046599/EU XXVII.GP
Eingelangt am 12/01/21

EUROPEAN
COMMISSION

Brussels, 12.1.2021
SWD(2021) 3 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 European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service

{COM(2021) 17 final}

www.parlament.gv.at

Contents

www.parlament.gv.at

1. INTRODUCTION AND BACKGROUND

The Agreement between the European Union (EU) and Australia on the processing and transfer of passenger name record (PNR)[1] data by air carriers to the Australian Customs and Border Protection (herein after "the Agreement") was concluded in order to enhance and encourage cooperation to effectively prevent and combat terrorism and serious transnational crime, while fully respecting fundamental rights and freedoms, in particular privacy and the protection of personal data. It entered into force on 1 June 2012 and allows for transfers of EU sourced PNR data to Australia, subject to the safeguards and controls included therein.

Australia requires each air carrier operating passenger flights to and from Australia to provide access to Passenger Name Record (PNR) data prior to the passenger arriving or leaving Australia. The legal basis for such data collection derives from the Australian Customs legislation, in particular section 64AF of the Customs Act 1901 of the Commonwealth ('Customs Act').

The Australian Border Force (ABF) is an operationally independent body within the Department of Home Affairs (herein after "the Department") of Australia, which main mission is to protect Australia's border and enable legitimate travel and trade, operates as a frontline border law enforcement agency and customs service. The Department is now the competent Australian Government agency for administering PNR data in accordance with the provisions of the Agreement. Once collected, the PNR data are processed, analysed and disseminated by dedicated divisions of the Department.

The two joint reviews of the Agreement - one in 2013[2] and one simultaneously[3] with the present joint evaluation - examined the practical application of the Agreement and proposed recommendations to further improve it.

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. The

---

1 Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, OJ L 186, 14.7.2012, p. 4.

2 Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, COM(2014)0458 final.

3 Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, COM(2020)701final.

www.parlament.gv.at

present document should be read in the light of these limitations, as well as in the light of the fact that all members of the EU team had to sign non-disclosure agreements exposing them to criminal and/or civil sanctions for breaches. The Department was be restrained in regard to what case studies and additional statistics could be provided for use in a public document, beyond what has already been provided as considered to reveal details on methods, capabilities and/or sensitive operations.provide details on methods, capabilities or sensitive operations.

These limitations have not come in the way of a thorough, open and frank exchange of views with the Australian authorities, who showed remarkable openness and a very constructive spirit. Therefore, the EU would like to confirm once again the excellent cooperation on the part of all the Department and other Australian personnel and express its gratitude for the way in which the questions of the EU team have been replied to. In January 2019, it was jointly agreed to launch the joint review and joint evaluation of the EU-Australia PNR Agreement exercise as foreseen in Article 24 thereof. This document includes the result of the joint evaluation process. Prior to its finalisation, it has been shared with the Australian authorities providing them with the opportunity to identify possible inaccuracies and to comment on its content.

2. METHODOLOGY

Although the Agreement at Article 23(4) does not state the scope and purpose of the evaluation, such exercise is meant to take a wider approach than the review of the EU-Australia PNR Agreement, analysing the operational added value of the Agreement and assessing its results and impacts, effectiveness and necessity, and proportionality. The evaluation also offers an opportunity to take stock of the evolution of the relevant legal framework and case law of both parties. The joint evaluation has taken place together with the regular joint review and has benefitted, from the same organisational measures and sources of information.

As was the case with the joint review, 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 and the Directorate General for Justice and Consumers, as well as data protection and law enforcement experts from EU Member States. Australia was represented by the Department of Home Affairs

www.parlament.gv.at

(herein referred to as "the Department"), with a team composed of officers from various units in charge of the PNR collection and analysis and led by the Assistant Secretary Border Intelligence Fusion Centre. A full list of the members of both teams appears in Annex B (composition of the teams).

The joint evaluation relied on the following elements:

- The questionnaire sent to the Department in advance of the joint evaluation and the replies to this questionnaire (Annex A).
- Visits to the Department premises in Canberra and the Border Intelligence Fusion Centre on 14 (dedicated day focused on the joint review) and 15 August 2019 (dedicated day focused on the joint evaluation);
- Exchanges with Department personnel responsible for the PNR programme, including analysts who use and have access to PNR data;
- The information provided during the visits to Australia and discussions with representatives from the Department, the Office of the Australian Information Commissioner, as well as the Office of the Commonwealth Ombudsman and the Department area responsible for privacy matters;
- Reports of formal audits conducted by the Office of the Australian Information Commissioner on PNR data processing by the Department;
- The joint review reports where relevant;
- Related legislation and case law; notably, the Opinion 1 /15 of the European Court of Justice on the envisaged EU–Canada PNR Agreement of 26 July 2017;[4]
- The evolution of the security environment in the EU, Australia and globally including the adoption of the United Nations Security Council Resolution 2396 (2017).[5]

The present document has received the unanimous agreement of the members of the EU team.It has also been shared with the Department, providing Australia with the opportunity to comment on inaccuracies and on information that could not be disclosed to public audiences. While the evaluation itself was conducted jointly, this document is not a joint report of the EU and Australian teams.

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

www.parlament.gv.at

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 use of PNR data is a key component of the Department's intelligence-informed targeting capability, used to identify serious threats to the Australian border in the air traveller domain. It allows the Department, including the Australian Border Force, to intervene while further checking a very small percentage of the travelling public and by targeting only the most serious threats to national security, and serious transnational crimes such as child exploitation, illicit drugs, organised crime, identity fraud and illicit tobacco smuggling in the air travel domain.

The use of PNR data is the primary mechanism that the Department and the Australian Border Force uses to reduce the volume of checks at the border, by providing the ability to target specific travellers through indicators and behaviours linked with identified risks. In identifying those travellers that present a credible and measurable risk beyond a predefined threshold, the use of PNR data allows the Department to facilitate those travellers that were not identified as high risk to transit the border without further intervention.

Results from PNR targeting rules in the period 2018-2019

In accordance to the information provided, between 2018 and 2019, 7.9 per cent of instances of closer questioning or examination of travellers identified from PNR-based targeting resulted in detention / arrest / seizure or further action outcomes;.

Of the total detention / arrest / seizure or further action outcomes:

***0.8 per cent** of travellers were detected with a significant quantity of **illicit drugs**,*
***0.6 per cent** of travellers were detected with **child exploitation material**,*
***32 per cent** of travellers were **refused entry to Australia**,*
***23 per cent** of travellers were detected with **undeclared revenue items (e.g. tobacco)** and finally,*
***43.6 per cent** of instances (of travellers whose entry to Australia was refused) resulted in **intelligence reports/files** being generated in relation to the threats covered by the Agreement (in addition to the above counts).*

www.parlament.gv.at

As regards the different ways in which PNR data are used, the Department staff conduct pre-arrival and pre-departure risk assessments of passengers travelling to (or in transit through) and from Australia using both EU and non EU-sourced PNR data, as well as other information, including Advance Passenger Information (API) data. In addition, the Department responds to requests for PNR data from other units within the Department and from other Australian government agencies or third country authorities as per relevant Memoranda of Understanding.

At each Australian international airport, officers are responsible for the facilitation of passenger processing and the application of risk management techniques to identify and intercept travellers who may pose a risk to the integrity of the border. In the framework of these operations, while the airport units may receive alerts about PNR data from the Department's competent authority, they do not themselves collect PNR data, nor are they involved in the disclosure of PNR data to other agencies or organisations.

The statistics on total air passenger movements show a total of 42,123 million passengers for the year which ended in June 2019[6]. In these circumstances it is necessary to conduct the risk assessment with the support of advanced technologies. According to the Australian authorities, **the value of PNR programmes consist therefore of the possibility, in combination with other sources of information, of screening effectively a large volume of passengers reducing interference with the normal flow of persons and goods at airports**. Additionally, the limited and carefully selected number of interventions on specific individuals, in combination with other sources of information maximises the use of available law enforcement resources. The procedures and controls applied before, during and after the creation of the models and criteria used in the pre-screening contribute to minimise the risk of bias and discrimination.

As to the techniques involved, the automated processing of PNR by the authorised staff of the Department implies different approaches in relation to whether it makes use of available intelligence on past suspicious behaviour, of known selectors and other available derogatory information, or of machine learning[7] techniques which do not rely on pre-existing information

---

6 Australian Department of Infrastructure, Transport, Cities and Regional Development. Data retrieved in September 2019 at https://www.bitre.gov.au/statistics/aviation/international.aspx.

7 Within the wider context of artificial intelligence, machine learning techniques refer to the use of algorithms and statistical models by computer systems so they can perform a specific task without using explicit instructions, but simply relying on patterns, associations and inference that the systems learn from large datasets.

or intelligence. These approaches are defined below respectively as threat profiling, predictive modelling and intelligence-led targeting, but such terminology should not be considered standard or commonly used.

3.2. Threat profiling

The specialised unit dealing with the automated processing of PNR data studies the information available on a specific group of persons known to be involved in a certain type of criminality. For instance known foreign terrorist fighters who have returned to Australia (or have not returned) may use specific air routes from certain conflict zones. Such knowledge based on past target behaviour is then used to build a profile, or set of criteria, which is then tested, validated and ultimately deployed in the pre-arrival screening in order to detect new, and previously unknown targets. The resulting matches are passed to the Australian Border Force, for additional human scrutiny, to determine any possible referral to airport operations.

The analysis of the past criminal behaviour (based on data retained under the conditions of the Agreement) requires in opinion of the Australian authorities, **the retrieval and use of historical PNR data** (past travel movements) for all the known individuals. Relying solely on a PNR where travel has not yet occurred does not allow identification of a change in pattern or behaviour in travel in the same way that is possible by combining previous and current PNR data.

Example: Comparative analysis between travellers suspected of illicit activity and other travellers.

Analysis of historic and current PNR data relating to travellers of known interest (data set A) compared to a larger group of travellers who are not of interest (data set B) was the only mechanism to verify the highest risk destinations, as well as other travel or booking behaviours. This process highlighted the general travel behaviour of high threat travellers as opposed to the travel behaviour of legitimate travellers, and therefore informed relevant targeting efforts. Abstract profiles were developed to ***identify travellers to be suspected of being in possession of child exploitation material or travelling to conduct child exploitation offences overseas.***

With minimal intervention, this effort led to: ***10 detections*** *of child abuse material, 5 detections of borderline child abuse material, and* ***12 instances*** *of high-value intelligence collection for further investigation into possible live streaming of child abuse in just three*

months. The development of this effort relied on historical PNR and has enabled the detection of this crime against otherwise unknown entities of interest.

Furthermore, the Australian authorities noted that during the assessment of a profile match, the ability to compare a current travel event to past behaviour and other available intelligence is equally essential in determining what is of interest. Neither can be achieved without access to historic PNR data in view of the Australian authorities.

3.3. Predictive modelling

Predictive modelling is a technique developed by data scientists which makes use of machine learning classification algorithms. The aim of this technique is to identify "unknown" individuals that may be of interest for law enforcement or border management authorities based on their similarity to historical "known" individuals of interest. It foresees three distinct phases: i) learning phase ii) testing phase and iii) deployment.

In the **learning phase,** the data scientist builds a predictive model using a historical set of passenger data where the subset of records related to individuals known for their involvement in a given type of criminality is clearly marked. The machine learning algorithm learns the characteristics or features that differentiate the prior "known" passengers of interest from other passengers.

In the **second testing phase,** the machine learning model is run on a different historical dataset, where the markings for the known criminals are not present in the PNR records. The system applies the model built during the first phase and identifies individuals suspected of criminality. The tester who created this second dataset is in fact in possession of the markings which identify the records of the passengers known to be involved in the targeted criminal behaviour and is therefore able to measure in how many cases the system identified the right targets. In essence, the test data is used to see how well the machine can predict new targets on a dataset that it has not previously seen.

The **last phase** is when the model is actually deployed in production in the course of the pre-arrival or pre-departure screening. Each traveller is scored against the model which allows a threshold to be set. A traveller that scores above the agreed threshold generates a match that is always further assessed and possibly referred for subsequent intervention.

Example: Predictive modelling

A model was built to identify travellers that may be importing illicit drugs to Australia. The model relied on all prior significant drug detections in the traveller stream where historical PNR was available. Once deployed, travellers that score above a set threshold on the model (approximately 0.05% of inbound passengers each day) generate a match prior to arrival for further assessment, and then possible intervention.

During the EU team's visit to Australia in August 2019, the Australian authorities informed that up to that date, nine drug couriers have matched the output of the model. In several cases, the couriers also matched other profiles or were identified through by other targeting means. However, three couriers were only identified due to the match on the model, resulting in the detection of a total of 4.5kg of methamphetamine and 6.5kg of ephedrine.

Comparisons between the performance of the model and similar coverage rules-based profiles indicate the model is more efficient, resulting in a similar number of detections, but from less than half the number of matches.

The Australian authorities reaffirmed that in order to build reliable and accurate predictive models, the training and testing datasets need to be generated making use of historical PNR data.

3.4. Other targeting possibilities

The EU experts, during their onsite visit to Canberra, were briefed in a secure room on operations and analyses of PNR data to identify individuals already known for their involvement in criminality or that can be connected to data elements which in the past were already associated to criminal behaviour. The experts had no access to the systems or any data processed.

While the identification of individuals would normally rely on the use of complete and verified biographic information, which is not present in PNR data, the Australian authorities noted that the use of other data such as a telephone number or an email address included in PNR records, can lead to the detection of suspects, either previously known or unknown.

PNR allows risk assessment in identifying unknown criminals (linked bookings)

A passenger travelling from the Middle East was subject to a routine inspection which revealed 7kg of heroin hidden in his hand baggage. The PNR included a telephone number. A few days later the same phone number appeared in the PNR of another national flying the same route. After a mandated check the individual was found in possession of 5kg of heroin.

www.parlament.gv.at

PNR analysis identified passengers suspect for drug smuggling. Further analysis and comparison with historical PNR data revealed that their booking was made by the same travel agent. Enquiries then showed that this travel agency was used by a drug network, which without the PNR data would not have been dismantled.

The PNR data have also been used to detect, investigate and prosecute people who have attempted to get to or have been to conflict zones. For example, since 2012, information made publicly available by the Australian Security Intelligence Organisation says that around 110 Australians had been known to be fighting or engaged with terrorist groups in Iraq and Syria.[8]

Example: PNR used to prevent a terrorist attack (real time)

In 2017, the Australian competent authority received information about a passenger who was travelling to Australia (Sydney) in order to carry out a terrorist attack using explosives. Historical PNR data was proven to be key during the investigation in order to identify the passenger, who was apprehended before carrying out the attack.

Such a case proved, in view of the Australian authorities, that PNR data are especially useful for running them against predetermined criteria (abstract profiles) in order to identify previously "unknown" suspects, and then, in a second step, for running their data against various databases of persons and objects sought, i.e. to identify persons that might potentially be of interest to law enforcement authorities and who were so far unsuspected.

Another important feature of PNR is that it allows the identification of criminal associates as individuals may appear together in the same travel reservation (co-travellers).

Example: PNR data use in investigations, prosecutions, unravelling of networks after a crime has been committed

PNR data was used to analyse a detection of border-controlled drugs , imported by an outlawed motorcycle gang and Asian organised crime syndicate, to assist with the identification of persons of interest and additional travel associates, following detection of the border control drugs in a sea cargo container.

[8] See: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22committees/estimate/fdff59a2-9694-43a8-bb17-3c452655dca6/0005%22

Investigators submitted requests for information to receive PNR information on a person of interest suspected to be involved in the importation. PNR data led to the identification of numerous travel associates who had previously travelled with the main person of interest, over a number of years.

These associates had not come to the notice of law enforcement agencies before this link was found in PNR. Historical PNR linked them to the main person of interest and subsequently enabled the deployment of operational resources to identify other illicit importation attempts by the syndicate. This case subsequently led to the arrest of 27 persons of interest across multiple states in Australia, all of whom were charged in relation to the attempted importation of border-controlled drugs.

In view of the Australian authorities, without the use of current and historic PNR data in the initial stages of the investigation, investigation strategies would not have been able to effectively capture all of the individuals involved in the main importation. Additionally, forensic evidence obtained during the course of the investigation would not have been obtained otherwise. Without identification of the linkages from PNR data, forensic evidence directly connecting travel companions to the importation would have been destroyed.

3.5. PNR as a facilitation tool

In identifying travellers that present a high and credible risk, the use of PNR data by Australian authorities facilitates travellers that are not identified as high risk, to transit the border without intervention. The limited interference to the transit is therefore impacting a very small percentage of the travelling public while allowing targeting only the most serious crimes such as child exploitation, illicit drugs, organised crime and identity fraud in the air traveller domain which match serious transnational crime and terrorist offence requirements.

Example: The number of potential hits generated remains very low

As an example of how the various types of processing of passenger data are effective, the use of PNR data to target travel behaviour consistent with international drug couriers, during a one year period, ***reduced the number of potential travellers targeted*** *(through manual physical intervention at the point of entry)* ***by 98.76 per cent*** *of the total that could be considered. Subsequent intelligence assessment, further increased this total to 99.88 per cent, meaning that* ***only 0.12 per cent of relevant air travellers were targeted for border***

www.parlament.gv.at

intervention *through this method and therefore, 99.88 per cent of travellers that would have been checked without the use of PNR data have not been considered for intervention.*

The Australian authorities are of the view that PNR data is critical in the identification and analysis of suspected drug couriers and, through the use and deployment of profiles and analytical models, the Department is able to focus its efforts on travellers who present the highest threat. For example, PNR data provides a more accurate picture of a traveller's itinerary, whereas the Advance Passenger Processing (APP) system – used to process Advance Passenger Information (API) - may only provide the last port of origin. If relying on the APP system for profiling and analytic models, a larger number of travellers would be of interest to the Department in the initial stages of assessment and therefore intervened with at the border. Through the use of PNR data elements, the Department is able filter out a larger number of legitimate travellers and focus analytical and operational effort on the highest risk travellers identified.

4. CONSISTENCY WITH OTHER INSTRUMENTS

4.1. Other instruments for the collection of travel related data

PNR data remains a critical data element for Australia in the identification of serious transnational crime and terrorism. Without it, it is certain that an increase of illicit or nefarious goods, or individuals that seek to cause harm to Australia and the global community through criminal and terrorist acts, will enter or leave Australia 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 is not 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.

This is also evident when comparing PNR to other systems created to collect travel related data. For instance, Advance Passenger Information (API) mostly include biographic information which is rather 'static' (it does not change substantially over time) and does not express a behaviour of the passenger (differently from PNR where one can detect choices made by the passenger, such as travelling only with hand baggage, paying in cash, make the

reservation in the last 24 hours from departure etc). Similarly, also the systems created to grant authorisation to travel mainly refer to biographic information and occasionally 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 provide an advantage to law enforcement authorities in allowing more time for its processing, analysis and any follow-up action.

4.2. Other instruments on PNR

Since the entry into force of the Agreement, new trends and new security threats have emerged. There is 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'[9]. 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).[10]

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

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

(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. Australia 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 Decision (EU) 2019/2107 of 28 November 2019[11] 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 Australia, 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.

---

[11] 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.

www.parlament.gv.at

The EU PNR Directive[12]

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. Identifying and tracing suspicious travel 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 24(6) of the EU-PNR Australia Agreement envisages the Parties' consultation if and when an EU PNR system is adopted to determine whether this Agreement would need to be adjusted accordingly to ensure full reciprocity. During the joint evaluation the EU team had the possibility to illustrate to the Department the key features of the EU PNR architecture. The Department recalled the good, although occasional, cooperation with EU authorities. Both parties agreed that the new EU PNR framework adds clarity to the relations between Australia and the EU as it now identifies specific counterparts in each Member States, i.e. the Passenger Information Unit (PIU) as the dedicated entity entitled to collect and process PNR data. In addition, the EU PNR Directive also foresees that each Member State designates its authorities entitled to request or receive PNR form the PIU. Such list is published and regularly updated by the European Commission. The Department is therefore able to verify whether requests submitted under Article 6 (2) of the Agreement come from authorities competent to process PNR. In this respect, the new EU framework on PNR complements and aligns with the Agreement. Nevertheless, the EU team as stated in the conclusions of the Joint

[12] 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.

review report,[13] notes that the procedures concerning law enforcement cooperation with the EU Member States and the EU agencies (Europol and Eurojust) shall be further improved to ensure the provision of relevant and appropriate analytical information.

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

In the course of the joint evaluation, the teams discussed the most important legal development since the entry into force of the Agreement, including the Court's Opinion 1/15 on the envisaged PNR Agreement with Canada as well as other recent developments concerning the negotiations with Canada and the EU PNR Directive. 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' departures 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.

[13] Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, COM(2020)701final.

www.parlament.gv.at

- The processing of sensitive data shall be prohibited.
- 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.

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

In the discussions on the Court's Opinion, the joint evaluation teams assessed the relevant safeguards that the Agreement already contains for the use of PNR, in particular:

- A strict purpose limitation, the use of PNR data being limited to the prevention, detection, investigation and prosecution of terrorist offences or serious transnational crime;
- The obligation for Australia to provide to competent authorities of the EU Member States or Europol or Eurojust analytical information obtained from PNR data;
- Safeguards applicable to the use of PNR, including, strong data security and integrity requirements;
- Rights of access, rectification and erasure and the possibility for EU citizens to obtain administrative and judicial redress under the terms of the Agreement;
- Independent oversight by the Office of the Australian Information Commissioner who has effective powers to investigate compliance with effective powers of investigation and enforcement;
- A PNR data retention limit of five years and a half; after the first three and a half years all elements of PNR data which could lead to the identification of passengers are already deleted.

In addition, the Australian authorities explained that:

- procedures to use PNR data in targeting activities (profiling) are part of the Department's governance processes. Each activity request is assessed individually, and where the attributes provided are considered to be too broad, or discriminatory as to capture an entire group of like travellers, the request is rejected and additional criteria are required. This ensures that travellers are not profiled purely based on race, ethnicity, stereotype or other sensitive attributes. Requests of this nature are rejected totally.
- There is no automated processing of 'sensitive data' and these attributes are removed from Automated Processing systems.
- PNR data is not compared to other databases and is stored in a separate database within the PNR System, which is partitioned from other Departmental sources.
- All processing of PNR data is performed for the purposes outlined within the Agreement.
- As regards onwards transfers to third countries, a formal Memorandum of Understanding must be in place between the Department and the third country/international agency in which consideration of the third country policies is included.
- All requests for PNR data from other Government authorities are logged and auditable, with assurance activities undertaken on a regular basis by internal Departmental work areas.
- As regards the retention of data, Australian authorities provided information that in their view constitutes an additional justification of the necessity to keep historical PNR data of passengers that have left their country to create and preserve the knowledge of the criminal phenomena with the dual objective of (i) learning the travel pattern of past criminals in order to detect new criminals and (ii) identify anomalies in current travel patterns when compared to previous typical and expected behaviour of regular passengers and (iii) retrieve flight details for criminal investigations.
- It is also worth noting that the Department confirmed that it applies the rules and safeguards laid down in the Agreement to all PNR data provided by airlines that operate air transportation to, from and through Australia and that process PNR data in the territory of an EU Member State (i.e. not only from EU sourced PNR data).

Despite meeting a number of the Court's requirements, 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 Australia Agreement was concluded before the Court delivered its Opinion. These concern the respect of information to passengers, retention of PNR data, onward transfers and the need for a prior independent review of the use of PNR data.

6. 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. Clear examples have shown that PNR, including historical PNR, has been critical to detect foreign terrorist fighters and to combat in particular drug crimes and child exploitation.

Its **value** lies first of all with the possibility of screening effectively a large volume of passengers while at the same time avoiding disruption or simple interference with the normal flow of passengers at airports. For such screening to be **timely**, in relation to the very limited timeframe available to the Australian authorities between the collection of the data and the arrival of the passengers, and **effective**, i.e. resulting in a very limited number of relevant passengers to be subject to further examination. Such a combination, also keeps to the minimum, the amount of data accessed by Australian officers. A number of **safeguards** operating before, during and after the screening process, including internal and external **oversight**, contribute to the aim that it remains objective and free from any form of discrimination.

The effectiveness and timeliness of the PNR screening also allows the vast majority of passengers to enjoy a **seamless travel experience** by transiting the Australian border faster and without interference.

In order for the PNR programme to preserve its value there is a constant need for the Australian authorities to build their knowledge of the criminal phenomena they aim to prevent and constantly refine and adapt such knowledge to new trends, threats and modi operandi deployed by criminals and terrorists to avoid detection.

www.parlament.gv.at

In this regard, the Australian authorities consider that there is sufficient proof of the **necessity** of historical PNR data to create and preserve the knowledge of the criminal phenomena with the dual objective of (i) learning the travel pattern of past criminals in order to detect new criminals and (ii) identify anomalies in current travel patterns when compared to previous typical and expected behaviour of regular passengers.

Another important feature of the Australian PNR programme (and of similar programmes adopted elsewhere) is the **uniqueness** of the specific data collected. No other travel related data provide this kind of information, which can be used to identify and target specific behaviours. Elements such as complete air route, means of payment used, and time of booking or baggage information remain crucial in the overall risk assessment and cannot be found in any other dataset used by the Australian competent authorities.

Besides having demonstrated its operational value and effectiveness, the Agreement's 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 recognised the efforts made by Australia to comply with the requirements of the Agreement as proven by the joint review[14]. 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 Australian Agreement was concluded before the Court delivered its Opinion. These concern the notification to passengers, the retention of PNR data, onward transfers and the need for a prior independent review of the use of PNR data.

[14] Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, COM(2020)701final.

www.parlament.gv.at

ANNEX A

Questionnaire[15] for the Australian Authority responsible for the processing of PNR data 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 use of PNR data is a key component of the Department of Home Affairs' (the Department) intelligence-informed targeting capability, used to identify serious threats to the Australian border in the air traveller domain. It allows the Department, including the Australian Border Force, to intervene with a very small percentage of the travelling public while targeting only the most serious national security, child exploitation, illicit drug, organised crime, identity fraud and illicit tobacco threats in the air traveller domain—that fit the serious transnational crime and terrorist offence requirements.

The use of PNR data to target travel behaviour consistent with international drug couriers, during a one year period, reduced the number of potential travellers targeted (through manual physical intervention at the point of entry) by 98.76 percent. Subsequent intelligence assessment further reduced this total by 99.88 percent, so that only 0.12 percent of relevant air travellers were targeted for border intervention – removing 99.88 percent of travellers that may have been considered for intervention.

The use of PNR data is the only mechanism that the Department and the Australian Border Force has to reduce the size of this cohort, by providing the ability to target specific indicators and behaviours that present likely risks.

In identifying those travellers that present a high and credible risk, the use of PNR data allows the Department and Australian Border Force to facilitate those travellers that were not identified as high risk to transit the border without intervention.

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

[15] The European Commission sent a questionnaire to Australia on. 28 June 2019. Australia provided written replies to the questionnaire on 19 September 2019.

www.parlament.gv.at

Between 2018 and 2019, 7.9 percent of instances of closer questioning or examination of travellers identified from PNR-based targeting resulted in detention / arrest / seizure or further action outcomes. (intelligence reports/files are excluded).

Category	***Outcome measure***
Detention and/or arrest	significant drug detection; detection of child exploitation material
Seizure	significant drug detection; detection of child exploitation material; seizure of undeclared revenue items
Further action	Traveller refused entry to Australia, generation of an intelligence report/file

Of the total detention / arrest / seizure or further action outcomes:

- 0.8 percent of travellers were detected with a significant quantity of illicit drugs
- 0.6 percent of travellers were detected with child exploitation material
- 32 percent of travellers were refused entry to Australia
- 23 percent of travellers were detected with undeclared revenue items (e.g. tobacco)[16]
- 43.6 percent of instances resulted in intelligence reports being generated (in addition to the above counts)

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-Australia agreement still relevant for the fight against terrorism and serious transnational crime?

The Department is charged with border-related functions to keep Australia safe and maintain our sovereignty. The PNR Agreement facilitates the transfer of PNR data, which is critical to the Department's ability to discharge these responsibilities, including the fight against terrorism and serious transnational crime. The Agreement remains necessary and relevant to

[16] From 1 July 2019, the Australian Government introduced a set of measures to combat the illicit tobacco trade. Part of these measures introduced changes to the Customs Act 1901, which makes the import of most tobacco products a prohibited import into Australia, without a permit.

www.parlament.gv.at

ensure the provision of PNR data to the Department, and to ensure that Australia continues to receive, store, access and use the data appropriately.

Section 64AF of the Customs Act is the Australian legislative basis for airlines to send PNR data to the Department, and the Agreement for PNR data addresses and resolves the conflict for airlines between European with Australian data protection laws. The proposed Agreement resolves this conflict by providing an appropriate legal framework and assurances that EU-sourced PNR data transferred to Australia will be processed in accordance with existing Australian data protection laws, striking an appropriate balance between national security and privacy protection considerations.

PNR data remains a critical data element for Australia in the identification of serious transitional crime and terrorism. Without it, it is certain that an increase of illicit or nefarious goods, or individuals that seek to cause harm to Australia and the global community through criminal and terrorist acts, will enter or leave Australia undetected—when they could have been otherwise prevented through the use of PNR data.

In addition, Qantas (Australia's largest national airline by number of international flights and passengers carried) uses a service provider with data warehouses within the EU. Qantas makes up approximately 15% of all seats to and from Australia. A further 25% of seats to and from Australia are operated by air carriers that also use service providers within the EU. This means approximately 40% of seats to and from Australia are operated by air service carriers that have their PNR data stored in the EU. This makes the PNR Agreement necessary to enable the Department to effectively identify the serious threats to the Australian border, in the air traveller domain.

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

There is information contained within PNR data that is not able to 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.

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?

These will be demonstrated through the relevant presentations during the Joint Evaluation, by the Department, the Australian Border Force and a partner security agency.

A written summary for disclosure, of these case studies, can be discussed during the sessions.

Q6: Does the Agreement sufficiently define mechanisms to ensure transparency, access and redress?

Yes, the Agreement provides sufficient information for the Department to ensure the Articles that address transparency, access and redress are fulfilled. The mechanisms remain aligned to the requirements that the Department is obligated to fulfil by law, under the *Privacy Act* and the *Freedom of Information Act*.

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?

The Department is responsible for centrally coordinated strategy and policy leadership in relation to domestic and national security arrangements, law enforcement, emergency management, counter-terrorism, social cohesion, the protection of our sovereignty and the integrity of our border, and the resilience of our national infrastructure.

The Australian Border Force, an operationally independent body within the Department of Home Affairs, is Australia's frontline border law enforcement agency and Australia's customs service. The Australian Border Force delivers critical border protection and national security outcomes while facilitating the movement of people and goods across the border. The Australian Border Force's mission is to protect Australia's border and enable legitimate travel and trade.

To enact these responsibilities, the purpose of the agreement adequately describes the purposes for which PNR data is used by the Department.

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?

PNR data is utilised for the Department in line with our responsibilities as outlined in Q1. PNR data is utilised daily to *"ensure security and to protect the life and safety of the public".*

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

Yes. The PNR data elements have not changed since prior to 2010.

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

Yes, the PNR data elements are still correct and up to date. The Department's PNR program aligns the data elements it collects with International Civil Aviation Organization (ICAO) DOC 9944 (Guidelines on Passenger Name Record (PNR) Data). These 19 data elements are included in the ICAO DOC 9944.

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

No.

Q6: Can you briefly explain what mechanism existed, before the EU-Australia PNR Agreements entered into force, which allowed for the collection of PNR? Are there any comparative data illustrating the effectiveness achieved after the adoption of the Agreement?

Section 64AF of the *Customs Act 1901* ("Obligation to provide access to passenger information") provides for the provision of PNR data to the Department in a particular manner and form.

Prior to the current 'PNR Push' method to receive data, airline operators would provide access via the 'PNR Pull' method, which is where access was provided into each airlines operating system. Authorised officers would have direct access into the operator's system and pull out the required data.

Prior to the PNR Agreement entering into force, PNR data was processed in line with the applicable legislative framework, including section 64AF of the *Customs Act 1901*, section 16 of the *Customs Administration Act 1985, the Privacy Act 1988 and the Freedom of Information Act 1982.* These Acts remain in force, except for the *Australian Border Force Act 2015*, which repealed the Customs Administration Act.

Safeguards

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

Yes.

The Australian Signals Directorate's Information Security Manual (ISM) provides the whole-of-Australian Government benchmark for security of equipment and data, and the Attorney-General's Department's Protective Security Policy Framework (PSPF) provides relevant policy. PNR data security as implemented in the Department's Data Warehouse complies

www.parlament.gv.at

with the ISM and PSPF. Many of the safeguards within the PNR agreement align with ISM controls and PSPF policies.

The Department also maintains an Integrity Framework for all staff. The Integrity Framework is an integrity model designed to protect the Department's people, property, systems and information from infiltration and corruption. The Integrity Framework is a component of the Professional Standards Framework.

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

The Department encrypts data at rest via Full Disk Encryption.

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

There have been no security breaches in relation to PNR data.

Q4: How many privacy incidents taken place since this agreement entered into force? What effective administrative, civil and criminal enforcement measures are been implemented under Australian law for privacy incidents?

There have been no privacy incidents since the Agreement came into force.

There have been several reforms of the Australian privacy laws since the Agreement came into force. Further detail will be provided as part of the 'General discussion of Australian privacy law' session presented by the Office of the Australian Information Commissioner (OAIC) on day 1 of the Joint Review.

Q5: 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 Australian competent authority?

Yes, the Department of Home Affairs via the Australian Border Force website provides information of the purposes for which the Department collects and uses personal data, including PNR data. The statement also outlines the purpose, authority, use and disclosure provisions relating to PNR data. The advice is publicly available at:

https://www.abf.gov.au/entering-and-leaving-australia/crossing-the-border/passenger-movement/collection-of-passenger-name-records

More generally, the *Privacy Act 1988* requires the Department to notify an individual of certain matters when it collects personal information about them. This is delivered through a

Privacy Notice. The Privacy Notice form (Form 1422i) is the notification method for these matters, and is available on the Department's internet site.

The audit reports from the Office of the Australian Information Commissioners (OAIC) audits are also publicly available on the OAIC's website.

Q6: 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?

No. Since 2014, the Department has averaged three (3) requests per year for PNR data through the Freedom of Information (FOI) request process.

Q7: Article 12 ensures individuals rights of access and provides in paragraph 3 that all restrictions to such access shall be set out in writing within 30 days. Can you please indicate the reasons for which the right of access of individuals to their own data can be restricted under Australian law?

The *Freedom of Information Act 1982* provides that the Department must provide an FOI applicant with a decision on access to the documents requested within 30 days of receipt of their request. There are a number of provisions to extend that timeframe under the Act, including extensions of time agreed by the FOI applicant or the OAIC, and formal consultation processes with affected third parties.

In regard to the reasons for which the right of access to an individual's own data is covered under Article 12 (2), certain information is exempt from disclosure under the FOI Act. Information may be exempt from disclosure under the FOI Act in accordance with the exemption provisions of Part IV of the FOI Act. These exemptions may include, but are not limited to, "the prevention, detection, investigation, or prosecution of criminal offences, to protect public or national security".

Q8: Has the requirement to store PNR data separately from any other data and to allow only data flow to the PNR system, but not from the PNR system to other databases, created problems for the processing of PNR data for the purposes outlined in the Agreement?

It has not created any issues with the separate storage of PNR data in the data warehouse. For new capabilities it has created some latency issues with constantly requesting data from the database. However, these issues affect other systems, and not with the processing of PNR data for the purposes outlined in the Agreement.

Q9: Have any challenges or concerns regarding the destruction, loss, disclosure, alteration,

access, processing or use of PNR been received? If so, please provide details.

It has been recently identified that some PNR data held prior to the Agreement coming into force (2012) has not been subject to the deletion / depersonalisation process. At the time of introducing the Airline Arrangement data, the receipt date does not align with the actual dates when the Department received the data. This matter is currently being addressed at a data warehouse level.

Q10: How many individuals sought administrative or judicial redress under the Agreement? What was the outcome of this procedure?

Nil.

Automated processing

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

The Data Warehouse section uses approved change control and testing processes that facilitate the development, testing and validation of criteria used for the testing of PNR data.

Procedures to use PNR data in profiling activity form part of the Department's Air Traveller Targeting Governance processes. An assessment is made on each profile request, which utilises PNR data, to ensure that the use of the PNR data is necessary, proportionate and compliant with the purpose limitations of the Agreement, prior to any development or testing.

Q2: How does the Australian Competent Authority ensure that such criteria are non-discriminatory and specific?

Prescribed procedures and test cases are used in the data warehouse environment.

Procedures to use PNR data in profiling activity form part of the Department's Air Traveller Targeting Governance processes. To remove the risk that profiling may be discriminatory or specific, each profile must use at least five (5) attributes so as to not be specific to individuals. Automated Processing activity that would be seen as discriminatory is rejected.

There is no automated processing on attributes that could be deemed 'sensitive data' and these attributes are removed from Automated Processing systems.

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

PNR data is not compared to other databases. PNR data is stored in a separate database within the PNR System, which is partitioned from other Departmental sources. All of the activities

undertaken with PNR data are performed for the purposes outlined within the Agreement.

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.

See 'Data Retention' attachment.

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

See 'Data Retention' attachment.

Information sharing

Q1: In what instances has PNR data been shared with other Government authorities listed in Annex 2 and in what proportion with each domestic authority has PNR data been shared?

PNR data has been shared with domestic government authorities listed in Annex 2 for the investigation of serious transnational crime and terrorist offences.

From 2015, disclosures, as part of the Request for Information process, to partner agencies listed in Annex 2 make up nearly 50% of disclosures of PNR data. The average proportion of PNR disclosures for each agency are as follows (as a percentage of total PNR disclosures):

- Australian Crime Commission/Australian Criminal Intelligence Commission: 3%
- Australian Federal Police: 32.9%
- Australian Security Intelligence Organisation/Attorney General's Department: 8.8%
- Department of Immigration and Citizenship: 0.7%*
- Commonwealth Director of Public Prosecutions: Nil disclosures recorded.
- Office of Transport Security, Department of Infrastructure and Transport: Nil disclosures recorded.

* The Department of Immigration and Citizenship integrated with Customs and Border Protection in 2015, and therefore disclosures from that time are considered and recorded as internal disclosures.

All requests for PNR data, through the Request for Information process, are assessed on a case-by-case basis. PNR data elements are not disclosed if the request does not satisfy the request, use or disclosure requirements for PNR data.

From 2015 to date, the Department processed 7970 requests for PNR data from domestic

www.parlament.gv.at

partner agencies and made 5208 disclosures - a disclosure percentage of 65.3%.

Q2: How is it being ensured that receiving authorities afford to PNR equivalent or comparable safeguards as set out in the agreement?

The Department cannot provide an absolute guarantee on other government authorities' actions; however, these government authorities provide a written and formal undertaking that they will only use information given to them by the Department for the purposes for which it was given and will not pass the information to a third party unless required to do so by law. The undertaking is a requirement before a receiving authority can be approved for an ongoing authorisation. Ongoing authorisations outline specific circumstances where specific classes of information may be released for a specific purpose.

All PNR data is disclosed in accordance with the Agreement and a caveat is provided outlining the conditions under which it is disclosed at each occasion of disclosure.

Q3: Are the requests for PNR data made by other Government authorities validated or approved by a judicial or other independent authority?

No. There is no requirement for requests for PNR data to be approved by a judicial or other independent authority.

All requests for PNR data from other Government authorities are all logged and auditable, with assurance activities undertaken on a regular basis by internal Departmental work areas.

Q4: Is there a need to add or remove departments or agencies - whose functions are directly related (or not anymore) to preventing, detecting, investigating or prosecuting terrorist offences or serious transnational crime - to this list in Annex 2?

Annex 2 reflects Departments that have functions that relate to the scope of the Agreement. Due to the extensive time elapsed since the agreement came into force, there are other Government authorities who also have a remit to protect the Australian community from acts of terrorism and serious transnational crime. These authorities work in collaboration with the Department in other ways, and there is no current requirement to add or remove other departments or agencies.

Since the Agreement was signed, Departments have changed names or have been administratively amalgamated:

- The Australian Crime Commission is now the Australian Criminal Intelligence Commission.

- The Department of Immigration and Border Protection, and the Office of Transport Security were amalgamated into the Department of Home Affairs.

Q5: With which countries has PNR of EU Member State citizens or residents been shared?

From 2015 to the current date, the Department has made 21 international disclosures of PNR data. The citizenship of the subject of the PNR data is not a mandatory field to capture in our record keeping systems.

We can advise that, in 2018, PNR data for one EU citizen (UK) was disclosed to the Australian Federal Police.

A request via the Australian Federal Police Operations Coordination Centre (AOCC), who stated that they 'may release the passenger information to a Foreign Law Enforcement Agency through INTERPOL or the AFP Liaison Network of the country or countries to which the passenger is travelling'.

The Department cannot confirm if the on-disclosure occurred.

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

All requests for PNR data come through the Tactical Intelligence (centralised operating work area) for determination as to whether PNR data will be disclosed to a third country authority.

A formal Memorandum of Understanding must be in place between the Department and the third country/international agency. Consideration of the third country policies and safeguards are a consideration for the development of the Memorandum of Understanding. Further, Tactical Intelligence may engage with the Department's International Policy areas, or our international diplomatic representatives (Counsellors/First Secretaries at international posts), on the Department's bilateral agreements and working arrangements with the requesting country/authority.

Furthermore, the request and disclosure for PNR data is assessed against the Department's secrecy and disclosure framework, which sets out the legislative and policy permissions for disclosure of information, including PNR data.

Q7: How is it being ensured that receiving authorities afford to PNR equivalent or comparable safeguards as set out in the agreement?

The Department cannot provide an absolute guarantee on other government authorities' actions; however, these government authorities provide a written and formal undertaking that they will only use information given to them by the Department for the purposes for which it was given and will not pass the information to a third party unless required to do so by law. The undertaking is a requirement before a receiving authority can be approved for an ongoing authorisation. Ongoing authorisations outline specific circumstances where specific classes of information may be released for a specific purpose.

All PNR data is disclosed in accordance with the Agreement and a caveat is provided outlining the conditions under which it is disclosed at each occasion of disclosure.

Q8: What are the mechanisms by which the Australian competent authority communicates with relevant EU Member States authorities, Europol or Eurojust?

Communication with international partner agencies may occur through different PROTECTED channels. This may include encrypted email, regular email (protected enclave) or appropriate cable terminals (eg. SATIN).

The Department may also utilise the Australian Federal Police (AFP) to disclose information through INTERPOL or the AFP Liaison Network of the requesting country, if appropriate.

ANNEX B

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

Igor Angelini, European Commission, DG Migration and Home Affairs

Manuel Garcia Sanchez, European Commission, DG Justice and Consumers

Sebastian Hummeler, expert on data protection in the law enforcement area from the German data protection authority

Laszlo Tarr, expert on law enforcement, Head of Passenger Information Unit, Hungary

The members of the Australian team were:

Richard Gray, First Assistant Secretary Intelligence Division

Michael Thomas, Assistant Secretary Border Intelligence Fusion Centre

David Vosnakes, Director Tactical Intelligence

Megan White, Assistant Director Tactical Intelligence (PNR Policy)

www.parlament.gv.at