In May 2014, DHS and a foreign law enforcement agency used historical PNR data to investigate two missing women feared to be victims of trafficking and forced prostitution. Based on a review of the victims' historical PNR, DHS and the foreign partner agency linked the two women to a suspected trafficker and to potential co-conspirators, and they also identified another possible victim. Based on this information, DHS was able to identify the suspected trafficker when he attempted to travel again to the U.S. in August 2014, and DHS arrested him.

More examples are available in Annex A and B.

The EU-U.S. Agreement allows PNR data to be retained in an active database for up to five years, but requires such data to be depersonalized and masked after six months. In line with the EU-U.S. PNR Agreement, after 5 years, PNR shall be transferred to a dormant database for a period of up to ten years and PNR data may be repersonalised during these ten years only in connection with law enforcement operations and where there is an identifiable case, threat or risk.

In this respect, the U.S. has provided figures[14] concerning the use of such dormant data over a twelve month period, showing a regular but reduced use of such information. Figures related to information sharing with other authorities show that PNR dataset's age (time since a record was collected from an airline) at the moment of disclosure was below one year in the

[14] Please see Annex B, under *data retention*.

overwhelming majority of the cases. The U.S. authorities noted that older PNR data have proven vital in a number of high profile counterterrorism investigations and prosecutions.[15]

Under the discussions on Article 8(6) of the EU-U.S. PNR Agreement, which states 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, the U.S. noted that the figures shared with the EU team clearly demonstrate the necessity of maintaining dormant PNR data. In particular, the Agreement requires that the dormant data be "subject to additional controls, including a more restricted number of authorised personnel and higher level of supervisory approval before access." It also requires, as noted above, that dormant PNR only be accessed "in connection with an identifiable case, threat and risk." According to the U.S., these controls greatly reduce the number of times dormant PNR would be used.

Although compliant with the Agreement, and given the comparatively reduced number of requests the EU team considers that the U.S. should continuously review the necessity of the dormant database in order to ensure that the use of PNR data remains relevant and necessary for the purposes for which it is collected. The U.S. committed to continue evaluating the utility of dormant PNR data during future joint reviews.

4. CONSISTENCY WITH OTHER INSTRUMENTS

4.1. Other instruments for the collection of travel related data

PNR data remains a critical data element in the identification of serious transnational crime and terrorism. The U.S. team highlighted that without it, it is certain that an increase of illicit or nefarious goods, or individuals that seek to cause harm to the U.S. and the global community through criminal and terrorist acts, will enter or leave the U.S. undetected; when they could have been otherwise prevented through the use of PNR data.

The necessity and peculiarity of collecting PNR data to fight terrorism and serious crime is also identified in relation to other measures available: there is information contained within PNR data that cannot be found in any other type of data collection. This information, like full travel paths, is a unique and critical information source in the identification of serious transnational crime and potential terrorist activity.

[15] See for example the David Headley case, page 58 example 2.

Example: PNR data as the key piece of intelligence

In December 2009, unbeknownst to the U.S. Government, a radicalised individual received explosives training in Waziristan, Pakistan from individuals affiliated with Tehrik-e-Taliban (TTP), a terrorist group based in Pakistan. In February 2010, he arrived in the U.S. from Pakistan. Immediately following a failed detonation of a vehicle-born improvised explosive device at Times Square in New York City on May 1, 2010, DHS, at the FBI's request, used API and PNR data to link him to information uncovered early in the time-sensitive investigation of the failed detonation. DHS also quickly discovered that he had just booked a flight to Dubai. DHS apprehended him at New York's JFK Airport as he was about to board the aircraft for the flight to Dubai. On June 21, 2010, he pleaded guilty to all ten offenses related to his attempt to detonate a car bomb in Times Square and he received a life sentence in prison.

The unique data contained within PNR becomes evident when comparing PNR data to data in other systems containing travel-related information (e.g. Visa data, Advance Passenger Information (API), and Electronic System for Travel Authorization (ESTA) data). For instance, API mostly includes biographic information that is rather 'static' (it does not change substantially over time) and does not show the behaviour of the passenger (as opposed to PNR data where one can see choices made by the passenger, such as baggage information, payment information, date of reservation/issuance of ticket, etc.). Similarly, the other systems created to grant authorisation to travel mainly rely on 'static' biographic information and are occasionally supplemented by some additional 'status' data such as level of education or occupation.

In addition, PNR can be made available much earlier than API data, and hence provides an advantage to law enforcement authorities in allowing more time for its processing, analysis and any follow-up action. Specifically, under the agreement, PNR data becomes available beginning 96 hours prior to departure although an airline may collect it weeks or months ahead of departure. On the other hand API data may not be transmitted until 72 hours before departure and may be much later depending on when the passenger checks in. The additional time to review and analyse the PNR information often proves critical to determinations on possible appropriate actions to be taken.

4.2. Other instruments on PNR

Since the entry into force of the Agreement, new trends and new security threats have emerged and continue to evolve. There is not only a growing interest in the use of PNR worldwide for anti-terrorism and law enforcement purposes, but also newly created international obligations.

At global level, the United Nations Security Council Resolution (UNSCR) 2396, adopted unanimously on 21 December 2017, requires UN Member States to 'develop the capability to collect, process and analyse, in furtherance of ICAO (the International Civil Aviation Organisation) standards and recommended practices, passenger name record (PNR) data and to ensure PNR data are used by and shared with all their competent national authorities, with full respect for human rights and fundamental freedoms'[16]. This Resolution has therefore placed a legal incentive on all UN States to develop effective PNR programmes. The scope of the Resolution, focused primarily on terrorism, being extended to organised crime by Resolution 2482 (2019).[17]

In those instruments, the UN Security Council decided that UN member states must collect, process and analyse PNR for effective border controls to prevent terrorist travel as well as to help security officials make connections between individuals associated to organised crime, whether domestic or transnational, and terrorists, to stop terrorist travel and prosecute terrorism and organised crime. This obligation is binding on all UN Member States and as a result, more countries are expected to soon begin establishing PNR programs. The UNSCR 2396 (2017) also urges ICAO 'to work with its Member States to establish a standard for the collection, use, processing and protection of PNR data'. Against this backdrop, ICAO started working on the development of a standard for the collection, use, processing and protection of PNR data. In March 2019, the ICAO Air Transport Committee (ATC) set up a Facilitation Panel Task Force to consider proposals for Standards and Recommended Practices (SARPs) on the collection, use, processing and protection of PNR data in line with UNSCR 2396. The U.S. participated in this Task Force, alongside several EU Member States, with the Commission representing the EU in an observer capacity. The position to be taken by the EU Member States when participating in these discussions was agreed by means of a Council

[16] Resolution 2396 (2017) - Adopted by the Security Council at its 8148th meeting, on 21 December 2017.
[17] Resolution 2482 (2019) - Adopted by the Security Council at its 8582nd meeting, on 19 July 2019.

Decision (EU) 2019/2107 of 28 November 2019[18] with a view to ensuring compliance with the applicable Union legal framework including the Charter of Fundamental Rights as interpreted in the Court of Justice's Opinion 1/15.

This required the EU Member States to act jointly in the interest of the Union in accordance with the objectives pursued within the framework of PNR policy and promote the inclusion in the ICAO SARPs of a number of principles on the modalities of PNR processing, the protection of personal data and information sharing among law enforcement authorities. Participating Member States and the Commission worked closely with the United States, as well as other nations, to achieve these goals.

A draft version of the PNR standards was approved by the ICAO Facilitation Panel in February 2020 and sent to the ICAO Contracting States for consultation. After a final review by the ICAO Air Transport Committee in May 2020, the SARPs were adopted by the ICAO Council in June 2020. At the moment of drafting this document the SARP is not yet into force and the Union has not taken a formal position in its regard. However, the entry into force of the SARPs create another, more detailed obligation on all States to establish PNR programs and will help ensure both that their programs are effective and that they meet a high standard of data protection.

These developments at international level demonstrate that there is now a global consensus and that it is necessary and appropriate for States to collect and process PNR routinely as part of a modern border management process. This is a significant change in the global environment and international law and, in the near future, the collection and use of PNR by governments to detect crime and terrorism at their borders will be the global norm, not the exception as it was when the EU began negotiating PNR agreements in 2003, beginning with the U.S..

The EU PNR Directive[19]

Within the EU, processing of PNR data constitutes an essential instrument in the common response to terrorism and serious crime and a building block of the Security Union.

---

18 Council Decision (EU) 2019/2107 of 28 November 2019, OJ L 318, 10.12.2019, p. 117. The position of the Union and its Member States has also been set out in an information paper on 'Standards and principles on the collection, use, processing and protection of Passenger Name Record data' that was submitted to the 40th Session of the International Civil Aviation Organisation Assembly.

19 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132.

Identifying and tracing suspicious patterns by processing PNR to gather evidence and, where relevant, find perpetrators of serious crime and their associates and unravel criminal networks is proving essential to prevent, detect, investigate and prosecute terrorist and serious crime offences.

On 27 April 2016, the European Parliament and the Council adopted Directive (EU) 2016/681 on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. This Directive enables EU national authorities to gain direct access to crucial information held by airlines, in full respect of fundamental rights, in particular, data protection rights. It provides all Member States with an important tool for preventing, detecting and investigating terrorism and serious crimes, including drugs and human trafficking and child sexual exploitation. The deadline for the Member States to transpose the PNR Directive into national law expired on 25 May 2018.

Article 20, paragraph 2, of the EU-U.S. PNR Agreement envisages the consultation of Parties if and when an EU PNR system is adopted to determine whether the Agreement would need to be adjusted accordingly to ensure full reciprocity. During the joint evaluation, the EU team showed DHS the key features of the EU PNR architecture. DHS recalled the good, although only occasional, cooperation with EU authorities stemming from these developments. Both parties agreed that the new EU PNR framework provides opportunities to improve operational cooperation between the U.S. and the EU as it now identifies specific counterparts in each EU Member State for handling PNR, i.e. the Passenger Information Unit (PIU) as the dedicated entity entitled to collect and process PNR data. In addition, the PNR Directive also foresees that each EU Member State designate authorities entitled to request or receive PNR from the PIU. Such a list is published in the Official Journal of the European Union and regularly updated by the European Commission. DHS could therefore verify whether requests for information and other types of cooperation under Article 18 (2) of the Agreement come from appropriate EU competent authorities. In this respect the new EU framework on PNR complements and generally aligns with the Agreement.

Further to the U.S.'s visit to the EU in October 2019, the U.S. stated that they had not observed any practices in the PNR programs of EU Member States that require it to exert its rights under Article 20, Paragraph 2. The United States informed the EU that they will continue to monitor developments in the EU to assess whether this situation changes. More generally, the United States applauded the EU's initial progress in establishing PNR

programs, which has led to a more secure and efficient Europe. The U.S. encouraged the EU to continue this work, and in particular, to empower their PIUs to learn from and work collaboratively with third countries to identify and share information on a case by case regarding suspicious and illicit travelers.

As countries around world adopt programs similar to those employed in the U.S. and EU, collaboration between States to protect the air transport system, in full respect for human rights and fundamental freedoms, will become even more critical.

5. SAFEGUARDS APPLICABLE TO THE USE OF PNR

5.1 Validation and review process for the access rights for officials and targeting rules

The users access PNR data at ports of entry and other field locations (by Border Patrol agents), at the NTC, at the CBP headquarters, and within DHS by DHS agents, analysts, and officers in DHS's Office of Intelligence and Analysis (I&A), Immigration and Customs Enforcement (ICE), U.S. Coast Guard, U.S. Citizen and Immigration Services (USCIS), and Transportation Security Administration (TSA). DHS maintains 24/7 operations at over 100 locations in the United States and abroad that are responsible for processing inbound and outbound traveller. Each of these locations maintains three shifts of frontline and supervisory officers who must access PNR to make accurate decisions on whether to admit travellers to the United States. The number of users fluctuates depending on mission need, coverage needed at points of entry, and job responsibilities, but the EU team is of the opinion that the number of authorised users (totalled 16,233 as of 6 August 2019, constituting 6.76% percent of approximately 240,000 DHS employees and 2% of nearly 700,000 sworn law enforcement officers in the United States) remains high. According to the U.S., these figures represent approximately 40 CBP users (at the ports of entry and NTC) per airport shift who over the course of year process 238.7 million travellers. In addition, the U.S. authorities informed the EU that DHS had to increase the number of officers with access to PNR in order to implement the Agreement's requirements for senior official approval to access masked and dormant data.

The U.S. also explained that access to ATS and PNR is limited to those individuals with a demonstrated need-to-know, based on the specific job responsibilities at ports of entry or the

NTC and that such determinations are regularly reviewed. Furthermore, access to PNR is further controlled by providing each user only those accesses required to perform the responsibilities of the position. The ATS database logs and maintains audit trails of what information has been accessed; these logs are maintained and used to support internal audits to ensure compliance with the stated purposes of the system. All officials with access to PNR data undergo initial training and bi-annual training on privacy, policy, and system requirements related to PNR data to access and maintain access to ATS. Users with access have to certify every six months that they have read and understood the conditions and requirements associated with the legal use of PNR data. In addition, CBP promptly removes access of individuals to information, including PNR data, if the individuals no longer require it, for example, when a DHS employee transfers to a new office or position where access to PNR is no longer necessary.

However, the EU team is of the opinion that the number of users with access to the system remains high taking also into account the consistent increase in the number since 2013. The EU team suggests DHS to put in place additional procedures aiming at ensuring that access is only granted under a strict need to know basis and only when the tasks carried out by the officer warrant it.

The U.S. team informed about how targeting rules are developed and implemented by the entrusted users at the NTC and Passenger Analytical Units at individual ports of entry. At the NTC, prior to the creation of the rule, consideration is given to its proportionality and the impact on the operations and the traveling public before implementing them. To accomplish this, each rule is tested against historical data to determine the likely number of travellers who will be referred for further examination. In addition, the NTC rules as well as the supporting intelligence or law enforcement information behind the rules are reviewed quarterly by CBP operational authorities and DHS Privacy Office, DHS Office for Civil Rights and Civil Liberties, and DHS Office of General Counsel. Targeting rules may match against PNR in dormant status, when necessary to identify possible high risk travellers with an association to illicit historical trends. This ensures that the targeting rules are tailored to minimise the impact upon bona fide passengers and that they comply with relevant legal authorities, regulations and policies. This review provides operational and oversight offices with an opportunity to identify and eliminate or deactivate rules that no longer address potential threats. In some cases, the U.S. Privacy Office, the DHS Office of Civil Rights and

Civil Liberties, and the U.S. Office of the General Counsel discussed with CBP whether specific rules may be further scoped to be made more effective.

The U.S. also noted that rules employed by the Passenger Analytical Units at individual ports of entry also have their own safeguards in place to provide a level of oversight and review. First, regional and local level rules have to be approved by senior managers. CBP headquarters recommends these senior managers require an impact assessment prior to approval. Further, during routine operations, when a regional or local level rule matches a traveller, CBP's IT systems send a notification to regional or local, supervisory CBP personnel to review the match. Additional research and analysis is conducted by the onsite officer on duty, and, based on all available information, a decision is made whether to send the traveller for a secondary inspection. In addition, NTC conducts an audit of Passenger Analytical Units developed rules twice a year and requires field and NTC users to certify that a rule is still valid and necessary. If no response is received, the rule is deactivated.

DHS does not develop rules at individual ports of entry for counterterrorism purposes but only utilizes them to address issues specific to a point of entry, such as localised smuggling trends. The EU team considers that rules designed at regional or local level do not benefit from the robust review system used for rules created at the national level, although they adhere to specific guidelines. In that regard the EU team recommends the U.S. including additional safeguards such as the generalisation of prior impact assessments before the approval of new rules.

The individual ports of entry generally develop rules in the same way as individual PIUs in EU Member States. DHS clarified that local rules are not subject to the same review process as national level counterterrorism rules because points of entry developed rules do not directly impact the traveling public. When a passenger matches a rule by a given port of entry, he or she is not automatically referred for a thorough exam. Instead, each rule match is reviewed by an onsite officer who takes into consideration the totality of information known about the passenger in addition to the rule match to decide if a secondary inspection is warranted. Nonetheless, rules for regional and local users have to be approved by Assistant Directors with an understanding of local illicit trends or their designees. Impact assessments are also a recommended best practice for regional and local rule requesters. If no response is received, the rule is deactivated. A very limited number of CBP users can access rule firing information; only persons in positions that have a need to know receive access; users who do

not already have access to PNR information cannot access it via this method. In fact, not every officer that receives rule matches/results has access to the actual rules.

During the visit, the U.S. informed the EU team that there are no specific rules on providing feedback on the impact of targeting rules in production. Against this background, the EU team suggests that systematic feedback from the law enforcement community about the follow up of the cases referred by CBP could further improve the quality of the targeting rules. The EU team also considers important that there is a validation and a review process of access rights and of the new and existing targeting rules implemented at all the locations. Future joint reviews should further examine the use by rules of PNR data in dormant status.

5.2 Sensitive data

According to Article 6 of the Agreement 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. The U.S. team informed the team that no sensitive data has been processed other than for the purposes of testing of the proper implementation of the safeguards designed to confirm this statement. The U.S. team confirmed that certain codes and terms that may be in a PNR but that have been identified as "sensitive" are automatically filtered out and blocked by CBP in the passenger mode of ATS and that ATS generates a daily email informing CBP management whether or not any sensitive data elements have been accessed.

Article 6 of the Agreement provides for the deletion of sensitive data no later than 30 days from the last receipt of PNR containing such data by DHS, unless it is used for a specific investigation, prosecution or enforcement action, in which case it may be retained for the retention period of that case. According to the U.S., all sensitive data have been deleted in accordance with the Agreement, which was internally verified during two separate tests of sensitive word data in February 2018. CBP conducted a test on 21 February 2018 using PNR for travel that occurred on 7 February 2018. The test confirmed that ATS automatically filters out sensitive word data from PNR. Also on 21 February 2018, but separate from the test on the 7 February 2018 PNR, CBP verified that ATS permanently deletes sensitive word PNR data after 30 days in accordance with the EU-U.S. PNR Agreement. These tests follow similar tests conducted on August 18, 2015 with the approval of the Deputy Commissioner of CBP. In addition, the U.S. confirmed that no sensitive data has been processed, other than for the purposes of testing the proper implementation of the safeguards designed to confirm this statement.

The EU team encourages DHS to continue to comply with the requirements of Article 6 of the Agreement including the employment of automated systems to filter and mask out sensitive data from PNR and its deletion not later than 30 days from the last receipt of PNR containing such data. In addition, it recommends the U.S. to put in place mechanisms aiming at immediately deleting sensitive data if received.

The U.S. however, stated that at first this recommendation would not address an identifiable privacy harm to the individual or situation of non-compliance with the Agreement. In addition, the U.S. expressed its opinion that the broad definition of sensitive data includes information that may be necessary to accurately identify an individual or tie a traveller to specific intelligence or law enforcement information in exceptional circumstances where the life of an individual could be imperilled or seriously impaired. DHS confirmed that it filters out sensitive data and has never used it. The U.S. further stated that the U.S. is fully compliant with this provision and there is no evidence to the contrary and that these measures protect individual privacy to an exceedingly high level. The U.S. further commented that any marginal privacy gained by immediately deleting sensitive data is outweighed by the potential risk of missing serious threats.

5.3 Mechanisms to ensure transparency, access, correction and redress

DHS provides transparency under Article 10 of the Agreement, by providing the travelling public with information on its collection and use of PNR. Such information is readily available on various DHS public websites (i.e. DHS Privacy Office and CBP) as well as through other official websites. General public notice is additionally provided through the publication of a System of Records Notice for the ATS and via websites of U.S. Embassies located in the EU. The Privacy Impact Assessments for the ATS, which is the system that maintains PNR, are posted on DHS public website. DHS further publishes the actual PNR Agreements that DHS has entered into, a CBP PNR Privacy Policy, and a list of Frequently Asked Questions and Answers.

The guidance provided to the affected carriers encourages 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, some with links to the government sites provided. CBP works with carriers to incorporate notices into their documents and websites, which travellers may see at the time of booking (more detailed

information provided by the U.S. in the replies to the questionnaire under Safeguards and Q7).

DHS Traveller Redress Inquiry Program ('TRIP') remains a single point of contact for individuals, regardless of citizenship or residency, who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like airports – or crossing U.S. borders From June 2015 to June 2019 there were only three EU inquiries including a reference to the travellers' PNR, each of which was sufficiently resolved as detailed below.

In 2016, an EU DHS TRIP inquiry went through the process and resulted in a letter to the traveller. There was no additional appeal from the traveller. In 2018, an EU DHS TRIP inquiry was received, but the traveller did not respond to a DHS request for additional information to process the request. There was no additional appeal from the traveller. In 2019, DHS Privacy Office received an inquiry from an EU traveller, which was determined not to be a DHS TRIP inquiry but was handled as a Freedom of Information Act (FOIA) request. There was no additional appeal from the traveller. All of these DHS TRIP inquiries were resolved and neither the CBP Customer Service Centre nor DHS Chief Privacy Officer have ever received any complaints of misuse of EU PNR data.

The U.S. informed that DHS has never received a request for correction or rectification of PNR data from EU citizens, as provided under Article 12, since the Agreement went into force in 2012. They also noted that, DHS nevertheless has sufficient mechanisms in place, in accordance with Article 12, to handle such requests. In addition, DHS practices exceed the requirements of Article 12 by including an automated mechanism to update its records when new information becomes available in order to avoid any future incident of misidentification stemming from the original record.

The EU team recommends the U.S. to assess possible ways to improve cooperation between DHS and air carriers concerning transparency and the exercise of passenger rights as recognized in the Agreement.

5.4 Oversight

The U.S. provided detailed explanations of how Personally Identifiable Information is processed by DHS in accordance with DHS policy and U.S. law. The U.S. has as a number of laws that govern privacy, and multiple entities in various branches of government that

conduct oversight of the collection and use of Personally Identifiable Information, including PNR. This approach begins with the U.S. Constitution which grants enumerated powers to the Executive, the Legislative and the Judicial branches of government, thereby creating a system of checks and balances. In particular, the U.S. Constitution does not authorise the Executive Branch to play a formal role in the legislative process or to direct Congressional oversight of the Executive branch. The U.S. Constitution established three separate, independent, and co-equal branches:

- The Executive Branch places privacy officers and officers for civil rights and liberties, government lawyers, and Inspectors General in each Department or agency. It also has a specialised entity named the Privacy and Civil Liberties Oversight Board, which initiated an oversight project in June 2019 related to the use of PNR.[20] This Branch implements the laws passed by Congress including the Privacy Act and the Freedom of Information Act.

- In the Legislative Branch, the U.S. Congress may pass or change U.S. laws, investigate the Executive Branch, issue reports, and withhold funding from the Executive branch based on negative findings in an investigation of an agency's handling of personal information. The oversight authorities of the Executive Branch are all required to keep Congress informed of their activities and to respond to congressional requests for information. An additional body, the Government Accountability Office, is an independent, nonpartisan agency that works for Congress under the Comptroller General of the U.S. It has the authority to audit and/or investigate Executive Branch programmes and activities, including those related to privacy or civil rights and liberties and issue reports with its finding and recommendations.

- The Judicial Branch provides independent judicial review and redress.

The Chief Privacy Officer of DHS has statutory authority and powers to investigate any departmental program under 6 USC. § 142, which allows her to fulfil the requirements of Article 14 of the Agreement. She may also refer any issue concerning the use of PNR to the

[20] https://www.pclob.gov/newsroom/20190626.html.

Congress or to DHS Office of the Inspector General. For serious cases of misconduct, she may refer the matter to the Department of Justice, which may issue an indictment against the individual. The U.S. representatives also noted the differences between the EU and U.S. respective EU and U.S. oversight systems while ensuring to demonstrate that, from a performance-based perspective, DHS protects the data in line with the requirements of the Agreement.

Concerning the application of Article 14(2), an independent review by DHS Inspector General, the General Accountability Office, or Congress, has not taken place since the Agreement was signed. According to the U.S., this is likely due to DHS compliance with the Agreement's terms, as verified by the prior independent and extensive joint reviews conducted by the Commission, and the lack of complaints from the public. Nonetheless, DHS Privacy Office has conducted five internal reviews, in addition to the three joint reviews of the Agreement with the EU. In addition, the CBP Privacy Officer, in cooperation with DHS Chief Privacy Officer, carries out ongoing oversight of the processing activities by ensuring that privacy compliance documentation is transparent and up to date. Since the implementation of the Agreement, the System of Records Notice has been updated once and the Privacy Impact Assessment has been updated four times. These documents are both available to the public.

The U.S. stated that it fully adheres to Article 14 of the Agreement and meets the EU legal requirements for independent oversight through the activities mentioned above. The EU team considers oversight activities as one of the key elements of the Agreement to ensure full compliance with the privacy safeguards and welcomes the continuous involvement of the Department's Privacy Officer on guidance and oversight activities. However, the EU team also considers essential that oversight activities are carried out in accordance with the requirements not only of Article 14(1) but also of Article 14(2) of the Agreement.

5.5 Method of PNR transmission

According to Article 15 of the Agreement, carriers shall be required to transfer PNR to DHS using the 'push' method, 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. On a case-by-case basis, DHS may require a carrier to transmit PNR between or after the regular transfers. In order to respond to a specific, urgent, and serious threat, DHS may require carriers, on a case-by-case basis, to otherwise provide access when

the carriers are unable for technical reasons, to respond in a timely manner. This in practice means using a 'pull' method to obtain PNR from carriers.

At present, all carriers affected by the Agreement are set up to push PNR. DHS has relied on the pull method in specific cases of carriers not being technically capable of transmitting the data for example when an airplane is unexpectedly rerouted to land in the U.S...

Following the joint review from 2017, DHS was recommended to improve the statistical collection and reporting related to the number of "pulls" of data collected under the Agreement. The EU team considers that, while this practice is in line with the provisions of the Agreement, the use of 'pulls' is more intrusive as requires the authorities to enter into the air carriers database. Hence, the use of this method must be regularly assessed. It should be adhered to only in fully justified and fully documented cases and minimized in full accordance with the conditions set out in Article 15.

5.6 Onward sharing to U.S. entities outside of DHS

The PNR information collected in the context of the Agreement may be made available to other government agencies outside of DHS for law enforcement or public health purposes only after DHS determines that the recipient has a need to know the information to carry out functions consistent with the "routine uses" included in the ATS System of Records Notice,[21] 77 Fed. Reg. 30297 (May 22, 2012)[22] and have sufficient capability to protect it consistent with the requirements of the Agreement. In accordance with U.S.'s Privacy Policy, and consistent with Article 16 of the Agreement, PNR information is not shared outside of DHS unless the receiving agency has a need to know the information for purposes specified in the Agreement and can ensure the information will be protected under the safeguards set out in the EU-U.S. PNR Agreement. The CBP ATS system of Records Notice lists a number of agencies that may request and, if consistent with the requirements and purposes specified in

---

21 Available at https://www.govinfo.gov/content/pkg/FR-2012-05-22/html/2012-12396.htm.

22 For instance, Routine Use G permits disclosure to: "appropriate federal, state, tribal, local, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where CBP believes the information would assist enforcement of applicable civil or criminal laws." Further, Routine Use H permits disclosure: "To federal and foreign government intelligence or counterterrorism agencies or components where DHS becomes aware of an indication of a threat or potential threat to national or international security, or to assist in anti-terrorism efforts." And Routine Use L permits disclosure to: "To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate in the proper performance of the official duties of the officer making the disclosure."

the Agreement, receive PNR data, including federal, state, tribal, or local organizations responsible for investigating and enforcing civil or criminal laws.

The EU was informed about the instances in which PNR data have been shared with other government authorities. Between 2012 and the Joint Evaluation in September 2019, PNR records have been disclosed to domestic authorities in 12.189 instances, 98% of which were made to other U.S. federal agencies and 2% to state or local agencies[23]. Only two percent of these disclosures to domestic authorities (242 total) were made to U.S. state or local level agencies. In almost all cases, DHS shared the information for purposes of fighting terrorism and serious transnational crime, with only few cases in which the purpose was the protection of health or public safety. The U.S. also provided information about the number of records shared between 2015 and 2019 according to the age of the PNR at the time of its onward disclosure. In that regard, in almost 80% of the cases, the PNR data requested and shared was only a year or less old. The requests resulting in PNR data shared older than 5 years are small in relation to the total amount.

Requests for PNR data by a non-DHS requestor, must be submitted in writing and must describe the information requested, the reason for the request and how the information will be used. All requests must be approved by the CBP Privacy Officer or by an individual who has been delegated by the authority to approve such requests. The written authorisation letter by CBP to the non-DHS requestor as a matter of course restricts the use of the PNR data consistent with the requirements and purposes specified in the Agreement, including requiring the non-DHS requestor to afford the PNR data equivalent or comparable safeguards as set forth in the Agreement. In addition, the non-DHS requestor is required to seek the express, prior written authorization of CBP to further share the PNR data or to use the PNR data for any other purpose. All sharing of PNR data is logged and is subject to routine audits by DHS Privacy Officer.

Article 16 of the Agreement requires that data may be shared only after a careful assessment of the purpose of the request to ensure that the receiving authorities afford equivalent or comparable safeguards to PNR data as set out in the Agreement. The U.S. informed the EU team that current practices are in their view consistent with the conditions of Article 16(1)(c). Disclosures of PNR data include a cover letter that specifically limits how the information

[23] More information can be found in ANNEX B, under *Information sharing.*

may be used and what, if any, onward disclosures may occur. The restrictions provided in the cover letter are consistent with Article 16(1)(c). The EU team welcomes the procedures in place, but is of the opinion that those procedures could be enhanced to improve the quality and consistency of the checks related to the existence of comparable safeguards, as per Article 16(c).

5.7 Onward transfers

According to the information received from the U.S., 70 PNR records of EU residents were disclosed to 19 countries, eight of which are EU Member States (the list of countries is available in Annex B). DHS ensures through the terms of a Memorandum of Cooperation or other written arrangement that the foreign government will treat such data as sensitive and confidential, will not provide such data to any other third party without the prior written authorisation of DHS, and that the data will be treated with equivalent and comparable safeguards as set out in the Agreement. Any access to PNR data is contingent upon an express understanding that the foreign government treat such data accordingly.

In particular, U.S. law requires that DHS share information with a foreign counterpart only if DHS obtains assurances that the information will be held in confidence and used for a law enforcement purpose consistent with the reason for which it was provided (19 USC. § 1628(b)). Further, U.S. law prevents DHS from sharing further information with any foreign law enforcement agency that does not adequately protect information. DHS implements both U.S. law and the PNR Agreement through a combination of formal agreements and case-specific assurances.

Also, DHS requires that a cover letter be included with the transfer of PNR data to a foreign authority that outlines the recipient's responsibility to protect the provided PNR consistent with the Agreement among other conditions, such as prohibiting onward transfer to any third party, such as a third country, without the express prior written authorization of DHS. This letter requires the receiving country to provide specific protections in addition to the general protections afforded under any applicable international agreement, such as the Mutual Legal Assistance Treaty or Customs Mutual Assistance Agreement in place between the U.S. and the receiving country. Should a recipient fail to adhere to these terms DHS will not share further information with the country pursuant to 19 USC. § 1628(b).

In addition, the U.S. illustrated by the means of examples the exchange of PNR data with the EU Member States and Europol.

Examples:

I. DHS used PNR data to support the investigation into a known European terrorist attack. In support of this investigation, historical PNR data led to the identification of several previously unknown suspects. The close coordination between U.S. law enforcement agencies and the EU Member State enabled security services to prevent follow-on attacks by associated individuals, similar to the follow-on attacks in Brussels in 2016 following the November 2015 attack in Paris.

II. In 2017, DHS supported an EU Member State's investigation of a terrorist attack in its territory. DHS analysis of U.S. historical PNR data dating back to 2014 identified one suspect with links to two other previously unknown individuals. DHS provided these leads to the Member State's law enforcement partners for use in the investigation into the attacks.

III. On October 20, 2018, DHS liaison officer at Europol received a request to support an EU Member State's investigation on subjects that were identified as being involved in an armed robbery. DHS uncovered and shared additional information and leads contained only in historical PNR data to support the investigation.

IV. In November 2014, DHS supported an investigation by an EU Member State by providing historical PNR data that resulted in the arrest of six criminals from Asia operating a smuggling ring in the EU. A review of historical PNR pointed to a single employee of a major European airline. Further review identified ten fraudulent identities used by the smuggling ring in fifteen smuggling attempts, thirteen of which were successful. DHS developed and provided evidence to the EU Member State, which then used the evidence to arrest the individuals through a joint operation. The EU Member State also adjusted domestic security procedures to reduce its vulnerability to the crimes identified in this investigation.

More examples are available in Annex A and C.

Article 17 of the Agreement requires that data is shared with third countries only after a careful assessment of the purpose of the request and when ensuring that the receiving authorities shall afford to PNR equivalent or comparable data privacy protections as set out in the Agreement.

The EU team welcomes the procedures in place but it is of the opinion that those procedures could be improved regarding the checks related to the existence of comparable data privacy protections, as per Article 17 (2) of the Agreement.

6. DATA PROTECTION SAFEGUARDS AND THE COURT'S OPINION ON THE ENVISAGED CANADA PNR AGREEMENT

Introduction

In the course of the joint evaluation, the teams discussed the most important legal development since the entry into force of the Agreement, i.e. the Court's Opinion 1/15[24] on the envisaged PNR Agreement with Canada. This Opinion lays down the following requirements (summarised) in order to ensure compliance of this Agreement with the EU Charter of Fundamental Rights:

- The purposes for which PNR data may be processed should be spelled out clearly and precisely;
- The PNR data elements to be transferred should be determined in a clear and precise manner;
- As long as passengers are in the country or are due to leave, the systematic retention and use of their PNR data (in the case of Canada for 5 years) is allowed. However, PNR data should be deleted after passengers' departure unless a risk assessment based on objective evidence indicates that certain passengers present, or specific categories of PNR data indicate, the existence of a risk in terms of the fight against terrorism and serious transnational crime;
- The use of PNR data for other purposes than security and border control checks should be subject to prior independent review carried out either by a court or by an independent administrative body, the decision of that court or body authorising the use being made following a reasoned request by those authorities, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime;
- Individuals should be notified of the use of their PNR and informed about their right to seek administrative or judicial redress;
- The processing of sensitive data shall be prohibited;

[24] Opinion 1/15 of the Court (Grand Chamber), ECLI:EU:C:2017:592.

- Automated processing of PNR data may only take place based on non-discriminatory, specific and reliable models and criteria. The databases used for matching purposes must be limited to those used in relation to the fight against terrorism and serious transnational crime.
- The onward transfer of PNR data to other government authorities should be subject to appropriate safeguards and, in case of disclosure to another third country, limited to countries which have concluded an equivalent Agreement with the EU or are subject to a decision of the Commission finding that the country ensures and adequate level of protection within the meaning of EU law (adequacy decision);
- Oversight of compliance with the Agreement shall be exercised by independent public authorities/an independent supervisory authority with effective investigative and enforcement powers.

U.S. considerations of the Court's Opinion

The U.S. considers that the Court's Opinion has no direct legal effect on other PNR instruments, including the EU-U.S. PNR Agreement. In particular, the U.S. explained that in their view the Court of Justice did not have the benefit of having the complete evidence regarding the use of PNR data – including retained PNR data – to protect the public. Thus, the U.S. further clarified that in addressing the PNR data retention provisions of the envisaged EU-Canada PNR Agreement, the Court of Justice explained that its ruling relied heavily on the information presented by the EU Council and the European Commission regarding the average lifespan of international serious crime networks. In speaking of the retention period provided in the EU-Canada PNR Agreement, the Court of Justice noted, "furthermore, the Council has not provided any justification, based on objective criteria, as regards the choice of such a period."

According to the U.S. such objective data exist with regard to the EU-U.S. PNR Agreement. In fact, DHS considers that it has demonstrated how it has successfully utilized historical PNR data to solve many high-profile counterterrorism cases in the U.S., as well as to assist EU authorities in responding to terrorist acts committed on EU soil. The U.S. stated that this evidence demonstrates the importance of retained PNR data as such data provides vital information not otherwise available to law enforcement agencies.

The U.S. team also highlighted the fact that, following the Opinion, PNR data have been recognized as a useful tool for border control and fighting terrorism. The U.S. representatives

also stated that, while recognizing the obligation of the EU to respect the applicable legal framework, the differences between the respective legal systems as well as the operational perspective need to be taken into account. They also reaffirmed their belief in the effectiveness of the agreement and on the PNR system in general in the light of almost 30 years of experience.

The U.S. further noted that the 2017 European Court of Justice Opinion regarding the envisaged EU-Canada PNR Agreement is not only limited to the facts before the Court, but also must now be read against the backdrop of the evolving international practices involving PNR. Considering also the growing international consensus regarding the need for retention and use of stored PNR and in addition to the adoption of UNSCRs 2396 and 2482, as well as the ICAO developments discussed above, at least fifty-two countries –--- currently collect and process PNR.

Assessment by the EU team

The EU team remarked that, it is nonetheless important to evaluate the EU-U.S. PNR Agreement also against the Court's Opinion.

The joint evaluation teams assessed the relevant safeguards that the Agreement already contains for the use of PNR, in particular:

- PNR data is being used for the prevention, detection, investigation and prosecution of terrorist offences or serious transnational crime and on a case-by-case basis where necessary, in view of a serious threat and for the protection of vital interests of any individual if ordered by a Court;
- The obligation for the US to provide to competent authorities of the EU Member States and Europol and Eurojust analytical information obtained from PNR;
- Safeguards applicable to the use of PNR, including strong data security and integrity requirements;
- Rights of access, correction or rectification and erasure and the possibility for EU citizens to obtain administrative and judicial redress under the terms of the Agreement;
- Review and oversight by authorities that have proven records of autonomy and can refer cases of violation of this Agreement for prosecution or disciplinary action;

- Conditions on the processing of sensitive data. PNR data are kept in an active database for up to 5 years. After the first 6 months, all information which could be used to identify a passenger are "depersonalized", meaning that data such as the passenger's name or her/his contact information are masked to the user. After the first 5 years, the data are moved to a "dormant database" for up to 10 years, with stricter access requirements for U.S. officials. In accordance with Article 8(4), following the dormant period, data retained, must be rendered fully anonymised, by deleting all information that could serve to identify the passenger to whom PNR relate, without the possibility of repersonalisation.

In addition, the U.S. authorities have explained that:

- All of the activities undertaken with PNR data are performed for the purposes outlined within the Agreement.
- No sensitive data has been accessed or used (see above under Chapter 5.2).
- Non-discriminatory targeting of individuals is based on specific and reliable pre-established models and criteria (see above) in order to identify those "who might be under a 'reasonable suspicion' of participation in terrorist offences or serious transnational crime."[25] The U.S. considers that is precisely the case under the EU-U.S. PNR Agreement. As demonstrated by the U.S., historical PNR data plays a prominent and indispensable role in the development, testing, evaluation, and approval of effective targeting rules under the EU-U.S. PNR Agreement. These rules are developed by taking account, in line with the observation of the Court of Justice, "statistical data and international research",[26] much of which DHS obtains from analysing historical PNR data.
- As regards onwards transfers to third countries, the U.S. reassured that through the terms of a Memorandum of Cooperation or other written arrangement with Foreign Authorities, these latter will treat such data as sensitive and confidential, they will not provide such data to any other third party without the prior written authorization of DHS, and will afford to the data equivalent of comparable safeguards as set out in the Agreement (see above, under 5.6).

---

25 *Id.* ¶ 172.
26 *Id.* ¶ 174.

- All requests for PNR data from other Government authorities are logged and auditable, with assurance activities undertaken on a regular basis by internal relevant Departments. CBP maintains records of requests for PNR data from U.S.-domestic Government and foreign Government authorities and logs all sharing of PNR data. Requests for PNR data and sharing of such data are subject to routine audits by the CBP Privacy Officer. In addition to the system-generated record of disclosures of PNR data, the CBP Privacy Officer maintains a separate record of disclosures to foreign Government authorities, which are retained to facilitate oversight, audit, and safeguarding practices. Both the original logs and the CBP Privacy Officer's review may be audited by the DHS Chief Privacy Officer.
- DHS further stressed that it is subject to robust layered oversight and that multiple competing authorities within the Executive, Legislative, and Judicial Branches oversee the data protection and privacy of personal information held by the Department.
- In addition, the U.S. authorities provided information showing in their view, that the retention of historical PNR data also of passengers that have left their country is necessary to create and preserve the knowledge of the criminal phenomena and the possibility to detect associations between past and current known and/or unknown criminals and terrorists (please see examples provided in Chapter 3 and Annex B of the present document).

The EU team recognises the efforts of the U.S. authorities in meeting the requirements of the Agreement from 2012 in both technical and organizational aspects, as well as the further improvements resulting from adopting the recommendations stemming from internal oversight activities and the joint reviews. The EU team notes that despite the numerous safeguards contained therein, several aspects of the Agreement are not fully in line with the Opinion 1/15 of the Court of Justice on the envisaged EU-Canada PNR Agreement, as the U.S Agreement was concluded before the Court delivered its Opinion. These concern the:

- retention of PNR data after the air passengers' departure,
- limitation to databases for matching purposes only to those used in relation to the fight against terrorism and serious transnational crime,
- processing of sensitive data,

- notification to passengers in case their data is used during their stay and after their departure,
- rules for onward sharing and onward transfers, especially to other third countries, as well as
- oversight by an independent supervisory authority and
- the prior independent review of the use of PNR data.

7. CONCLUSIONS

The information gathered in the context of the joint evaluation confirms the added value and operational effectiveness of the Agreement in the fight against terrorism and serious transnational crime. The EU welcomes DHS's commitment to ensure compliance with the Agreement's terms, as noted in the 2013 and 2015 Joint Reviews, as well as the Agreement's proven effectiveness in providing procedural and substantive safeguards to PNR data in line with the EU-U.S. PNR Agreement. Examples provided during the evaluation have shown that PNR, including historical PNR, being a **unique dataset**, have been critical to prevent the return of foreign terrorist fighters and to combat in particular drug crimes and child exploitation.

During the joint evaluation, the U.S. authorities have provided material to show the **necessity** of historical PNR data to create and preserve the knowledge of how terrorists and criminals use travel to commit illicit acts, which itself further aids border inspections and investigative matters. Numerous case studies and examples have been provided to this end, many of which are included in this document. Besides having demonstrated its **operational value and effectiveness**, the EU-U.S. PNR Agreement objectives are consistent with the international obligations to collect, process and analyse PNR data for effective border controls to prevent terrorist travel as well as to help making connections between individuals associated to organised crime, and prosecute terrorism and organised crime.

The EU team recognises the efforts made by U.S. to comply with the requirements of the Agreement from 2012 in both technical and organisational aspects, and recommends DHS to continue its efforts to i) limit the number of users who have access rights to PNR data, ii) comply with the requirements on sensitive data and to put in place mechanisms aiming at immediately deleting sensitive data if received, iii) review the necessity of keeping PNR in a

dormant status, iv) improve the systems in place concerning onward case-by-case sharing to U.S. entities outside of DHS and to other third countries, v) ensure feedback concerning the effectiveness of targeting rules at a regional and local level and vi) ensure that the requirement, in specific cases, to air carriers to provide access to DHS is regularly assessed and overly minimised.

As a result of the comparison of the Agreement and Opinion 1/15 of the Court of Justice on the envisaged PNR Agreement with Canada, the EU team noted that despite the numerous safeguards contained therein, several aspects of the Agreement are not fully in line with Opinion 1/15 of the Court of Justice, as the U.S Agreement was concluded before the Court delivered its Opinion. These concern the retention of PNR data, the processing of sensitive data, notification to passengers, prior independent review of the use of PNR data, rules for domestic sharing and onward transfers, independency of oversight and the sole use of databases in relation to the fight against terrorism and serious transnational crime for cross-checking of PNR data.

ANNEX A
CASE STUDIES

Child Abduction and Sexual Exploitation

In 2015, DHS learned that a court order restricted a traveler from taking his children outside of the U.S. without prior approval from the court. DHS later saw a travel reservation via PNR for the traveler and his children to travel to a foreign country. DHS worked with local authorities to detain the traveler. Local authorities arrested the traveler and placed his children with the appropriate child protection entity.

In 2018, DHS used PNR to identify a traveler traveling from a foreign country to the U.S. based on available information may be involved the sexual exploitation of children. DHS/CBP referred the traveler for secondary inspection, which led to the discovery of child sexual exploitation material. The traveler was arrested.

Drug Trafficking

In August 2019, DHS identified a previously unknown narcotics trafficker who had been receiving and distributing shipments of hundreds of kilograms of cocaine in the U.S. and the EU. DHS used historical and current PNR data to identify the trafficker. In October 2019, DHS and other U.S. law enforcement agencies arrested the trafficker upon return from the EU to the U.S. After the arrest, the trafficker provided information to U.S. law enforcement that he had been facilitating a 3,200-kilogram shipment of cocaine to the EU.

In January 2020, a U.S. law enforcement agency requested DHS assistance in identifying an EU citizen suspected of coordinating narcotics shipments to the EU. Using information provided by the agency, DHS researched historical and current PNR data to identify the subject. DHS provided the information to the appropriate EU Member State for further investigation and support.

Since the beginning of 2020, DHS has used historical PNR data along with information from international partners to identify over 40 suspected narcotics couriers. Of those couriers, 10 have already been intercepted and found carrying many kilograms of cocaine or heroin. DHS

has shared information on all identified suspected couriers with appropriate international partners to assist their efforts with countering drugs trafficking.

Fraud

In February 2017, PNR indicated that an alleged EU citizen scheduled to travel from the EU to the U.S. matched information identifying him as a high risk for fraud. DHS/CBP determined that the individual had fraudulent documents and was, in fact, a citizen of different foreign country. DHS recommended that the airline not board the traveler.

In 2017, DHS identified, via PNR, two travelers scheduled to travel to the U.S. matching information to possible document fraud. Working with foreign security at the airport, DHS determined that the travelers possessed fraudulent passports. The local authorities of the foreign country apprehended the traveler who admitted to being nationals of a different foreign country.

In 2017, an EU citizen arriving from the EU at a U.S. airport was referred for secondary inspection based on PNR indicating an association to a known fraud ring that uses credit card skimming machines. During the inspection, DHS discovered a picture of a credit card skimming machine. DHS/CBP found the traveler inadmissible and returned him to the EU.

In 2017, an EU citizen arriving from the EU at a U.S. airport was referred for secondary inspection based on information discovered in PNR. During the inspection the traveler admitted to coming to the U.S. to work illegally. DHS/CBP refused entry of the traveler and returned him to the EU.

Human Trafficking/Human Smuggling

In June 2019, DHS received information about a known alien smuggler moving aliens from the EU to the United States. DHS identified two previously unknown associates of the smuggler, who were facilitating the smuggling, based solely on information contained in PNR data. DHS coordinated with the Department of State to revoke the nonimmigrant visas for the associates.

Counterterrorism

In 2019 a U.S. citizen travelled to the U.S. from Europe. DHS/CBP referred him for inspection because his historical PNR matched an illicit trend used by known or suspected

terrorists. The subject claimed that he had been overseas for a few years attending school and working. When asked if he knew anyone involved in the Syrian conflict, he stated that he attended a mosque that was soliciting funds to support the conflict in Syria. During the inspection, DHS discovered in his electronic devices photos of weapons, of the subject aiming a gun at someone, and of a video of militants wearing ISIS patches. Based on this inspection, DHS referred him to law enforcement for further investigation.

In 2016, a foreign passenger arrived at a U.S. airport was referred for secondary inspection because his PNR matched an illicit trend used by known or suspected terrorists. During the inspection, DHS discovered terrorist propaganda and videos of a known fundraiser for a terrorist organization and of an execution. DHS found him inadmissible and referred him to law enforcement for further investigation.

ANNEX B
Questionnaire[27] for the Department of Homeland Security and replies

Questions of general nature

Q1: What has the wider impact of the Agreement been on the travelling public? Have less people been physically stopped as a result of the use and processing of PNR?

The transfer, processing, and analysis of PNR data under the Agreement facilitates the expeditious entry of the overwhelming majority of travellers who do not pose a threat to public safety. It also contributes to the effective and accurate identification of individuals who should undergo further inspection upon arrival. It complements other information about a traveller and their journey such as Advance Passenger Information (API), visa applications, Electronic System for Travel Authorization (ESTA) applications, and biometrics to provide a complete and accurate picture of the traveller's identity and means of travel. When processed and analysed along with other information, such as the Terrorist Screening Database (TSDB), past enforcement actions and known or suspected illicit trends, it helps the U.S. Department of Homeland Security (DHS) to limit inspections to travellers posing higher relative risk, thereby expediting the admission of all other travellers. Without PNR data, DHS Officers would need to undertake much more intrusive and time-consuming interviews and inspections of each and every traveller, significantly delaying passengers and the operation of the international air transportation system. PNR data allows DHS to focus on high-risk individuals, thereby reducing passenger wait times and inspections at ports of entry for nearly all travellers to a few minutes or less. The negative impact of not having PNR data on passengers can be seen during a recent DHS system outage which increased wait times at ports of entry nation-wide to multiple hours per passenger.

Q2: What proportion of people subject to closer questioning or examination have led to a detention / arrest / seizure or further action?

Such statistics are Law Enforcement Sensitive and cannot be publicly released as part of this survey. During the Evaluation meeting, the U.S. Delegation provided additional information about PNR's contribution to security.

[27] The European Commission sent a questionnaire to the U.S. on 2 August 2019. The Department of Homeland Security provided written replies to the questionnaire on 9 January 2020.

Q3: In order to assess the necessity and proportionality of PNR processing under the Agreement, can you please indicate to what extent is the EU-U.S. agreement still relevant for the fight against terrorism and serious transnational crime?

The collection, processing, and analysis of PNR data remains a critical tool for effective national border security and controls, as recognized by the United Nations Security Council in Resolution 2396 and Resolution 2482. PNR data serves at least four critical functions. First, PNR data helps border officials to identify individuals traveling to or from their territory who may have a nexus to terrorism or transnational crime. Second, PNR data contributes to the accumulation of important historical information for use in border inspections and criminal investigations. Third, PNR data improves the government's understanding of how terrorists and criminals use travel to commit illicit acts, which then further aids border inspections and investigative matters. Fourth, PNR data often contains contact information that government health officials may need to notify travellers in an emergency, such as exposure to deadly diseases during a pandemic. Because the Agreement provides air carriers with a legal basis under EU law for complying with the U.S. legal requirement to transfer PNR data to DHS, the Agreement remains vital.

Q4: What is the specific added value obtained through the PNR collection which is not available through other type of data collections?

PNR data contains elements that are not available through other means, such as API. Some of these elements include additional data and other identifiers that are used in risk assessments as well as to validate the travel of law-abiding travellers. These additional data points assist DHS in identifying high risk travellers who are not otherwise known to law enforcement agencies and are critical in carrying out the anti-terrorism and law enforcement mission of DHS.

Example 1: In December 2009, unbeknownst to the U.S. Government, Faisal Shahzad received explosives training in Waziristan, Pakistan from individuals affiliated with Tehrik-e-Taliban (TTP), a militant extremist group based in Pakistan. In February 2010, Shahzad arrived in the U.S. from Pakistan. Immediately following a failed detonation of a vehicle-born improvised explosive device at Times Square in New York City on May 1, 2010, DHS at the FBI's request used PNR data to link Shahzad to information uncovered early in the time-sensitive investigation of the failed detonation. DHS also quickly discovered that Shahzad had

just booked a flight to Dubai. DHS apprehended Shahzad at New York's JFK Airport as he was about to board the aircraft for the flight to Dubai. On June 21, 2010, Shahzad pleaded guilty to all ten offenses related to his attempt to detonate a car bomb in Times Square and he received a life sentence in prison.

Example 2: In a 2003 case, PNR data alerted DHS to an airport insider-threat scheme to smuggle drugs into the U.S.. The critical information in this case was not personally identifiable information nor did it implicate the specific travellers associated with the PNR, but illustrated that the travellers were unwitting victims of the scheme. DHS's detection of the scheme allowed it to identify the actual criminals.

Example 3: In December 2014, during a routine review of PNR data, DHS matched elements only available in the PNR to a second individual known to law enforcement as an alleged terrorist. Further research validated the connection between the two individuals. Based on all available information, DHS requested revocation of his non-immigrant visa (NIV) from the Department of State (DOS). DHS determined that the traveller would likely be found inadmissible to the US if permitted to travel, and the traveller was denied boarding by the airline. U.S.

Example 4: In December 2018, an individual travelled from the U.S. to an African country through the EU. The PNR record showed that he checked a weapon and ammunition in his bags. DHS determined that the individual attempted to export multiple firearms, ammunition, and accessories without an export license, and confiscated the items because the individual failed to obtain an export license. DHS seized the items.

Example 5: In January 2019, an EU citizen sought to travel from the U.S. to the EU with a weapon in his checked baggage. DHS learned that the individual had checked several rifles in his luggage but had not obtained an export license. DHS seized the items.

PNR also provides insight into the travel of the individual, including multiple legs of the journey, prior to and after arrival that is not available from other information. For example, in January 2015, DHS referred an individual for a secondary inspection, because information in his PNR matched the modus operandi of known terrorists. During the secondary inspection, a review of the traveller's electronic device revealed disturbing images related to terrorist

activities. The traveller could not explain why he had these images. Based on this secondary inspection, DHS referred him to another law enforcement agency for further investigation.

Q5: In order to assess the necessity and proportionality of the retention of PNR data, can you please illustrate by means of examples how PNR has been the key piece of intelligence in a law enforcement investigation?

Example 1: One large-scale and important example of the usefulness of retained PNR relates to the investigation of transnational criminal networks. In 2019, historical PNR data retained over many years provided investigators with leads that resulted in the identification of previously unknown co-conspirators who had committed home burglaries, theft, and fraud across the U.S.

Example 2: In August 2019, DHS identified a previously unknown associate of a known or suspected terrorist based on matches to PNRs belonging to the previously unknown associate. DHS's ability to validate the association between the two individuals proved critical to establishing reasonable suspicion. DHS referred the individual to law enforcement for further investigation.

Example 3: In January 2014, a U.S.. law enforcement agency asked for DHS's assistance in locating a criminal fugitive, wanted since 2004 and believed to have fled the country. Using historical PNR, DHS identified the probable residence of the subject in a foreign country. The U.S. law enforcement agency, with assistance from the foreign country, located the subject in the other country in June 2014, and successfully had the subject extradited back to the U.S..

Example 4: In 2004, U.S.. authorities detained a woman who had smuggled children into the U.S.. A transnational criminal organization recruited her to smuggle the children into the U.S. where the organization's operatives sold them. Through information gained during her interview about the organization's routine operations, DHS used historical and current PNR data to identify additional potential smugglers and victims previously unknown to U.S. law enforcement. The U.S. and a foreign government conducted joint law enforcement operations to shut down two transnational criminal organizations who used the same technique to smuggle children into the U.S.. The joint operations resulted in the arrest of dozens of criminals and the return of dozens of children to their parents in foreign countries. The modus

operandi discovered by this case supported law enforcement investigations and interdictions for many years, leading to additional arrests and rescued children.

Example 5: In 2012, the U.S. investigated an individual for child sex tourism. Similar allegations about the subject had been made since the 1970's, and he had been previously charged in the U.S., the UK, and Egypt. DHS provided certified copies of historical PNR data to the Assistant U.S. Attorney for use at trial. The historical PNR data showed the subject's travel, his use of aliases, and the identity of third parties who paid for his tickets. On February 28, 2013, a U.S. district court found the individual guilty of child sex tourism charges.

Example 6: In October 2013, DHS inspected a traveller's luggage after reviewing the person's PNR, which revealed a possible link to illicit activity. A single PNR data element linked the subject to a person who had previously been arrested with 5.82 pounds of crystal methamphetamine. DHS searched the subject's luggage and found amphetamine.

Example 7: In the 1990s, an individual joined al Qaeda and fought in Afghanistan. When he returned to the U.S., U.S. authorities arrested him for planning to set off bombs in the U.S. and Europe. DHS provided U.S. prosecutors with historical PNR data of his travel to various countries with a significant terrorist presence, data which DHS retained at a time when the individual was not under suspicion of any criminal activity. The retained PNR contributed to his conviction and 15-year prison term for conspiring to use weapons of mass destruction and providing support to terrorists.

Q6: Does the Agreement sufficiently define mechanisms to ensure transparency, access, correction and redress? How is the U.S. ensuring transparency so that all passengers are aware of the redress mechanisms in place?

Yes. Transparency is the first of eight principles and a core tenet of DHS's implementation of the Fair Information Practice Principles[28] The E-Government Act of 2002[29] requires DHS to

[28] See DHS Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, available at: https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles.

[29] Pub.L. 107-347, 44 USC. § 101.

"make the Federal Government more transparent and accountable," as well as "to provide enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy, national security, records retention, access for persons with disabilities, and other relevant laws." This law requires all federal agencies to conduct a privacy impact assessment (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII), or for a new aggregation of information that is collected, maintained, or disseminated using information technology. PIAs for the ATS, the system that maintains PNR, are posted to the DHS public website[30] Additional information specific to DHS's collection and use of PNR is also available on various DHS public websites (i.e., the DHS Privacy Office[31]) as well as on websites of U.S. Embassies located in the EU. The Department of Homeland Security Traveller Redress Inquiry Program (DHS TRIP) is a single point of contact for individuals, regardless of nationality, country of origin, or place of residence, who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs - like airports - or crossing U.S. borders.[32] DHS TRIP is a widely-used resource for EU travellers. Indeed, DHS TRIP receives on average 236 inquiries from EU travellers each month, approximately two of which mention PNR.

Q7: Have there been any cases in which the Department of Homeland Security pulled PNR data from the air carriers? If so, for what reasons?

All 63 air carriers covered by the U.S.-EU PNR Agreement push PNR to DHS on a regular schedule, beginning 96 hours prior to departure. If DHS requires the transmission of PNR outside of the covered carrier's normal push schedule, DHS will send the carrier a request for an additional push. Such requests are made on a case-by-case basis only after a supervisor has confirmed the need for the additional push. Should a carrier be unable to send a timely push, DHS may pull the data from the airline. This may occur to meet immediate operational needs,

30 See: https://www.dhs.gov/publication/automated-targeting-system-ats-update.

31 See: https://www.dhs.gov/investigations-reviews; https://www.cbp.gov/travel/clearing-cbp, https://www.cbp.gov/document/forms/procedures-access-correction-or-rectification-and-redress-passenger-name- records-pnr, https://www.cbp.gov/site-policy-notices/foia/records and https://www.cbp.gov/document/forms/passenger-name-record-pnr-privacy-policy

32 See: https://www.dhs.gov/dhs-trip.

such as when a flight is diverted due to weather or other emergency, the itinerary suddenly changes without an associated push of PNR or because of a specific, urgent, and serious threat.

Purpose and scope

Q1: The purpose of the agreement is defined as being "to ensure security and to protect the life and safety of the public". Does this cover all reasons for which PNR is currently required/used and processed?

Yes, DHS has only used PNR data to ensure security and to protect the life and safety of the public as stated in the Agreement.

Q2: Have all the reasons for which PNR can be used and processed under the terms of the Agreement been utilised since the agreement came into force?

Yes.

Q3: Does the agreement capture all of the data necessary to achieve its objectives?

Yes. The Agreement describes all of the data that may be transmitted to DHS and how DHS must handle the data. DHS finds that all of this data helps meet the objectives of security and protection of public safety. At present, DHS does not require or specify the PNR data elements that airlines must collect or require airlines to store PNR data. For this reason, it is important to note that all of the data elements covered by the Agreement may not be available for all travellers depending on what each airline has collected in the PNR to manage the individual's journey. As we learn more, we may discover that other data is useful for these purposes.

Q4: Are the PNR data types listed in the Annex to the agreement still correct and up to date?

Yes.

Q5: Are you aware of any type of PNR information that is no longer required for the same purposes and if so, which?

No, DHS continues to need all available elements to effectively and efficiently evaluate travellers.

Q6: In relation to any instrument/mechanism that existed before the current EU-U.S. PNR Agreement entered into force, are there any comparative data illustrating the effectiveness achieved after the adoption of the Agreement?

The U.S. concluded PNR Agreements with the EU in 2003, 2006, 2007 and 2011, which DHS has executed in good faith as evidenced during multiple Joint Reviews. Each of the earlier PNR agreements were terminated by the EU, not for a lack of effectiveness, but due to legal and/or procedural issues on the EU side. Further, the U.S. has collected PNR from carriers since 1992. Given the 20-year period between the U.S.'s initial collection of PNR and the entry into force of the current Agreement, comparative data would likely be of questionable value given changes in both the air transport (e.g., increased passenger volumes) and the security environment (i.e., the evolution of transnational crime and terrorism). Nonetheless, as noted earlier, the processing of PNR is critical to both security and facilitating passenger throughput at ports of entry. This can be demonstrated by a brief period after 2001 in which DHS had to identify and implement a process for the manual collection of PNR data to accommodate EU concerns. Over a period of one week at several airports around the nation, DHS attempted to collect this data from every passenger traveling on an EU-based airline. This manual collection required the secondary inspection of all passengers and the review of multiple documents in possession of every passenger. The collection of this data took anywhere from 5-20 minutes per passenger. This data collection effort resulted in some passengers waiting over three hours to be inspected, which the EU considered an extreme disruption of the passenger clearance process.

Safeguards

Q1: Are the data security safeguards in the Agreement sufficient to ensure the security and integrity of the PNR data stored?

Yes. DHS has a number of physical and procedural safeguards to protect personal privacy and the integrity of PNR data, including physical security, access controls, data separation and

encryption, audit capabilities, and accountability measures. Records in ATS are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies[33]. DHS imposes strict controls to minimize the risk of compromising the stored information.

Q2: Are there any additional data safeguarding and integrity measures or approaches in place?

Yes. All DHS users of PNR must undergo privacy training and obtain authorization from their supervisor and the ATS system owner before gaining role-based access to ATS. Data may only be accessed using the DHS network with encrypted passwords and user sign-on. 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 would 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 DHS. DHS limits access to ATS and PNR to those individuals with a need to know the information in order to carry out their official duties. Furthermore, DHS further controls access to PNR by providing each user only those accesses required to perform his or her job. Within the ATS database, DHS maintains audit trails of what information has been accessed by whom and uses the audit trials to support internal audits to ensure compliance with the stated purposes of the system. DHS requires all ATS users to undergo regular training, including annual privacy training, to maintain their system access.

Q3: Have there been any security breaches which could have been prevented had the Agreement required additional safeguards?

There have been no breaches; the safeguards work as designed.

Q4: How many privacy incidents taken place since this agreement entered into force? What were the causes?

---

[33] At a minimum, DHS Sensitive Systems Policy Directive 4300A, available at: https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf.

Since July 2015, the DHS Privacy Office has received only one report of a suspected incident involving PNR. This suspected incident did not involve EU-related PNR and, upon investigation, the Privacy Office determined it was not an actual incident. The reporting of the suspected incident, however, demonstrates DHS employees' awareness of the incident reporting requirements and allows the DHS Privacy Office to further fine-tune guidance and continue to raise awareness. DHS Instruction Guide 047-01-008, Privacy Incident Handling Guidance,[34] defines a privacy incident as the "loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence when (1) a person other than the authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an unauthorized purpose. Once discovered, DHS personnel should report privacy incidents that are either suspected and/or confirmed."

Q5: What effective measures have been implemented under the U.S. law for privacy incidents?

DHS has an obligation to safeguard personally identifiable information and implement procedures for handling both privacy and computer security incidents. This obligation is defined in numerous federal statutes, regulations, and directives, including:

Federal Statutes

- Title 5, U.S. Code (USC.), Section 552a, "Records Maintained on Individuals" [The Privacy Act of 1974, as amended]
- Title 6, USC., Section 142, "Privacy Officer"
- Title 44, USC., Chapter 35, Subchapter II, "Information Security" [The Federal Information Security Modernization Act of 2014, as amended (FISMA)]

OMB/Government-wide Regulations and Guidelines

- Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Resources (updated July 28, 2016)
- OMB Memorandum 16-24, Role and Designation of Senior Agency Officials for Privacy (September 15, 2016)

[34] Available at: https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017_0.pdf.

- OMB Memorandum 18-02, Fiscal Year 2016 - 2017 Guidance on Federal Information Security and Privacy Management Requirements (October 16, 2017)
- OMB Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)

DHS Policy

- DHS Delegation 13001, "Delegation to the Chief Privacy Officer"
- DHS Delegation 04000, "Delegation for Information Technology"
- DHS Directive 047-01, "Privacy Policy and Compliance"
- DHS Instruction 047-01-008:005, "Component Privacy Officer"
- DHS Instruction 047-01-006, "Privacy Incident Response and Breach Response Team"
- DHS Privacy Policy Directive 140-10, "Handbook for Safeguarding Sensitive Personally Identifiable Information"
- DHS 4300A, "Sensitive Systems Policy," DHS 4300A Sensitive Systems Policy Handbook, Attachment F, "Incident Response"
- DHS 4300 B, "National Security Systems (NSS) Policy"
- DHS Management Directive 026-04, Protection of Human Subjects
- DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information
- DHS Management Directive 11056.1, Sensitive Security Information.

Additionally, the DHS Chief Privacy Officer sits on the DHS TRIP Advisory Board. The DHS Privacy Office reviews all redress inquiries alleging non-compliance with DHS Privacy policy, including the mishandling of PII.

Q6: Please indicate the ways in which the Department of Homeland Security provides information to the travelling public regarding its use and processing of PNR.

DHS informs individuals that it receives PNR and how they can seek redress. It does so by publishing various compliance and information documents. Although DHS does not have the ability to notify individuals at the time of collection, DHS provides public notice through a

published System of Records Notice for the Automated Targeting System.[35] DHS works with carriers to incorporate notices into their documents and websites, which travellers may see at the time of booking. Additionally, DHS regularly updates and publishes the Automated Targeting System Privacy Impact Assessment (PIA), which outlines the privacy implications associated with the collection and use of PNR data, as well as the Department's strategies for mitigating those risks. The PIA outlines all of the possible venues available for individuals to seek redress, including through the DHS Traveller Redress Inquiry Program.[36] DHS has also developed and publicly posted a number of informational documents that describe the type of data transferred pursuant to PNR Agreements, as well as how it is maintained, used, and the conditions under which it may be disclosed. The informational documents include the actual PNR agreements, a DHS PNR Privacy Policy, and a list of Frequently Asked Questions/Answers.[37] DHS posts PIAs for the Automated Targeting System (ATS) (the system that maintains PNR) to the DHS public website.[38] Additional information specific to DHS's collection and use of PNR is also available on various DHS public websites (i.e., the DHS Privacy Office[39]) as well as through websites of U.S. Embassies located in the EU.

Q7: In relation to the question above, can the Department of Homeland Security also provide the ways in which they cooperate with the aviation industry in order to better inform the travelling public of the processing of their PNR data?

As discussed in the response to the previous question, DHS encourages carriers 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, some with links to the government sites provided.

All carriers provide public notice about the transfer of personal information to the U.S. Government in the Contract of Carriage, which as of June 18, 2019, reads as follows:

---

35 See: https://www.govinfo.gov/content/pkg/FR-2012-05-22/html/2012-12396.htm.
36 See: https://trip.dhs.gov/.
37 See: https://www.cbp.gov/document/forms/procedures-access-correction-or-rectification-and-redress-passenger-name-records-pnr, https://www.cbp.gov/site-policy-notices/foia/records, and https://www.cbp.gov/document/forms/passenger-name-record-pnr-privacy-policy.
38 See: https://www.dhs.gov/publication/automated-targeting-system-ats-update.
39 See: https://www.dhs.gov/investigations-reviews; https://www.cbp.gov/travel/clearing-cbp.

The passenger recognizes that personal data has been given to Carrier for the purposes of making a reservation for carriage, obtaining ancillary services, facilitating immigration and entry requirements, and making available such data to government agencies. For these purposes, the passenger authorizes Carrier to retain such data and to transmit it to its own offices, other Carriers, or the providers of such services, in whatever country they may be located.

A number of carriers also provide their passengers with information about the transfer of PNR to DHS and other governments on their websites. For example:

Air France:

As outlined by French and international laws and regulations, Air France, as well as any other airline, may be required to communicate personal data to authorized local authorities (customs, immigration, police, etc.) both in France and overseas. For example, this may be necessary in order to complete required immigration formalities and to prevent and combat terrorism and other serious crimes. In accordance with Article L.237-7 of French Internal Security Code, please be informed that airlines may be required to communicate personal data to authorized booking, check-in and boarding data collected from their passengers (API/PNR) to the French authorities for the purposes and under conditions as defined in the Decret N° 2014-1095 dated 26/09/2014. (https://www.airfrance.fr/FR/en/common/transverse/footer/edito_psc.htm)

American Airlines:

Please note that the laws and regulations of several countries, including without limitation, the requirements imposed under the Transportation Security Administration Secure Flight program, require us to provide foreign and domestic government agencies with access to the personal information you disclose to us and data that we have about you and your travel plans, history, or status, including both before and after a flight arrives. For example, American and other airlines comply with legal obligations in the U.S., United Kingdom (UK) and other countries to provide border control agencies and customs authorities with access to booking and travel data when you fly to and from such countries, including stopover or layover destinations or countries that you may overfly en route to your destination. American does not have control or knowledge of the storage and use of that data after it has been delivered to

the respective government entity. Further, to the extent required by law, we may disclose personal information to government authorities, or to third parties pursuant to a subpoena or other legal process, and we may also use or disclose your information as permitted by law to protect the rights or property of American, our customers, our services, or its users. (https://www.aa.com/i18n/customer-service/support/privacy-policy.jsp)

British Airways:

The laws of certain countries, such as the UK and USA, require airlines to provide certain passenger information to the border and immigration authorities. (https://www.britishairways.com/en-gb/information/legal/privacy-policy)

Lufthansa:

5. Disclosure of personal data to third party we may be required to forward your personal data to third parties within or outside the Lufthansa Group in order to be able to offer you our products and services on the basis of our contractual obligations or our legitimate interests. These recipients can be categorized as follows:

- Service providers
- Transportation and logistics
- Marketing
- IT
- Government bodies and authorities
- Members of the Lufthansa Technik Group

In the process, personal data may be transferred to third countries or international organizations. In order to protect you and your personal data, there are suitable safeguards in such cases as stipulated by and in compliance with statutory requirements (in particular the use of EU standard contractual clauses) or there is an adequacy decision adopted by the EU Commission (Article 45 of the GDPR).

You can find information on EU standard contractual clauses at [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF]. The EU Commission provides information on its adequacy decisions at

[https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en#dataprotectionincountriesoutsidetheeu].

We are also obligated by law to provide personal data to German and international authorities (Article 6 (1) point (c) of the GDPR in conjunction with local and international regulations and agreements. (https://www.lufthansa-technik.com/privacy-policy)

United Airlines:

Law enforcement/Legal processes/other uses. *United may also disclose your information: if required to do so by law, court order, subpoena or other legal process; as requested by a governmental or law enforcement authority; to protect the rights or property of United, its customers, its sites or site users; or when we believe in good faith that it is in the interests of aviation security or that disclosure is otherwise necessary or advisable. In certain ccircumstances, United's third party service providers may be required to disclose information to government or law enforcement authorities. Security, health and customs and immigration laws in the U.S. and many other countries require all airlines, including United, to provide border control agencies or other governmental authorities with passenger data. In order to comply with these laws we may disclose information about you and your travel arrangements to such authorities.*
(https://www.united.com/ual/en/us/fly/privacy.html#disclosing_information)

Q8: Have there been any instances of redress? How can an individual appeal to correct, rectify or delete information held about him/her?

The DHS Traveller Redress Inquiry Program (DHS TRIP) provides a single point of contact for individuals (regardless of nationality, country of origin, or place of residence) who have inquiries or seek resolution regarding difficulties they experience during their travel screening at transportation hubs - like airports - or crossing U.S. borders. Individuals file an inquiry providing additional personal information to process the inquiry. Based on DHS TRIP submissions from June 2015 to June 2019, EU inquiries averaged 13.8 percent of total inquires. Year-to-year monthly averages showed consistency of inquiries leading the DHS

Privacy Office to determine that EU travellers were aware of their redress options and took advantage of DHS TRIP to mitigate their travel related concerns. Of those EU inquiries, three included reference to the traveller's PNR. In 2016, an EU DHS TRIP inquiry went through the process and resulted in a letter to the traveller. There was no additional appeal from the traveller. In 2018, an EU DHS TRIP inquiry was received, but the traveller did not respond to a DHS request for additional information to process their request. There was no additional appeal from the traveller. In 2019, the DHS Privacy Office received an inquiry from an EU traveller, which was determined not to be a DHS TRIP inquiry but was handled as a Freedom of Information Act (FOIA) request. There was no additional appeal from the traveller. On average it takes DHS approximately 40 days to process a DHS TRIP request from a U.S. traveller and 42 days to process a DHS TRIP request from an EU traveller.

Q9: Do the mechanisms in place to inform passengers in relation to the processing of their PNR data afford passengers the possibility of knowing whether their data has been used by the Department of Homeland Security?

Yes. DHS processes all PNR data it receives from the airlines. Everyone can therefore confidently know that DHS has processed their PNR data.

Q10: Has there been any increase in the number of information requests from the public since the information regarding how PNR is processed and used has been published?

Yes, there has been an increase in the number of information requests from the public since the information regarding how PNR is processed and used was published.

Fiscal year 2019: 211 requests received through 8/7/2019
Fiscal year 2018: 233 requests received
Fiscal year 2017: 180 requests received

Q11: Article 11 ensures individuals rights of access and provides in paragraph 3 that all restrictions to such access shall be set forth in writing and provided to the individual on a timely basis. Can you please indicate the reasons for which the right of access of individuals to their own data can be restricted under the U.S. law? Have there been any examples in which the U.S. restricted the right to access to individuals? If so, for what reasons and when was the individual informed?

All individuals may request and obtain a copy of their own PNR data. If an individual fails to provide the necessary information for a request under the Freedom of Information Act, such as a date of birth or signing the penalty of perjury statement, then DHS will not provide a copy of the PNR data.

Q12: Have any challenges or concerns regarding the destruction, loss, disclosure, alteration, access, processing or use of PNR been raised? If so, please provide details.

No. DHS is not aware of any challenges or concerns regarding the destruction, loss, disclosure, alteration, access, processing, or use of PNR.

Q13: How many individuals sought administrative or judicial redress under the Agreement? What was the outcome of this procedure?

DHS is not aware of any EU individuals seeking judicial redress under the Agreement. Instances of administrative redress through DHS TRIP are provided in the response to Question 8 above.

Q14: Has the Department of Homeland Security accessed any sensitive data?

Yes, but only to confirm through testing that DHS systems work as intended by deleting sensitive data consistent with the terms of the Agreement. The tests that DHS conducted are discussed in the response to the next question.

Q15: How many times has the Department of Homeland Security not deleted sensitive data after the period of 30 days as stated in the Agreement? For what reasons? Please provide specific examples.

None. DHS deletes all sensitive data in accordance with the Agreement. DHS recently verified its compliance during two separate tests of sensitive word data in February 2018. The first test, conducted on non-EU PNR data, verified the notification, authorization, and approval process for accessing sensitive data contained in PNR less than 30 days old. The second test was conducted on a PNR that was over 30-days old. Although DHS received special permission to

conduct the second test in accordance with the DHS PNR Directive, DHS did not retrieve sensitive word information during the test as it had been permanently deleted from the PNR in question.

Q16: Are there necessary procedures in place for filtering out and masking out sensitive data from the PNR data received?

Yes. All PNR data received is screened for sensitive data, filtered and masked accordingly.

Q17: Is the U.S. applying the same data protection requirements to all PNR acquired regardless of whether they are sourced from inside or outside the EU?

Yes. The ATS PIA explains the data protections in place for all PNR regardless of whether the PNR is sourced inside or outside the EU.[40]

Q18: How many officials of the Department of Homeland Security are authorised to access depersonalised PNR data from the initial receipt to the end of the 10 year dormant period? In which ways the number of personnel having access reflects the current threat environment and the Department of Homeland Security's needs?

As of August 6, 2019:

- 16,233 officials are authorized to access PNR data
- 1,484, or .09% of DHS officials with access to PNR data are authorized to access depersonalized PNR data
- 1,138 or .07% of DHS officials have authority to grant access to dormant PNR data.

The statistics above reflect the global nature and 24/7/365 pace of DHS operations. On average, DHS processes the PNR of 358,448 air passengers per day at 153 airports in the U.S. and at 16 preclearance sites outside of the U.S. Most airports and the DHS NTC (DHS's PIU) maintain multiple shifts in order to maintain round-the-clock coverage. During each shift at each location DHS officers must access to PNR to fulfil their duties and responsibilities. Additionally, DHS requires multiple levels of supervisory approval before a DHS officer can

[40] See: https://www.dhs.gov/publication/automated-targeting-system-ats-update.

access some PNR data. The foregoing reasons account for the number of authorized officers with access to PNR.

Automated processing

Q1: What is the procedure to develop, test and validate the criteria used for the automated processing of PNR data?

The DHS Privacy Office participates on the Oversight Team in quarterly reviews of ATS targeting rules,[41] along with the Office for Civil Rights and Civil Liberties and the Office of the General Counsel to ensure that the targeting rules are relevant, reliable, up to date, tailored to minimize the impact upon bona fide travellers' civil rights, civil liberties, and privacy, and are in compliance with relevant legal authorities, regulations, and DHS policies. The Oversight Team also reviews these rules to ensure that they are based on up-to-date information regarding specific threats and that the rules are deactivated when no longer needed to address those threats.

Q2: How does the Department of Homeland Security ensure that such criteria are non-discriminatory and specific? Is the Privacy Office still involved in the development and quarterly review of the targeting rules? Is not, what are the changes introduced?

The DHS Privacy Office, the Office of Civil Rights and Civil Liberties, and the Office of General Counsel all review DHS targeting rules on a quarterly basis. The Oversight Team reviews all new rules and all modifications in light of current information identifying specific threats.

Q3: Are all databases against which PNR data are compared limited to those used in relation to countering terrorism and serious crime?

Yes. DHS compares PNR data against databases used in relation to countering terrorism and serious crime, databases used in relation to law enforcement and border security functions, as

41 See ATS PIA https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_ats006b_0.pdf for complete discussion of Rules development.

well as databases that apply to a combination of the previous uses. All databases against which PNR is compared are done so consistent with the purposes set forth in the 2011 Agreement.

The Privacy Impact Assessment for the Automated Targeting System lists the databases which it may compare data against, including: U.S. Customs and Border Protection's Automated Commercial Environment (ACE), Automated Commercial System (ACS), Overstay Leads from Arrival and Departure Information System (ADIS), Automated Export System (AES), Advance Passenger Information System (APIS), Border Crossing Information (BCI), Electronic System for Travel Authorization (ESTA), Electronic Visa Update System (EVUS), Global Enrollment System (GES), I-94 data, Non-Immigrant Information System (NIIS), Seized Asset and Case Tracking System (SEACATS), and TECS; the U.S. Citizenship and Immigration Services' (USCIS) Central Index System (CIS) data received through TECS, and special protected classes data; the U.S. Immigration and Customs Enforcement's (ICE) Student Exchange and Visitor Information System (SEVIS) and Enforcement Integrated Database (EID), which includes Criminal Arrest Records and Immigration Enforcement Records (CARIER); Secure Flight Passenger Data (SFPD) and Master Crew List/Master Non-Crew List data from Transportation Security Administration (TSA); the Department of Justice's (DOJ) National Crime Information Center (NCIC) and Federal Bureau of Investigation (FBI) Interstate Identification Index (III) hits for manifested travellers; Electronic Questionnaires for Investigations Processing (e-QIP); historical National Security Entry-Exit Registration System (NSEERS); Flight Schedules and Flight Status OAG data; Social Security Administration (SSA) Death Master File; TSDB (Terrorist Screening Database), which ATS ingests from the WLS (Watchlist Service); and Non-immigrant and Immigrant Visa data from Department of State (DOS) Consular Consolidated Database (CCD), Refused Visa data from CCD, and the Consular Electronic Application Center (CEAC), CBP's ADIS, Border Patrol Enforcement Tracking System (BPETS), Enterprise Geospatial Information Services (eGIS), e3 Biometrics System, and U.S. and Non-U.S. Passport Service through TECS; ICE's Enforcement Integrated Database (EID); DHS Automated Biometric Identification System (IDENT); USCIS's Person Centric Query System (PCQS); DOS CCD; commercial data aggregators; National Law Enforcement Telecommunications System (NLETS),; Interpol; and the private database of stolen vehicles maintained by the National Insurance Crime Bureau (NICB).

Q4: What are the procedures in place to ensure that the models and criteria used for the automated processing are reliable, relevant and up to date?

The information contained in the responses to Questions 1 and 2 above address how DHS develops and reviews targeting rules to ensure that the models and criteria used for the automated processing are reliable, relevant, and up to date.

Data retention

Q1: What was the contribution to activities of prevention, investigation or prosecution of terrorism or other serious crimes of PNR data retained for more than six months? Please provide examples.

As the case studies provided throughout this response show, DHS uses historical PNR data to discover previously unknown persons of interest with ties to known or suspected terrorists, criminal networks and other illegal activities, to investigate terrorist attacks and serious crime, and to ensure that targeting rules are based on relevant, accurate, and objective criteria.

Q2: Can you illustrate to what extent the retention of PNR data of passengers who have already left the U.S. has been essential in this context? Please provide examples.

Example 1: In February 2010, Najibullah Zazi pleaded guilty to conspiring to conduct suicide attacks against the New York City subway system. Zazi and two co-conspirators planned to travel from the U.S. to Afghanistan to join the Taliban and fight against the U.S. military and its allies. Another U.S. law enforcement agency requested immediate assistance from DHS in investigating Zazi due to his involvement in imminent attack planning. DHS's research indicated that Zazi travelled to Pakistan with two other individuals, who were previously unidentified co-conspirators at the time DHS conducted the research. If DHS had deleted Zazi's and the others' PNR after their departure from the US, DHS would not have been able to help the U.S. law enforcement agency to identify the co-conspirators and the full scope of the plot and network supporting it.

Example 2: In March 2010, David Coleman Headley pleaded guilty to helping plan the November 2008 terrorist attacks in Mumbai that killed 164. He also admitted to planning a

second attack in Denmark. U.S. prosecutors secured the conviction in part on DHS's ability to match investigative data from the FBI against historical PNR, despite the fact that Headley had previously departed from the U.S. when he was not under suspicion of criminal activity. DHS arrested Headley in 2009 when he again attempted to depart the U.S., an operation also facilitated by PNR data.

Example 3: In April 2017, a traveller arrived at a U.S. land port of entry. By reviewing the traveller's historical PNR data from 2012, DHS officers determined the individual had a connection to a recently identified known or suspected terrorist. The linkage between the two travelers was supported by information in the known or suspected terrorists 2015 PNR. During inspection, DHS discovered that the traveller's phone contained several images of persons holding what appeared to be an AK-47 assault rifle, and images of people bound and gagged who appeared to be dead. DHS officers also discovered several images of what appeared to be the traveller brandishing weapons while with a group of fighters. Further questioning confirmed the ties between the traveller and the known or suspected terrorist.

Example 4: In October 2017, a U.S. law enforcement agency learned information pertaining to an unknown subject who had created and published media promoting violent extremism. Because the agency did not know the subject's name, the agency asked DHS for assistance. By researching historical PNR, DHS matched the identifiers to an individual who had previously traveled to the U.S. and who had departed without raising any suspicion of criminal activity. DHS referred the individual to secondary inspection when he travelled to the U.S. in November of that year. During the secondary examination, the individual revealed that the identifier belonged to another associate. The use of the PNR led to the discovery of two previously unknown individuals being identified as needing additional investigation due to possible illicit activity. Based on all available information, DHS found the traveller inadmissible.

Example 5: In May 2014, DHS and a foreign law enforcement agency used historical PNR data to investigate two missing women feared to be victims of trafficking and forced prostitution. Based on a review of the victims' historical PNR, DHS and the foreign partner agency linked the two women to a suspected trafficker and to potential co-conspirators, and they also identified another possible victim. Based on this information, DHS was able to

identify the suspected trafficker when he attempted to travel again to the U.S. in August 2014, and DHS arrested him.

Example 6: In April 2008 an EU Member State informed DHS about an individual it had apprehended at its border for smuggling cocaine from New York's JFK Airport. DHS conducted research and, using historical PNR of the apprehended individual, uncovered the identity of a co-traveller that neither government had previously suspected. The co-traveller's current PNR disclosed that the co-traveller was scheduled to fly to the EU Member State the following week. DHS arrested the co-traveller at the U.S. border when it found him to be carrying cocaine.

Q3: Has the requirement to store PNR data in a dormant (non-active) database for ten years affected the processing of PNR data for the purposes outlined in the Agreement?

Yes, but DHS does not know the extent to which the requirement to place all PNR into a dormant status after five years, consistent with the Agreement, harms operations. The administrative burden of obtaining specific approval to access the PNR held in a dormant status may discourage individual officers from obtaining approval to use the dormant data and thereby complicates U.S. investigations.

Q4: In how many cases has the 10-year dormant period been proven to be necessary for the Department of Homeland Security for the fight against terrorism and serious crime? Can you please provide examples?

Between 2015 and 2019, dormant PNR contributed to the identification of 2,985 persons who should undergo further inspection because they matched a trend that is linked to possible illicit activity. In addition, the table below summarizes the number of requests made to access Dormant PNR data over a 12-month period.

Q5: Following the ten years of the dormant period, how does the Department of Homeland Security ensure full anonymization of the data? Can you please illustrate with examples the

added value, if any, of the anonymization of PNR data in comparison to deletion of the PNR data?

Under the U.S.-EU PNR Agreement, DHS plans to anonymize PNR data beginning in 2027. DHS plans to delete certain data elements to make it impossible to link PNR data to any individual, consistent with the terms of the Agreement. DHS expects that the anonymized data will still be useful in assessing and discovering criminal practices and trends that can inform future investigations and targeting rules.

Information sharing

Q1: In what instances has PNR data been shared with other Government authorities and in what proportion with each domestic authority has PNR data been shared? Are you able to break down such sharing in relation to the uses mentioned in Article 4, paragraphs 2, 3 and 4?

EU PNR records have been disclosed in 12,189 instances to domestic agencies.

- 11,979 or 98% of disclosures were made to other U.S. federal agencies
- 210 or 2% of disclosures were to U.S. state or local agencies

These statistics include information shared for the following purposes:
Terrorism - 9,243
Serious Transnational Crimes - 4,153
Health/Public Safety – 108

Between 2015 and 2019, DHS disclosed 4,006 records, ranging between zero and five years old.

Times EU PNRs Disclosed				**PNR Age at Disclosure, In Years**			
Disclosure Year	**0 – 1**	**1 – 2**	**2 – 3**	**3 – 4**	**4 – 5**	**Over 5**	**Grand Total**
2015	1,058	91	47	30	17	31	1,274
2016	803	38	19	19	11	33	923

2017	1,012	72	39	24	27	38	1,212
2018	699	65	57	37	37	49	944
2019	434	54	7	5	1	10	511
Grand Total	**4,006**	**320**	**169**	**115**	**93**	**161**	4,864

Q2: Can you describe what mechanisms of authorisation are in place to retrieve PNR data in circumstances other than the automated processing and the processing related to the typical border and security checks shortly before arrival and departure of passengers (e.g. historical searches upon request of other Government authorities)?

Requests for ad hoc access to PNR data by a non-DHS requestor, including a foreign authority, must be submitted in writing (transmitted by any appropriate medium) to DHS and describe the specific information requested, the reason(s) for the request (e.g., nature of the investigation or prosecution and the need for PNR), and how the information is to be used (e.g., disclosure in public court proceeding, held in confidence in connection with an investigation). All ad hoc requests from non-DHS requestors must be approved by the DHS Privacy Officer via email, or by an individual to which authority has been delegated. Only under exigent circumstances may PNR information be disclosed based on a verbal request. If such disclosure occurs, a written request must be submitted as soon as possible following the disclosure of the PNR information based on verbal representations. All sharing of PNR data must be appropriately logged and is subject to routine audits by the DHS Privacy Officer.

Q3: With which countries has PNR of EU Member State citizens or residents been shared?

We are unable to determine if a subject has EU residency based on PNR information. The initial data pull shows the disclosure of 70 PNR records of EU citizens to 19 countries, which are listed below, for authorized purposes:

Australia

Bahamas

Belize

Brazil

Bulgaria

Canada
Colombia
Denmark
Dominican Republic
Hungary
Ireland
Ivory Coast
Japan
Latvia
Mexico
Netherlands
South Africa
Spain
United Kingdom

Q4: How does the Department of Homeland security ensure that the provisions of Article 17 are complied with when it discloses PNR data to the authorities of third countries?

U.S. law requires that DHS may only share information with a foreign counterpart may only be provided if DHS obtains assurances that the information will be held in confidence and used for a law enforcement purpose consistent with the reason why it was provided.[42] Further U.S. law prohibits DHS from sharing further information with any foreign law enforcement agencies that does not adequately protect information. DHS implements both U.S. law and the PNR Agreement through a combination of formal agreements, arrangements, and securing case-specific assurances.

DHS's PNR Directive requires that a cover letter be included with the transfer of PNR data to a foreign authority that outlines the recipient's responsibility to protect the provided PNR consistent with the Agreement, which among other conditions, prohibits onward transfer of the information to any third party, such as a third country, without the express prior written authorization of DHS. This letter requires the receiving country to provide specific protections

42 19 USC §1628. https://www.law.cornell.edu/uscode/text/19/1628.

in addition to the general protections afforded under any applicable international agreement, such as the Mutual Legal Assistance Treaty or Customs Mutual Assistance Agreement in place between the U.S. and the receiving country. The use of this cover letter comports with international practice. Law enforcement agencies around the world use similar cover letters when sharing law enforcement sensitive information.

Q5: How is it being ensured that receiving authorities afford to PNR equivalent or comparable safeguards as set out in the agreement?

DHS ensures that receiving authorities afford to PNR equivalent or comparable safeguards as set out in the Agreement through the cover letter provided with the PNR data, as well as through the terms of a written agreement and any associated technical data security documents.

Q6: What procedures are in place to assess and validate or refuse the sharing of PNR data with such countries?

In addition to the requirements for access imposed on domestic Non-DHS Users, DHS requires that foreign governments to demonstrate that they can protect the data in a manner consistent with DHS standards and applicable U.S. laws, regulations, and international agreements and arrangements. DHS makes access to PNR data contingent upon an express understanding that the foreign government will treat the data as sensitive and confidential, will not provide the data to any other third party, to include another foreign government, without the prior written authorization of DHS, and will afford to the data equivalent or comparable safeguards as set out in the 2011 U.S.-EU Agreement.

As discussed in the response to Question 4 above, U.S. law prohibits DHS from sharing any information with foreign customs or law enforcement agencies that have violated any obligationsto hold the information in confidence and to use it only for the law enforcement purposes for which the information was provided. 19 USC. § 1628(b).

Q7: What are the mechanisms by which the Department of Homeland Security communicates with relevant EU Member States authorities, Europol or Eurojust?

DHS communicates with relevant EU Member States authorities and Europol through DHS liaison officers at Europol.

Q8: Please provide statistics and case examples on the exchange of PNR data with the EU Member States, Europol and Eurojust.

Example 1: DHS used PNR data to support the investigation into a known European terrorist attack. In support of this investigation, historical PNR data led to the timely identification of several previously unknown suspects. The close coordination between U.S. law enforcement agencies and the EU Member State enabled security services to prevent follow-on attacks by associated individuals, similar to the follow-on attacks in Brussels in 2016 following the November 2015 attack in Paris.

Example 2: In 2017, DHS supported an EU Member State's investigation of a terrorist attack in its territory. DHS analysis of U.S. historical PNR data dating back to 2014 identified one suspect with links to two other previously unknown individuals. DHS provided these leads to the EU Member State's law enforcement partners for use in the investigation into the attacks.

Example 3: In 2018, the DHS liaison at Europol received a request to support an EU Member State's investigation on subjects that were identified as being involved in an armed robbery. DHS uncovered additional information and leads contained only in historical PNR data that was used to support the investigation.

Example 4: In 2014, DHS supported an investigation by an EU Member State by providing historical PNR data that resulted in the arrest of six criminals from Asia operating a smuggling ring in the EU. A review of historical PNR pointed to a single employee of a major European airline. Further review identified ten fraudulent identities used by the smuggling ring in fifteen smuggling attempts, thirteen of which were successful. DHS developed and provided evidence to the EU Member State, which then used the evidence to arrest the individuals through a joint operation. The EU Member State also adjusted domestic security procedures to reduce its vulnerability to the crimes identified in this investigation.

Example 5: In 2016, DHS determined that an EU national scheduled to fly from the EU to the U.S. had information in his PNR that matched information tied to a known or suspected

terrorist. Because of the early receipt of PNR, DHS liaisons in the EU asked an EU Member State to interview the traveller prior to departure. This interview confirmed the individual's ties to the known or suspected terrorist and based on all available information, DHS recommended that the airline not board the traveller and, then referred the case to the EU Member State for further investigation.

Example 6: In 2010, an EU Member State contacted the FBI about one of its nationals who had recently travelled to the U.S., and who was believed to have been radicalized and "traveling to Pakistan to die." At the time, the EU Member State believed he had returned to Europe, but sent a follow up inquiry to DHS. DHS confirmed the individual was still in the U.S. and scheduled to depart the next day along with a co-traveller. DHS created a record to identify these individuals and shared information with U.S. and European law enforcement agencies.

ANNEX C
Composition of the evaluation teams

The members of the EU team were:

Laurent Muschel, Director, European Commission, DG Migration and Home Affairs – Head of the EU delegation

Monika Maglione, European Commission, DG Migration and Home Affairs,

Manuel Garcia Sanchez, European Commission, DG Justice and Consumers,

Igor Angelini, Europol expert

Ines Walburg, expert on data protection in the law enforcement area, the Hessian Commissioner for Data Protection and Freedom of Information, Germany

Daan Vertongen, expert on law enforcement, Deputy Director of the Passenger Information Unit Belgium

The members of the U.S. team were:

U.S. Department of Homeland Security

Michael Scardaville, Office of Strategy, Policy and Plans

Andrew Williams, Office of the General Counsel

Shannon Ballard, Office of the Chief Privacy Officer

U.S. Customs and Border Protection

Office of Field Operations

CBP Office of International Affairs

CBP Office of Information Technology

CBP Office of Chief Counsel

CBP Privacy and Diversity Office

U.S. Department of Justice

Thomas Burrows, Office of International Affairs

U.S. Department of State

Lee Skluzak, Office of European Union and Regional Affairs

Karen Zareski, Bureau of Counterterrorism
Sean Cooper, Bureau of Counterterrorism