EUROPEAN
COMMISSION

Brussels, 12.1.2021
SWD(2021) 5 final

COMMISSION STAFF WORKING DOCUMENT
Accompanying the document

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(2021) 19 final}

Contents

1. BACKGROUND AND METHODOLOGY OF THE JOINT REVIEW 2
2. RELEVANT ORGANISATIONAL CHANGES OCCURRED IN AUSTRALIA..... 5
3. RECOMMENDATIONS FROM THE 2013 REVIEW 7
   3.1. Retention of data - data used in a specific investigation (Article 16) 7
   3.2. Police, law enforcement and judicial cooperation (Article 6) 8
4. THE OUTCOME OF THE 2019 JOINT REVIEW 8
   4.1. PNR processing activities 8
   4.2. Main findings 10
      4.2.1. Geographical scope (Article 2(d)) 10
      4.2.2. Scope of application (Article 3) 10
      4.2.3. Provision of PNR data (Article 4) 11
      4.2.4. Police and judicial cooperation (Article 6) 12
      4.2.5. Data protection and Non-discrimination (Article 7) 13
      4.2.6. Sensitive data (Article 8) 13
      4.2.7. Data security (Article 9) 14
      4.2.8. Oversight and accountability (Article 10) 16
      4.2.9. Transparency (Article 11) 18
      4.2.10. Access, rectification and erasure, and redress (Articles 12-14) 19
      4.2.11. Automated processing of PNR data (Article 15) 20
      4.2.12. Retention of data (except for data used in a specific investigation)(Article 16) 21
      4.2.13. Logging and documentation of PNR data (Article 17) 22
      4.2.14. Domestic sharing and onward transfers (Article 18) 22
      4.2.15. Transfers to authorities of third countries (Article 19) 23
      4.2.16. Method and frequency of transfer (Articles 20-21) 25
   4.3. Summary of recommendations 25
5. CONCLUSIONS 27

ANNEX A 29

1. BACKGROUND AND METHODOLOGY OF THE JOINT REVIEW

In order to enhance and encourage cooperation to effectively prevent and combat terrorism and serious transnational crimethe European Union and Australia concluded an Agreement on the processing and transfer of PNR data by air carriers to the (at the time) Australian Customs and Border Protection Service (herein after "the Agreement").[1] The Agreement entered into force on 1 June 2012.

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

Under the Customs Act, the authority to request such data is conferred to the Comptroller- General of Customs, who then delegates dedicated officers to access and process the data. After recent organisational changes and amendments to relevant national legislation (see chapter 2), the function of "Comptroller-General of Customs" is now performed by the Australian Border Force Commissioner, who has overall responsibility for the enforcement of customs law and collection of border-related revenue.

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

According to Article 24(2) of the EU Australia PNR Agreement, the Parties shall jointly review the implementation of the Agreement and any matters related thereto one year after its entry into force and regularly thereafter. The review should in particular look into the mechanism of masking out data according to Article 16(1)(b), any difficulties related to the operational efficiency or cost effectiveness of the mechanism, and experience acquired with

[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.

similar mechanisms in other mature PNR schemes, including the EU scheme. The first joint review of the Agreement took place in Canberra on 29-30 August 2013 and its outcome was reported on by the Commission to the European Parliament and the Council in 2014[2]. The second joint review was carried out in Canberra on 14 August 2019 and was combined with the joint evaluation of the same agreement (conducted on 15 August and reported separately[3]).

Also in occasion of the second joint review, and in line with the terms of Article 24(3) of the Agreement, the EU was represented by the European Commission. The dedicated team was led by the Director for Security of the Directorate General Migration and Home Affairs (DG HOME) and composed by a policy officer from DG HOME, a policy officer from the Directorate General Justice and Consumers (DG JUST), as well as one law enforcement expert and one data protection expert, both from the EU Member States.

Australia was represented by 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.

A specific methodology, in line with the review conducted in 2013,was agreed with the Australian counterpart and applied in the joint review exercise:

- A questionnaire was sent to the Department in advance of the joint review. This questionnaire contained specific questions in relation to the implementation of the Agreement by the Department and on the organisational changesin the Australian system. The Department provided written draft replies to the questionnaire prior to the joint review and a consolidated version thereafter (see Annex A).
- The EU team was granted access to the Department's premises and carried out a site visit to the Border Intelligence Fusion Centre. The EU team had no access to any system processing PNR data.

[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 of 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 Australia, COM(2020)702.

- The EU team had the opportunity to have exchanges with Department personnel responsible for the PNR programme, including targeters and analysts who use and have access to PNR data.
- The replies to the questionnaire were discussed in detail with the Department. The EU team also had the opportunity and the time to raise further questions with Department officials and address all the various aspects of the Agreement.
- The EU team had an exchange of views with representatives of the Office of the Australian Information Commissioner, following a presentation on the relevant aspects of its oversight activities carried out in the context of the Agreement, as well as the Office of the Commonwealth Ombudsman and the Department area responsible for privacy matters.
- Upon request by the EU team, further documentation was made available during and after the joint review, including reports of formal audits conducted by the Office of the Australian Information Commissioner on PNR data processing by the Department.
- At the request of the Department, all members of the EU team signed a non-disclosure agreement as a condition for their participation in this review exercise.
- For the preparation of this report, the EU team used information contained in the written replies that the Department provided to the EU questionnaire, information obtained from its discussions with the Department, other Australian personnel and during the visit, information contained in the aforementioned documentation received before, during and after the joint review, as well as information contained in other publicly available Department documents. The EU team had no access to the information systems processing PNR data.

Due to the sensitive nature of the PNR programme, some information was provided to the EU team with the condition that it would be treated as classified up to the level of EU Secret. Moreover, the review relies heavily on the interview technique in oral and written form rather than sampling or technical inspections. The present report should be read in the light of these limitations, as well as in the light of the fact that all members of the EU team had to sign non-disclosure agreements exposing them to criminal and/or civil sanctions for breaches.

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 Commission would like to confirm once again the excellent cooperation on the part of all Department and other Australian personnel and express its gratitude for the way in which the questions of the EU team have been replied to.

The mandate of the EU team was limited to review the compliance of the Australian Authorities with the different provisions of the EU Australia PNR Agreement. The Opinion of the Court of Justice[4] on the envisaged EU-Canada PNR Agreement, including its impact on the relevant articles of the Agreement was discussed in detail during the day dedicated to the evaluation of the EU-Australia PNR Agreement (see the evaluation report[5]) as well as the main components and functioning of the EU PNR system as mandated by the EU PNR Directive[6].

Ultimately, the overall scope of the Joint Review was to verify that Australia continues to implement the Agreement in line with the conditions set out therein, to follow up on the recommendations from the previous Joint Review and, if any, breaches of the Agreement since the previous Joint Review.

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 review itself was conducted jointly, this document is not a joint report of the EU and Australian teams.

2. RELEVANT ORGANISATIONAL CHANGES OCCURRED IN AUSTRALIA

According to Article 24 of the Agreement, the Parties shall notify each other of any legislative or regulatory changes which may materially affect the implementation of the Agreement.

In 2015, Australia notified the Commission of legislative and organisational changes concerning the Australian Customs and Border Protection Service (ACBPS). At the time, the Minister for lmmigration and Border Protection announced that the ACBPS would merge

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

5 Report from the Commission to the European Parliament and the Council of 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 Australia, COM(2020)702.

6 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.

with the Department of lmmigration and Border Protection (DIBP) and consequently cease to exist on and from 1 July 2015.

This was the effect of the adoption of the Australian Border Force Act 2015 (ABF Act) which repealed the Customs Administration Act 1985 and abolished the ACBPS as a separate statutory agency. The ABF Act established the ABF within the DIBP and created the position of the ABF Commissioner who was then entrusted with the functions of Comptroller-General of Customs, giving him/her, among other things, the authority to collect PNR data from airlines. At the time, Australia confirmed that the introduced legislative changesdid not have any material impact on the way Australia managed its obligations under the Agreement.

In addition to the notification provided in 2015 to the Commission, on occasion of the present joint review Australia informed the Commission that on 20 December 2017 a new Department (the Department of Home Affairs – referred to as "the Department" within the broader Portfolio) was established through an Administrative Arrangements Order. This renamed the DIBP to Home Affairs, and also brought together the policy responsibilities of the government's national security, border control and law enforcement agencies.

Currently the Department delivers immigration and customs border policy functions previously delivered by the DIBP. The Department incorporates national security, emergency management and criminal justice functions from the Attorney-General's Department. It also now embeds the Office of Transport Security from the Department of Infrastructure and Regional Development, multicultural affairs from the Department of Social Services, and the counter-terrorism coordination and cyber security policy functions previously attributed to the Department of the Prime Minister and Cabinet.

The ABF remains part of the Department, staffed by Departmental officers and headed by the Australian Border Force Commissioner, who, under the ABF Act, continues to perform the function of the Comptroller-General of Customs. Section 64AF of the Customs Act 1901, which gives authority to collect PNR data, remains unchanged through the reorganisation. The organisational changes do not impact the authorisation process under section 64AF, for officers who are authorised to access PNR data.

Australia has confirmed that the Department is currently the competent Australian Government agency for processing PNR data and continues to administer PNR data in accordance with the Agreement. Any reference in the Agreement to the ACBPS should now be read as referring to the Department.

3. RECOMMENDATIONS FROM THE 2013 REVIEW

The 2013 joint review assessed whether Australia had implemented the EU Australia PNR Agreement in line with the conditions set therein. The overall finding was that Australia had fully implemented the Agreement and respected its obligations as regards the data protection safeguards under the Agreement, and processes PNR data in compliance with the strict conditions set out in therein. Australia does not process any sensitive data held in PNR data obtained under the Agreement, and it is actively seeking to further improve the automated identification and deletion of sensitive data. The very targeted way in which Australia assesses PNR data against risk indicators usefully minimises the access to personal data. In addition, the processing of PNR data under the Agreement is subject to a high level of independent oversight by the Office of the Australian Information Commissioner.

As regards issues to be further addressed, the EU team invited Australia to implement measures to ensure the masking out of all data elements after three years which could serve to identify the passenger to whom the PNR data relate. These measures had by the 2019 review been implemented and an automated process runs daily to identify those records that have reached three years since their receipt. It had also been noted that law enforcement cooperation based on the sharing of analytical information obtained from PNR data required more attention. In this respect, Australia was invited to enhance its efforts to ensure reciprocity and pro-actively share analytical information obtained from PNR data with Member States and, where appropriate, with Europol and Eurojust.

Australia was also requested to set up a reporting mechanism that would enable Australia to inform Member States if PNR data received under the Agreement, or analytical information containing such data, was eventually shared with a third country. According to the information provided during the 2019 review, the EU team considers that further improvements can be made for the development of reporting mechanisms and has issued a recommendation in this respect.

3.1. RETENTION OF DATA - DATA USED IN A SPECIFIC INVESTIGATION (ARTICLE 16)

Recommendation from the 2013 Joint Review: While it is in line with the objective of Article 16(3) of the Agreement that different retention requirements apply to PNR data extracted from the PNR data store in specific cases of terrorism or serious transnational crime, ACBPS should continue to ensure that the safeguards set out in the Agreement are also afforded to extracted PNR data.

Progress: Completed

As recommended, information sharing of PNR data must meet specific disclosure provisions in addition to the conditions of the PNR Agreement, and an appropriate caveat is applied to the extracted data transferred to partner law enforcement agencies.

3.2. POLICE, LAW ENFORCEMENT AND JUDICIAL COOPERATION (ARTICLE 6)

Recommendation from the 2013 Joint Review: The EU team welcomed the efforts made by ACBPS to improve the sharing of analytical information obtained from PNR data with the EU that is relevant for the combating of terrorism and serious transnational crime, e.g. by developing system capabilities to better identify such relevant analytical information. The EU team noted that law enforcement cooperation under the Agreement – based on the sharing of analytical information obtained from PNR data – leaves room for improvement and requires more attention. ACBPS was thus requested to respect its commitment to ensure reciprocity and pro-actively share analytical information obtained from PNR data with Member States and, where appropriate, with Europol and Eurojust. The EU team suggested organising a workshop to explore ways on how to improve this cooperation. This workshop took place in Brussels on 28 February 2014.

Progress: Improvements made, ongoing.

4. THE OUTCOME OF THE 2019 JOINT REVIEW

This Chapter provides the main findings resulting from the 2019 joint review of the EU team.

4.1. PNR PROCESSING ACTIVITIES

The joint review team verfied that within the Department, different units are entrusted with specific activities related to the processing of PNR, for both technical and operational functions. The Data Division is responsible for the acquisition of PNR data from carriers and for compliance with all applicable legislative controls. The Department's Enterprise Analytics and Data Science area are responsible for the application of analytical techniques to datasets and develop analytical profiles on PNR data. This area sits within Data Division, which is responsible for enterprise wide data management, which governs at a strategic level how data is collected, stored, quality assured, used, shared and released.

The Intelligence Division is responsible for the operational use, access and disclosure of PNR data for operational purposes and are the main users of PNR data in an operational context. This includes:

- Operational Policy and Compliance
- Air Traveller Profiling (rules development)
- Tactical Intelligence

The Tactical Intelligence area has access to PNR data in order to respond to PNR Requests for Information (RFI) or PNR Alerts from within the Department and from appropriate external partner law enforcement agencies. In this typical reactive function, the Tactical Intelligence area may also use PNR data as part of its intelligence analysis in the occasion of the detection of illicit goods or other crime related events at the border. In that case, the unit may produce an Immediate Detection Analysis (IDA) report which is disseminated to other relevant law enforcement entitites and border crossings to assist in further identifying immediate serious transnational crime or terrorist threats.

The more proactive activities, aimed at accessing PNR data in the risk assessment and verification of passengers who are a potential match to an air traveller profile tailored on serious transnational crime or terrorist offences are performed by the National Border Targeting Centre (NBTC). The NBTC reports to the Australian Border Operations Centre, within the ABF, while being co-located within Intelligence Division's Border Intelligence Fusion Centre. The Department made an statement confirming that PNR data is only accessed when it has been established that a serious transnational criminal in the sense of Article 3(3) of the Agreement is suspected of or has been commited or in the event of a terrorism related request. The authorised officer has to confirm that the access to PNR data meets the relevant threshold.

4.2. MAIN FINDINGS

4.2.1. Geographical scope (Article 2(d))

As foreseen by Article 2(d), the Agreement covers "air carriers that have reservation systems and/or PNR data processed in the territory of the European Union and operate passenger flights in international air transportation to, from or through Australia". It is therefore the aspect of data processing – i.e. whether an airline processes PNR data in a reservation system

located in the territory of an EU Member State – that, inter alia, determines whether the Agreement applies.

The Department uses a Global Flight Schedule provided by a specialised private company to determine that the data being provided stems from a flight operating to, from or through Australia. In the unlikely event that PNR data are not related to a flight that operates to, from or through Australia and are "pushed" by an airline, the message and associated data are rejected.

In the context of the overall scope of the Agreement, it is worth noticing that the Department confirmed that it applied the rules and safeguards as 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.

The Department also confirmed that currently all PNR data are exclusively collected through the so-called "push method", i.e. the data are sent by the air carriers, at regular intervals for each flight concerned, to Department storage IT systems and no access to the airlines' reservation systems is performed.

Conclusion: The EU team considers that the Department applies the rules and safeguards of the Agreement to all flights that are covered by its scope. The Department only collects data by means of the "push method".

4.2.2. Scope of application (Article 3)

Article 3 of the Agreement sets out the purpose limitation of the processing of PNR data under the Agreement. While the Department confirms that the notion of terrorism as set out in Article 3(2) of the Agreement does not give reasons for concern, the definition of serious transnational crime as set out in Article 3(3) of the Agreement continues, at times, to present a challenge. The Department assesses each request on a case-by-case basis and the circumstances surrounding the case, to establish if there are appropriate transnational aspects in the request. This ensures that a consistent definition of "transnational" is applied, and any request that seeks to obtain PNR data has a clear "transnational" aspect. Where the application of the "transnational" definition is not clear, legal advice is requested for the specific case that may be then further used as a precedent by which future requests will be assessed.

Under Article 3(4) of the Agreement Australia can process PNR data for the protection of the vital interests of an individual, such as risk of death, serious injury or threat to health. In 2015, the Department utilised PNR data in the course of the Ebola outbreak as part of the screening aimed at identifying individuals who had left Australia and were returning from high risk areas declared by the World Health Organisation. Such travellers were sent for a health assessment at the airport. The related profile created to identify these travellers matched 2464 passengers, and 1434 of those were referred at the airport for health assessment.

Conclusion: The EU team considers that the Department process PNR data in accordance with the scope of the the Agreement. Procedures have been established to ensure that PNR data are only processed in relation to the purposes of the Agreement, in particular when requests are based in the transnational nature of the crime.

4.2.3. Provision of PNR data (Article 4)

Article 4 of the Agreement regulates the provision of PNR data by air carriers. PNR data are collected directly by the Department using its IT facilities which ensure connection with the airline service providers (Customs Connect Facility – CCF). Irrespective of the specific data formats used by the data suppliers, data items outside the elements listed in Annex 1 of the Agreement are removed and deleted prior to being loaded into the dedicated PNR Data Storage environment within the Department.

Conclusion: The EU team considers that according to the information provided, the Department ensures that only the 19 data elements listed in Annex 1 to the Agreement are kept in the system.

4.2.4. Police and judicial cooperation (Article 6)

According to Article 6 of the Agreement, a set of provisions are in place for police and judicial cooperation between Australia and Member States' authorities or EU agencies involved in law enforcement and judicial cooperation (Europol and Eurojust). Such cooperation can be proactive, whereas Australia ensures the availability, as soon as practicable, of relevant and appropriate analytical information obtained from PNR data to

police or judicial authorities of the Member State of the European Union concerned, or to Europol or Eurojust within the remit of their respective mandates.

The cooperation can also be reactive, whenever Australia responds to a request from police or judicial authority of a Member State of the European Union, or Europol or Eurojust within the remit of their respective mandates, for PNR data or relevant and appropriate analytical information obtained from PNR data, which is necessary in a specific case to prevent, detect, investigate, or prosecute within the European Union a terrorist offence or serious transnational crime.

While there has not been any proactive cooperation initiated by Australia, since the last Joint Review, the Department has received five (5) requests from police or judicial authorities of EU Member States, Europol or Eurojust for PNR data, through the Request for Information (RFI) process.

The Department has made two (2) disclosures. Both disclosures occurred in April 2015. PNR data was accessed and disclosed via the Australian Federal Police (AFP) to Europol.

Both requests were received via Interpol, on behalf of the United Kingdom. Europol was attempting to monitor a Scottish resident, who the United Kingdom suspected was currently in Australia. The person of interest was under investigation for its suspected lead involvement in the trafficking of hard drugs.

Conclusion: The EU team considers that according to the information provided, the Department complies with the provisions of the agreement under Article 6. However, the EU team **recommends** 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 proactive provision of relevant and appropriate analytical information.**

4.2.5. Data protection and Non-discrimination (Article 7)

According to Article 7(1), PNR data under the Agreement shall be subject to the provisions of the Australian Privacy Act 1988 governing the collection, use, storage and disclosure, security and access and alteration of personal information held by most Australian Government

departments and agencies, subject to the oversight by the Office of the Australian Information Commissioner (OAIC) in accordance with Article 10.

According to Article 7(2) of the Agreement, Australia shall ensure that the safeguards applicable to the processing of PNR data under the Agreement and relevant national laws apply to all passengers without discrimination, regardless nationality or country of residence or physical presence in Australia. According to information provided by Australia, the Department applies the same strict data protection safeguards to the processing of all PNR data it receives, irrespective of the data subject's nationality, country of residence or physical presence in Australia.

Conclusion: The EU team considers that according to the information received, Australia complies with the obligation of non-discrimination.

4.2.6. Sensitive data (Article 8)

According to Article 8 of the Agreement, any processing of sensitive PNR data shall be prohibited. Moreover, Article 8 also regulates that to the extent that the PNR data of a passenger which is transferred to the Department include sensitive data, such data shall be deleted.

Department representatives explained the procedures in place for the handling of sensitive data in the event they are transmitted. To that end the Department:

- applies filters over Salutation and Special Service Requests (SSR) (i.e. meal types and special passenger requirements).
- ensures that there is no automated processing over fields that may contain sensitive data (i.e. no profiling or watchlist processing is applied to fields that may contain sensitive data).
- maintains a combination of manual and automated controls to prevent processing fields that may contain sensitive data.
- undertakes a manual review prior to disclosing relevant PNR data elements to external agencies to ensure that the information to be disclosed does not contain any sensitive data.

These controls are further outlined in the Department's PNR Control Framework.

Conclusion: The EU team considers that the Department provides for controls to prevent access to sensitive data. and does not use sensitive data.**However, the EU team recommends that the Department puts in place mechanisms aiming to immediately delete sensitive data if detected. The EU team recognises the Department's confirmation, received in the meantime, that work has already commenced into putting these mechanisms in place. The team also recommends including this question in future oversight activities by the Office of the Australian Commissions (OAIC) as regards compliance to other relevant principles in the context of the processing of PNR data like cross-border disclosure of personal data or the deletion of sensitive data.**

4.2.7. Data security (Article 9)

According to the information provided by Australia, the Department continues to apply a rigid PNR control framework that provides a complete inventory of the security safeguards and the automated and manual controls in place over PNR data. In addition, the Department has implemented some further key controls:

- Full disk encryption, encrypting data on the hardware and the operating system, including data at rest.
- No automated disclosures of PNR data, and ensuring that other agencies do not receive feeds of PNR data.
- Intelligence reports or other intelligence products are distributed using email, with dissemination limiting markers where appropriate. Reports and products can also be sent over a security-classified network for documents classified as Secret or above, or distributed by hand.
- All staff must complete privacy induction training when they commence employment.
- Authorised officers who handle PNR data must complete a PNR training module (online or eLearning) before they are granted access to PNR data.

The EU team was informed that the dedicated teams with access to PNR data are located in a secure area with restricted access, and a layered level of logins are required to access the information technology systems. User access controls are in place and each user profile must

be authorised by the ABF Commissioner. Every activity conducted by an user on PNR data is logged.

Access to PNR data is limited to a restricted number of officials within the Department who are specifically authorised by the ABF Commissioner under Section 64AF of the Australian Customs Act. There are 259 officers who are authorised officers with access to PNR data. Of that, 140 fall within the scope of Information Technology , who perform different roles in the maintenance of the PNR System and the development of new and improved capabilities or the replacement of existing capabilities.

It should also be reported that on 12 March 2014, a new set of Australian Privacy Principles (APPs) and amendments to the Privacy Act 1988 (Cth) came into force. The new APPs replaced the National Privacy Principles and Information Privacy Principles. The Department has an obligation under APP 11 of the Privacy Act 1988 to take reasonable steps to protect the information it holds from misuse, interference and loss; and from unauthorised access, modification or disclosure.

In 2017, changes to the Privacy Amendment (Notifiable Data Breaches) Act 2017 came into force. The Department implemented procedures with respect to the reporting of suspected privacy breaches.

Suspected privacy breaches are reported to the Department's Privacy section, who are responsible for providing policy advice about the Privacy Act. The procedure supports prompt reporting of a suspected breach to ensure that appropriate containment measures are taken and that the Department reports eligible data breaches to the Office of the Australian Information Commissioner (OAIC), and the individuals whose personal information was affected by the breach. There have been no changes from a technical perspective.

In 2015, the Department notified the European Commission of a breach against the provisions of the PNR Agreement, which occurred in 2014. There have been no other privacy breaches of PNR data through a breach of data security or other reported breaches of data security.

The Department also informed the EU team that The OAIC can investigate a privacy breach, including a breach of data security, either following a complaint or on the Commissioner's own initiative. This may result in enforcement action being taken by the OAIC, which includes powers to accept an enforceable undertaking and bring proceedings to enforce an enforceable undertaking, make a determination and bring proceedings to enforce a

determination, seek an injunction to prevent ongoing activity or a recurrence, or apply to court for a civil penalty order for a breach of a civil penalty provision.

Conclusion: The EU team considers that according to the information provided, the Department complies with its data security obligations under the Agreement. However, **the EU team notes that while the overall number of officers having access to PNR data seems reasonable, the proportion of IT system administrators (140) is quite important and recommends that the Department should limit access rights to PNR data only to those with an operational need to use and view that data.**

4.2.8. Oversight and accountability (Article 10)

Overall compliance with data protection rules by the Australian government authorities processing PNR data continues to be subject to the oversight by the OAIC. During the joint review, the EU team met with and received presentations from representatives of the OAIC. The reference national framework is mainly contained in the Privacy Act 1988 (Privacy Act) which was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations handle personal information.

The Privacy Act includes 13 Australian Privacy Principles (APPs), which apply to most Australian Government agencies, including the Department.

In line with Article 10(2) of the Agreement, the Department and the Office of the Australian Information Commissioner (the OAIC) have a Memorandum of Understanding in place, which provides a regular audit program for the Department's use, disclosure, storage and security of Passenger Name Record (PNR) data.

This Memorandum of Understanding has regard to the oversight and accountability functions of the OAIC contained in Article 10 of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record data by Air Carriers to the Australian Customs and Border Protection Service (the Agreement).

The Department's records show that PNR audits have been conducted by the OAIC since 2009, and that four (4) PNR audits were conducted since the previous joint review. The reviews mainly focused on Australian Privacy Principles 6 (use and disclosure) and 11 (security of information). Compliance to other relevant principles in the context of the

processing of PNR data, like cross-border disclosure of personal data or the deletion of sensitive data, have not been subject so far to review by the OAIC.

The EU review team went through the recommendations made by OAIC and related implementation carried out by the Department. Such recommendations refer, i.a., to the information related to processing activities that should be publicly available, security safeguards, including the need to implement regular audit or quality assurance programmes for specific processing activities as well as de-personalisation and destruction obligations for PNR data.

OAIC representatives also informed the team about the follow-up activities carried out in relation to the recommendations made in each annual reviews.

The Assistant Commissioner of the Office of the Australian Information Commissioner explained that the formal audits had shown a high degree of compliance in the way the Department had processed PNR data.

The EU team was informed that no complaints related to the Agreement have been lodged with the Australian Information Commissioner or with the Commonwealth Ombudsman.

In addition to independent external oversight, the Department has maintained internal audit and oversight mechanisms in place for its PNR system. This includes quality assurance processes implemented by the Department Policy Section (e.g. review of the enforcement of instructions and guidelines for PNR and the PNR controls framework), systems monitoring by the IT division, reviews of user access and audit logs, and further internal audits. The Department underlined its commitment to continuing to work closely with the OAIC to ensure oversight and accountability of the PNR program is achieved.

Conclusion: The EU team considers that both the Department and OAIC take oversight and accountability obligations seriously under Article 10, including annual reviews. However, the team notes that some recommendations could have been fulfilled more swiftly and efficiently by the Department. Moreover, the fact that the audit reports of 2017 and 2018 have not been yet adopted may have an impact on the proper functioning of the oversight mechanism. Furthermore, the EU team **recommends to broaden the scope of the regular PNR audits carried out by the OAIC including on issues concerning onward sharing and cross-border disclosure of personal data**.

4.2.9. Transparency (Article 11)

Article 11 of the Agreement sets out the obligations to ensure transparency in relation to the collection and processing of PNR data, including requesting air carriers to provide passengers with clear and meaningful information in relation to the collection, processing and purpose of the use of PNR data

The Department website provides information on the purposes for which the Department collects and uses of PNR data. The statement also outlines the purpose, authority, use and disclosure provisions relating to PNR data[7].

Concerning the obligation to request air carriers to provide passengers with clear and meaningful information in relation to the collection, processsing and purpose of the use of PNR data, the Department informed the team that the information to the passengers remain within the remit of the air carriers; air carriers being subject to the Australian Privacy Principles (APPs) will typically satisfy their obligations under APP 5 by including information about their information handling practices in the terms and conditions on the ticket at the time of purchase. The EU team notes that the Department should request that air carriers to include in their privacy notices information in relation to the disclosure of PNR data to the Australian authorities.

Moreover, 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 1442i) is the notification method employed[8]. This form is broad and contains extensive information on all possible data collection and processing activities of the Department. Information on the purpose of collection and use of PNR is described very briefly. It does not contain information on how to request access, correction and/or redress but provides a link to the relevant website of the Department. The collection of PNR does not trigger a notification with this form.

Conclusion: **The EU recommends that Australia improves the information to passengers in relation to the processing of PNR data and requests that air carriers provide**

[7] 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.

[8] The form is available on the Home Affairs website at the following link: https://immi.homeaffairs.gov.au/form-listing/forms/1442i.pdf.

passengers with clear meaningful information in relation to the collection, processsing and purpose of the use of PNR data.

4.2.10. Access, rectification and erasure, and redress (Articles 12-14)

Article 12 of the Agreement gives to any individual the right to access his or her PNR data, following a request made to the Department. Under Australian Privacy Principle (APP) 12, the Department has an obligation to give an individual access to personal information held about them. If there is a specific exemption, then an individual may submit a Freedom of Information request under the Freedom of Information Act 1982. In its reply to the questionnaire, the Department explained it had not received any request or application for access to information under APP 12 for PNR data. Conversely, the Department has received twelve (12) requests for access to information under the Freedom of Information Act 1982 where the scope has included PNR data and has disclosed PNR data in all 12 instances, within the applicable deadline (30 days form the date of the request).

Individuals have a right to request correction of their own personal information under Australian Privacy Principle (APP) 13, contained in Schedule 1 of the Privacy Act 1988 and section 48 of the Freedom of Information Act 1982.

Similarly, there have been no complaints lodged by individuals with the OAIC against a decision by the Department to refuse or restrict access to PNR data.

According to Article 13 of the Agreement, any individual shall have the right to seek the rectification of his or her PNR data processed by the Department where the data is inaccurate. Individuals have a right to request correction of their own personal information under Australian Privacy Principle (APP) 13, contained in Schedule 1 of the Privacy Act 1988 and section 48 of the Freedom of Information Act 1982. In its reply to the questionnaire, the Department explained it had not received any request seeking the rectification of PNR data.

According to Article 14 of the Agreement, any individual shall have the right to effective administrative and judicial redress in case any of his or her rights referred to in the Agreement have been violated. In its reply to the questionnaire, the Department explained that any individual – including persons not present in Australia – has means available to seek administrative or judicial redress without discrimination. The Department stated that no individual had sought administrative or judicial redress in cases related to the rights referred to in the Agreement.

The procedures on how to exercise the right of redress are explained on the Department's website[9]. Also OAIC confirmed that they had received no requests from individuals seeking administrative redress related to the rights referred to in the Agreement.

The Australian Privacy Commissioner also explained that on the basis of the Australian Ombudsman Act, any person – including persons not present in Australia – aggrieved by actions taken by the Department can submit a complaint to the Office of the Ombudsman. Between January 2014 and July 2019, the Commonwealth Ombudsman has had no approaches recorded regarding the EU-Australia PNR agreement (see also replies to the questionnaire, available in Annex A). This avenue is also open to people who are not satisfied with the way their matter has been dealt with by the Office of the Australian Information Commissioner.

Conclusion: The EU team considers that according to the information provided, Australia complies with the obligation to provide the right of access, rectification, erasure and redress.

4.2.11. Automated processing of PNR data (Article 15)

Article 15(1) of the Agreement regulates that no decision shall be taken solely on the basis of automated PNR processing which significantly affects or produces an adverse legal effect on a passenger. According to the information presented to the team, the Department follows the principle for machine learning and artificial intelligence that no decision which negatively impacts an individual or organisation is to be made by a computer and that potentially negative decisions must be passed to a human to review the information and make a decision. This aligns with the criteria of Art. 15(1) of the Agreement.

Article 15(2) regulates that the Australian Customs and Border Protection Service shall not carry out the automated processing of sensitive data. In compliance with the Agreement, the Department ensures that there is no automated processing over fields that may contain sensitive data. The Department additionally maintains a combination of manual and automated controls to prevent processing over fields that may contain sensitive data.

[9] https://www.homeaffairs.gov.au/access-and-accountability/our-commitments/privacy/explaining-and-reviewing-decisions

Conclusion: The EU team considers that according to the information provided, Australia complies with the requirements under Article 15.

4.2.12. Retention of data (except for data used in a specific investigation)(Article 16)

Article 16 of the Agreement sets out the requirements for the retention and deletion of PNR data. The Department retains PNR data, obtained under the Agreement, separately from other systems and data it collects and stores. In compliance with the Agreement, the Department retains PNR data for five and a half years, with an automated process in place for inserting timestamps used to derive the masking and deletion date. After that period, PNR data is automatically deleted.

Article 24(2) of the Agreement sets out that the joint review should in particular look into the mechanism of masking out data according to Article 16(1)(b). At the time of the previous review such mechanism was being finalised, as the three years period for applying the masking had not elapsed yet. The EU team was informed that since then, the Department has implemented the measures to mask out data after three years. An automated process now runs daily to identify those records that have reached three years since they were collected. A summary of results are emailed to the PNR mailbox. These records are then masked from view.

Conclusion: The EU team considers that according to the information provided, the Department retains and deletes PNR data in full compliance with the Agreement.

4.2.13. Logging and documentation of PNR data (Article 17)

Article 17(1) of the Agreement regulates that logging and documentation procedures are applied by the Department for the purpose of verification of lawfulness of the data processing, self-monitoring and ensuring appropriate data integrity and security of data processing.

The EU team was informed that the Department complies with that requirement by employing audits logging in relation to PNR data: i) audit logging of all users access, ii) audit logging at the PNR database level and iii) logging and record-keeping of all information disclosures to other government authorities.

Conclusion: The EU team considers that according to the information provided, Australia complies with the obligations under Article 17.

4.2.14. Domestic sharing and onward transfers (Article 18)

Article 18 of the Agreement regulates the onward transfer from the Department to other government authorities of Australia. The Department explained that it shared PNR data on a case-by-case basis with the government authorities of Australia listed in Annex 2 of the Agreement in accordance with the Agreement.

From 2015, disclosures, as part of the Request for Information process, to partner agencies listed in Annex 2 of the Agreement make up nearly 50% of disclosures of PNR data. The average proportion of PNR disclosures to each agency, on a case by case basis, 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.

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.

The EU team was provided with a copy of the form (Client Request for Information (RFI) form) used. The requestor has to specify the specific offence undergoing investigation justifying the request, the intendend use of the data as well as some background information on the events jusfifying the query. For EU PNR data, an statement is made in the sense that data can only be processed “for the purpose of detecting, investigating and prosecution of terrorists offences or serious transnational crime” in accordance with Article 3 of the Agreement. The form also includes a reference to the definition of serious transnational crime under Article 3.3 of the Agreement.

The form also includes a statement on the obligation not to "further use or disclose the information except for the purpose for which it was provided, unless permission in writing is first sought from the Department or such use or disclosure is required or authorised by law.

From 2015 to date, the Department processed 7970 requests for PNR data from domestic partner agencies and made 5208 disclosures - a disclosure percentage of 65.3%.

The Department explained that all disclosures of PNR data included a caveat governing the use, storage and further disclosure of PNR data disclosed by the Department. For instance, each caveat clearly states the purpose limitation of the PNR data, and that the PNR data cannot be further disclosed without the prior written permission of the Department.

Conclusion: The EU team considers that according to the inforomation provided, the domestic sharing of PNR data with other government authorities of Australia takes place in compliance with the Agreement. However, the EU team reccomends to put in place follow-up controls to ensure that all the conditions in Article 18 are fulfilled, in particular on specific restrictions to the access, use and further disclosure of the information.

4.2.15. Transfers to authorities of third countries (Article 19)

Article 19 of the Agreement regulates the onward transfer from the Department to authorities of third countries. These kind of requests come through the Tactical Intelligence area (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 Australia's international diplomatic representatives (Counsellors/First Secretaries at international posts), on the Department's bilateral agreements and working arrangements with the requesting country/authority.

The Department is obligated under the Privacy Act and Australian Privacy Principle 8 – Cross-border data flows – to take reasonable steps to verify that the third-party overseas recipient is subject to laws providing substantially similar protection as the APPs, unless

certain exceptions apply, including obtaining the individual's consent to the transfer of information or if there is a serious threat to life, health or safety or to public health or safety. Under Australian Privacy Principle 8 and 16C of the Privacy Act, if the Department discloses personal information to an overseas recipient, they are accountable for any acts or practices of the overseas recipient in relation to the information that would breach the Australian Privacy Principles unless an exception is applied to the requirement in APP8.1. At the same time, the government agencies from third countries receiving the PNR data must 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. From 2015 to the current date, the Department has made 21 international disclosures of PNR data.

Information on which third countries PNR data has been disclosed by Australia in reply to a third country request was not disclosed for confidentiality reasons. In that regard, the EU team notes that the joint declaration on the Agreement includes, in the context of the joint review, the exchange of information regarding the transfers of European Union citizens' and residents' PNR data to the authorities of third countries as laid down in Article 19 of the Agreement.

Moreover, the joint declaration on the Agreement expressly states that where the data of a European Union citizen or resident is transferred under Article 19(1)(f), specific reporting mechanisms between the authorities of Member States and of Australia should be established. According to the information provided, these mechanisms have not been established so far.

Conclusion: The EU team welcomes the efforts made by the Department to fulfill the its obligations in accordance with Article 19 of the Agreement. However, The EU team notes that, in order to assess the level of compliance, information on the third countries to which EU PNR data has been disclosed should have been provided. The lack of such information prevents a comprehensive assessment of the fulfilment of the obligations under Article 19. The EU team also considers, according to the information provided, that the relevant reporting mechanisms mentioned in the joint declaration on the Agreement have not yet been established.

4.2.16. Method and frequency of transfer (Articles 20-21)

Articles 20 and 21 of the Agreement regulate the method and frequency of PNR data transfers. The Department confirmed that the "push" method is the exclusive method of transfer of PNR data for air carriers that have a reservation systems or data processing in the territory of an EU Member States.

The Department requires airlines to push PNR data a total of five times: 72 hours before departure, 24 hours before departure, two hours before departure, one hour before departure and at the actual departure time. The EU team was informed that exceptions according to Art. 21 (2) and (3) have not occurred.

Conclusion: The EU team considers that the Department fully complies with the Agreement in relation to the adoption of the "push" method.

4.3. SUMMARY OF RECOMMENDATIONS

1) ***Article 6: Police and judicial cooperation*** - if there is available intelligence or information suggesting that broader criminal networks identified by processing PNR data are potentially affecting the EU Member States, the Department should consider launching a PNR data exchange pilot between the relevant EU and the Australian authorities, with the involvement of Europol. Such a pilot project could potentially serve to further define and enhance the process for PNR data sharing and operational cooperation between Europol, Member States' competent authorities and the Australian competent authorities.

2) ***Article 8: Sensitive data*** - the Department should put in place mechanisms aiming to immediately delete sensitive data if detected.

3) ***Article 9: Data Security*** - the Department should limit access rights to PNR data only to those with an operational need to use and view that data.

4) ***Article 10: Oversight and accountability*** - The periodical assessments made by the OIAC should go into greater details on the various aspects of PNR processing.

5) ***Article 11: Transparency*** - the Department should improve information to passengers in relation to the processing of PNR data and to further encourage air carriers to provide passengers with information in relation to the collection, processing and purpose of the use of PNR data.

6) **Article 18: Domestic sharing and onward transfers** - the EU team reccomends to put in place follow-up controls to ensure that all the conditions in Article 18 are fulfilled, in particular on specific restrictions to the access, use and further disclosure of the information.

7) **Article 19: Transfers to authorities of third countries** - the Department is requested to respect its commitments to provide information in line with the joint declaration to the Agreement, including regarding the set up of reporting mechanisms.

5. CONCLUSIONS

The joint review process has enabled the EU team to better understand how the data is used in practice and provided the opportunity for direct communication with targeting and analytical staff and other officials involved in the processing of PNR. During this joint review, the overall finding is that **the Department implements the Agreement in accordance with its terms**.

Australia respects its obligations as regards the data protection safeguards under the Agreement, and processes PNR data in compliance with the strict conditions set out therein. Moreover, Australia provides for controls to prevent access to sensitive data and complies with its obligation to provide the right of access, rectification, erasure and redress. In addition, the processing of PNR data under the Agreement is subject to a high level of independent oversight by the Office of the Australian Information Commissioner.

As regards issuses to be further addressed, Australia is invited to enhance its efforts to ensure reciprocity and pro-actively share analytical information obtained from PNR data with Member States and, where appropriate, with Europol and Eurojust. The EU team recognised the efforts made by Australia to comply with the Agreement and the positive steps taken to implement all recommendations from the 2013 review. However, even if the Department provides for controls to prevent access to sensitive data and does not use sensitive data; immediate deletion of such data, if received, should be ensured. Additionally, the number of IT staff with access to PNR has been raised by the EU team as a concern.

Whilst the EU team is satisfied that oversight mechanisms are in place, it is important that the assessments of the OAIC to be broader and adopted on time. Importantly, the EU team notes that the Department should encourage air carriers to include in their privacy notices information in relation to the disclosure of PNR data to the Australian authorities and for the Australian authorities to improve information to passengers in relation to the processing of PNR data. The Department should also carry out follow-up controls concerning the domestic sharing and onward transfers of information. Finally, the Department should ensure information in line with Article 19 and the joint declaration to the Agreement is provided, including to EU Member States where the data of a European Union citizen or resident is transferred to a third country.

A number of recommendations are made to the Department in Chapter 4. These should be reviewed in the next regular joint review.

ANNEX A

Questionnaire[10] for the Australian Authority responsible for the processing of PNR and replies

Questions of a general nature

Q1: Are all mechanisms required to properly implement the Agreement, in particular those aimed at implementing the safeguards, in place and operating satisfactorily?

Yes. The Department believes that the technical requirements are being met satisfactorily. For example, role-based access controls are in place to ensure that only authorised and approved officers have access to the data, and audit/event logs are maintained and sent to a Security Information and Event Management (SIEM) application in a secure network.

Q2: Have any specific incidents occurred during the implementation of the Agreement?

No. No specific incidents have occurred regarding the implementation of the Agreement's requirements.

Q3: Have legislative or regulatory changes occurred, which could affect the Agreement as described in Article 24 paragraph 1?

No. There have been no legislative or regulatory changes to Australian legislation that would materially affect the Agreement.

Amendments to the *Privacy Act 1988* and the Australian Privacy Principles, which came into force in 2014, strengthened the collection and handling of personal information by Australian Government agencies and many businesses in a range of sectors, as well as new reporting obligations. These changes will be covered in more detail during the applicable agenda item during the Joint Review.

-Q4: Could you provide an outline of the structural and organisational changes that have taken place and a description of the new organisational structure that underpins the processing of PNR data received under the Agreement?

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

In addition to the advice provided in 2015 on the organisational and legislative changes relating to the Australian Customs and Border Protection Service, the Department advises that—on 20 December 2017—the Department of Home Affairs (the Department) was stood up through an Administrative Arrangements Order. This renamed the Department of Immigration and Border Protection to the Department of Home Affairs, and also bought together the policy responsibilities of the government's national security, border control and law enforcement agencies.

The Department of Home Affairs continues to deliver immigration and customs border policy functions previously delivered by the Department of Immigration and Border Protection. It also incorporated national security, emergency management and criminal justice functions from the Attorney-General's Department; the Office of Transport Security from the Department of Infrastructure and Regional Development; multicultural affairs from the Department of Social Services; and the counter-terrorism coordination and cyber security policy functions from the Department of the Prime Minister and Cabinet.

We confirm that the Department remains the competent Australian Government agency for processing Passenger Name Record data (PNR data) and continues to administer PNR data in accordance with the European Union-Australia PNR Agreement (PNR Agreement).

Section 64AF of the *Customs Act 1901* remains unchanged through the recent Machinery of Government change to form the current Department. We confirm that the organisational changes do not impact the authorisation process under section 64AF, for officers who are authorised to access PNR data.

The Australian Border Force (ABF) remains part of the Department. The ABF forms part of the Department, is staffed by Departmental officers and headed by the Australian Border Force Commissioner (who is appointed under the ABF Act as both ABF Commissioner and the Comptroller-General of Customs). The ABF is responsible for performing the operational and enforcement functions of the Department. The ABF is not a separate statutory agency.

The organisational structure that underpins the processing of PNR data remains relatively unchanged. While there have been some administrative changes to internal reporting lines and broad organisational structure, the key work areas remain as the subject matter experts.

In summary, the Data Division are responsible for the acquisition of PNR data from carriers and for compliance with stringent legislative controls. The Department's Enterprise Analytics

and Data Science area is also within the Data Division.

The Intelligence Division is responsible for the operational use of PNR data and are the main users of PNR data. This includes:

- Operational Policy and Compliance
- Advanced Analytics
- Air Traveller Profiling (rules development)
- Tactical Intelligence

The Department operates a centralised model for access to PNR data. Tactical Intelligence access PNR data to facilitate PNR Requests for Information or PNR Alerts from within the Department and from appropriate external partner law enforcement agencies. Tactical Intelligence may also use PNR data as part of their intelligence analysis to formulate an Immediate Detection Analysis (IDA) report to assist in further identifying immediate serious transnational crime or terrorist threats and risks following detections of illicit goods or other relevant potential border threats.

The National Border Targeting Centre report to the Australian Border Operations Centre, within the ABF, while being co-located within Intelligence Division's Border Intelligence Fusion Centre. They access PNR data in the risk assessment and verification of passengers who are a potential match to an air traveller profile focusing on serious transnational crime or terrorist offences.

The Department's organisational structures can be found on the Department's internet site at the following links:

Department of Home Affairs -

https://www.homeaffairs.gov.au/about-us-subsite/files/home-affairs-org-structure.pdf

Australian Border Force -

https://www.homeaffairs.gov.au/about-us-subsite/files/abf-org-structure.pdf

Q5: Have changes occurred under Article 18, paragraph 2 of the Agreement?

No. No changes have been made to the list of authorities in Annex 2.

As outlined in question 4, the Department of Immigration and Border Protection and the Office of Transport Security were amalgamated into the Department of Home Affairs.

Q6: Can you please outline how it is ensured that any such changes and any related new arrangements for the handling of PNR data are consistent with the obligations under the Agreement?

The functions for border control remain within the Department and the processes established in implementing the PNR Agreement remain in place.

Any structural changes have not had any material impact on how we manage our obligations under the Agreement. PNR data is integral to our risk assessment approach to the border, and critical to identifying serious transitional crime and terrorist offences that present threats to Australia and the global community. We continue to take our obligations regarding data protection, privacy and the Agreement very seriously, and have maintained a strong focus on clear and consistent governance and management of the data to ensure that any access and dissemination remains appropriate and robustly considers legality and proportionality.

I. General provisions

a) Article 2 – definitions

Article 2(d):

Q1: Has Australia obtained any PNR data from flights that depart from the territory of an EU Member State but do not have a stop-over or the final destination in Australia?

No. PNR data is only collected for flights operating to, from or through Australia.

Q2: If so, is there a mechanism in place to filter out PNR data for such flights and to delete related PNR data if obtained by Australia?

The Department uses the OAG Flight Schedule—from the OAG company—to determine that the data being provided is for a flight operating to, from or through Australia. If we were to receive a push of PNR data not related to a flight that operates to, from or through Australia, we would reject the message and associated data.

b) Article 3 – scope of application

Article 3(2):

Q1: Have there been any difficulties in applying the definition of terrorist offences?

No. Article 3 clearly outlines the definition of terrorist offences, and the application of this definition to processing PNR data in the operational environment is straightforward.

Article 3(3):

Q2: At the time of the previous review, Australia identified difficulties in the application of the definition of "transnational" in relation to serious crimes. Whilst this did not impact the ability to apply the definition, which steps has Australia taken to overcome this difficulty and improve the process?

Applying the "transnational" definition continues, at times, to present a challenge. As such, the Department assesses each request on a case-by-case basis and the circumstances surrounding the case, to establish if there are appropriate transnational aspects to the request. This ensures that a consistent and appropriate definition of "transnational" is applied, and any request that is actioned has a clear "transnational" aspect. Should a request be complex in nature, where the application of the "transnational" definition is not clear, legal advice is requested.

Q3: Have there been any difficulties identified in applying the definition of serious transnational crime?

Although the definition of "transnational" requires more robust assessment to ensure it is appropriately applied, the definition of "serious crime" and the application of this definition is straightforward.

Article 3(4):

Q4: In how many cases did Australia process PNR data obtained under the Agreement for the protection of the vital interests of an individual, such as risk of death, serious injury or threat to health?

The Department has not processed PNR data solely for the purpose of the risk of death or serious injury to an individual. The Department utilised PNR data in the Ebola outbreak of 2014/15. It formed part of the enhanced traveller view to identify travellers who were

travelling from high risk areas declared by the World Health Organisation. Travellers who arrived into Australia from Ebola-affected source countries were sent for a health assessment at the airport. The profile created to identify these travellers matched 2464 travellers between 9AUG2014 and 8JAN2016, and 1434 of those were referred at the airport for health assessment.

Q5: What are specific examples of such cases?

See Q4.

Article 3(5):

Q6: In how many cases did Australia process PNR data obtained under the Agreement for the purpose of supervision and accountability of public administration and the facilitation of redress and sanctions for the misuse of data?

Nil cases.

Q7: What are specific examples of such cases?

N/A.

c) Article 4 – ensuring provision of PNR data

Article 4(2):

Q1: Has the Australian Competent Authority required air carriers to provide PNR data which are not held in their reservations systems or already collected?

No.

Article 4(3):

Q2: Have you identified any problems with the mechanism to filter out and delete PNR data received beyond those listed in Annex 1 of the Agreement?

There has been no change to the way the Department receives PNR data, and no associated problems or issues. There are two data formats received by the Department, as outlined below:

a) SBRRES/PRL EDI format PNR data from a service provider is received via a secure channel that provides a direct link between the airline service provider and the Department. EDI Messages from the service provider are received via the Department's Gateway and

Customs Connect Facility (CCF). PNR data beyond those listed Annex 1 of the Agreement is removed within the CCF prior to the PNR data being loaded into the PNR Data Store.

b) PNRGOV format PNR data is also received via the Department's Gateway and CCF. The PNR Collect and Store capability transforms the message from EDI to PNR-centric output XML, which only includes data listed in Annex 1 of the Agreement. The output XML will then be made available for subsequent store in the PNR Data Store.

For both formats, data beyond the elements listed in Annex 1 of the Agreement is removed and deleted prior to being loaded in the PNR Data Store.

Q3: Has this mechanism been audited and if so, which conclusions have been drawn?

For both SBRRES/PRL EDI and PNRGOV format, data outside the elements listed in Annex 1 of the Agreement is removed and deleted prior to being loaded into the PNR Data Store.

The process to ensure that only the data elements listed in Annex 1 of the Agreement are stored has been subjected to internal testing as part of the quality assurance associated with the implementation of the PNR System. This testing successfully demonstrated that only the data elements listed in Annex 1 of the Agreement are stored. The team responsible for the quality assurance of the PNR system are independent of the design and build of the system.

Q4: Has the Australian Competent Authority ever used information held in PNR obtained under the Agreement beyond those listed in Annex 1 of the Agreement, including sensitive information?

No. The Department is not aware of any additional PNR data elements received or used. The data elements provided within the PNR message are based on the agreed 19 elements from the Agreement and also specified within the International Civil Aviation Organization (ICAO) Document 9944 Guidelines on Passenger Name Record.

Q5: If so, how many times and for what reasons?

N/A.

e) Article 6 – police and judicial cooperation

Article 6(1):

Q1: How do you determine whether analytical information obtained from PNR data is "relevant and appropriate" to be made available to the police or judicial authorities of the

EU Member States, Europol or Eurojust?

Each request for analytical information is assessed on a case-by-case basis, to ensure it is relevant and appropriate. The purpose for the request is examined and must satisfy Australian Government information sharing legislation, as well as the provisions within the PNR Agreement. This ensures that the request meets both the conditions set out in the Agreement, as well as Australia's information sharing legislation and policy requirements.

Q2: How have your procedures improved in automating the process for identifying and sharing such information?

The Department's focus has been on improving our analytical capability. This includes improved systems to automate advanced analytic activity, like behavioural modelling. There is no automated process for identifying and sharing of analytical information. Any provision of PNR data outside of the Department is manually assessed on a case-by-case basis to ensure that it meets the relevant requirements.

Q3: In how many cases did the Australian Competent Authority provide analytical information obtained from PNR data to police or judicial authorities of EU Member States, Europol or Eurojust?

Nil cases.

Q4: What are specific examples of such cases?

N/A.

Q5: What criteria does the Australian Competent Authority apply to define 'as soon as practicable' in order to provide analytical information obtained from PNR data?

Any request for PNR data, including any analytical information, would be processed within the standard times for processing a Request for Information. Each request is assessed on a case-by-case basis and, depending on the complexity of the request, may be serviced within a day or a longer period with a time agreed to between the parties—depending on the priority and urgency of the request.

Q6: Does the Australian Competent Authority use additional information exchange channels to provide analytical information obtained from PNR data to police or judicial authorities of EU Member States, Europol or Eurojust?

In terms of potential additional information exchange channels, 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.

Article 6(2):

Q7: How many requests has the Australian Competent Authority received from police or judicial authorities of EU Member States, Europol or Eurojust for access to PNR data or analytical information obtained from PNR data received under the Agreement?

Since the last Joint Review, the Department has received five (5) requests from police or judicial authorities of EU Member States, Europol or Eurojust for PNR data, through the Request for Information (RFI) process.

Q8: In how many cases did the Australian Competent Authority made such information available?

The Department has made two (2) disclosures.

Q9: What are specific examples of such cases?

Both disclosures occurred in April 2015. PNR data was accessed and disclosed via the AFP (Interpol) to Europol.

Both requests were received via Interpol, on behalf of the United Kingdom. Europol was attempting to monitor a Scottish resident, who the United Kingdom suspected was currently in Australia. The person of interest was under a covert investigation for suspected lead involvement in the trafficking of liquid cocaine.

II. Safeguards applicable to the processing of PNR data

a) Article 7 – data protection and non-discrimination

Article 7(2):

Q1: As mentioned in the previous review, do you continue to apply the same data protection safeguards to the processing of all PNR data received under the Agreement, irrespective of

the data subject's nationality, country of residence or physical presence in Australia?

Yes. The safeguards are not based on the content of the data, but on PNR data as a whole.

b) Article 8 – sensitive data

Q1: How does the Australian Competent Authority filter out and delete sensitive data from PNR obtained under the Agreement?

The current requirement to manage PNR data in both SBRRES/PRL and PNRGOV formats requires data to be loaded into the PNR Data Store within the Electronic Data Warehouse (EDW) prior to being filtered. The SBRRES/PRL and PNRGOV format does not readily allow for the identification of sensitive data prior to it being received by the Department; therefore, sensitive data cannot be filtered out until after the PNR data is received.

In order to filter out and delete any sensitive data that may be contained in PNR data, the Department:

- applies filters over Salutation and Special Service Requests (SSR) (i.e. meal types and special passenger requirements).
- ensures that there is no automated processing over fields that may contain sensitive data (i.e. no profiling or watchlist processing is applied to fields that may contain sensitive data).
- maintains a combination of manual and automated controls to prevent processing over fields that may contain sensitive data.
- undertakes a manual review prior to disclosing relevant PNR data elements to external agencies to ensure that the information to be disclosed does not contain any sensitive data.

These controls are further outlined in the Department's PNR Control Framework.

Q2: Has the Australian Competent Authority ever used sensitive data held in PNR obtained under the Agreement?

No.

Q3: Have you managed to further improve the automatic identification of sensitive data contained within PNR received under the Agreement?

The Department continues with the same process in relation to sensitive data, which has

proven to be an effective control.

c) Article 9 - data security and integrity

Q1: Have there been any changes to the technical and organisational measures implemented to protect personal data and personal information contained in PNR?

The Department has implemented some further key controls:

- Full disk encryption, encrypting data on the hardware and the operating system, including data at rest.
- No automated disclosures of PNR data, and ensuring that other agencies do not receive feeds of PNR data.
- Intelligence reports or other intelligence products are distributed using email, with dissemination limiting markers where appropriate. Reports and products can also be sent over a security-classified network for documents classified as Secret or above, or distributed by hand.
- All staff must complete privacy induction training when they commence employment.
- Authorised officers who handle PNR data must complete a PNR training module (online or eLearning) before they are granted access to PNR data.

Article 9(1):

Q2: Have there been any changes to the measures in place to prevent accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any unlawful forms of processing?

On 12 March 2014, a new set of Australian Privacy Principles (APPs) and amendments to the *Privacy Act 1988* (Cth) came into force. The new APPs replaced the National Privacy Principles and Information Privacy Principles. The Department has an obligation under APP 11 of the *Privacy Act 1988* to take reasonable steps to protect the information it holds from misuse, interference and loss; and from unauthorised access, modification or disclosure.

In 2017, changes to the *Privacy Amendment (Notifiable Data Breaches) Act 2017* came into force. The Department implemented procedures with respect to the reporting of suspected privacy breaches.

Suspected privacy breaches are reported to the Department's Privacy section, who are

responsible for providing policy advice about the Privacy Act. The procedure supports prompt reporting of a suspected breach to ensure that appropriate containment measures are taken and that the Department reports eligible data breaches to the Office of the Australian Information Commissioner (OAIC), and the individuals whose personal information was affected by the breach.

There have been no changes from a technical perspective.

Article 9(1)(d):

Q3: How often is the access to PNR data audited?

There is an on-going quality assurance framework, which is managed by the Department and includes specific measures to ensure the on-going application of the safeguards required in the Agreement, including PNR System user access monitoring and review.

Regular reviews are undertaken, on average every six months, which compare PNR users' access to those staff approved to access PNR data under delegation from the Comptroller-General of Customs, under s64AF of the Customs Act.

Article 9(2):

Q4: Has there been any breach of data security?

In 2015, the Department notified the European Commission of a breach against the provisions of the PNR Agreement, which occurred in 2014.

There have been no other privacy breaches of PNR data through a breach of data security or other reported breaches of data security.

Article 9(3):

Q5: if yes, have the Australian Competent Authority taken any measures to prevent any data breaches to occur in the future?

The Department applies a layered approach to data security. Measures are applied at the technical, capability, governance and operational levels. The measures listed at Article 9 Q1 have been implemented to prevent any future data breaches.

The Department constantly strengthens its data protection measures, maintains training and awareness sessions to officers, and endorses relevant policy documentation.

Q6: Has the Australian Competent Authority reported any breach of data security to the Office of the Australian Information Commissioner?

The breach mentioned at Q4 above, was initially reported to the OAIC.

There have been no further data security breaches of PNR data.

d) Article 10 – oversight and accountability

Article 10(2):

Q1: How many audits of the Australian Competent Authority's processing of PNR data have been conducted by the Australian Information Commissioner since the last review? What was the outcome of these audits?

The Department's records show that PNR audits have been conducted by the OAIC since 2009, under a Memorandum of Understanding between the Department and the OAIC. There have been five (5) PNR audits since January 2014.

The PNR audit reports and recommendations can be found on the OAIC's website:

https://www.oaic.gov.au/privacy/privacy-assessments/

Article 10(3):

Q2: How many complaints related to the Agreement have been lodged with the Australian Information Commissioner?

Nil complaints.

Q3: What were the issues raised and what was the outcome of the investigation of these complaints?

N/A.

Q4: What was the average response time by the Australian Information Commissioner to such complaints?

N/A.

Article 10(4):

Q5: How many complaints related to the Agreement have been lodged with the Commonwealth Ombudsman?

Nil complaints. Between January 2014 and July 2019, the Commonwealth Ombudsman has had no approaches recorded regarding the agreement.

Q6: What were the issues raised and what was the outcome of the investigation of these complaints?

N/A.

Q7: What was the average response time by the Commonwealth Ombudsman to such complaints?

N/A.

d) Article 11 – transparency

Article 11(1):

Q1: Have there been additional measures implemented together with airlines to provide passengers with clear and meaningful information in relation to the collection, processing and purpose of the use of PNR data?

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.

Advice to passengers from air carriers falls outside the legislative remit of the Department, and therefore, this has not been asked of airlines when requesting them to supply PNR data.

However, the Department notes that passengers are advised on their air tickets and on the airline operator website that PNR data may be used by destination countries for customs, immigration and security purposes.

Q2: How do you ensure that airlines provide passengers with clear and meaningful information in relation to the collection, processing and purpose of the use of PNR data?

See Q1 above.

Article 11(2):

Q3: what measures does the Australian Competent Authority implement to provide the public with information on the purpose of collection and use of PNR data?

The Department of Home Affairs (including the ABF) website provides information on the

purposes for which the Department collects and uses of 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 at the following link:.

https://immi.homeaffairs.gov.au/form-listing/forms/1442i.pdf

Q4: Has the way in which Australia provides the public with information on how to request access, correction and redress under the Agreement changed?

No.

d) Article 12 – right of access

Article 12(1):

Q1: How many requests from individuals for access to PNR data have been received by the Australian Competent Authority?

Under Australian Privacy Principle (APP) 12, the Department has an obligation to give an individual access to personal information held about them. If there is a specific exemption, then an individual may submit a Freedom of Information (FOI) request under the *Freedom of Information Act 1982*. A FOI request is processed through the Department's FOI section and the scope of the request is clarified with the individual before processing the request.

The Department has not received any requests under APP 12 from individuals seeking access to the PNR data that the Department holds about them.

The Department has received twelve (12) requests for access to information under the *Freedom of Information Act 1982* where the scope has included PNR data.

Q2: How many times has PNR data been disclosed to individuals upon request?

Twelve (12) times, related to the twelve instances mentioned in Q1 above.

Q3: How many requests did the Australian Competent Authority receive for access to

documents held by the Australian Competent Authority as to whether or not data relating to the requesting individual were transferred or made available and information on the recipients or categories of recipients to whom the data were disclosed?

There have been twelve (12) requests through the Freedom of Information process for access to PNR data, as noted in Q1 and Q2 above.

Q4: How many times have such documents been disclosed to individuals upon request?

PNR data was made available for all twelve (12) request.

Q5: What was the average response time to such requests for access?

The *Freedom of Information Act 1982* states that the Department must provide an FOI request applicant with a decision on access to the documents requested within 30 days of receipt of their request.

Q6: Has PNR data been disclosed to any other persons other than the requesting individual? If so how many times?

No.

Article 12(2):

Q7: In how many cases was the disclosure of information limited and for what reasons?

Nil cases.

Article 12(3):

Q8: How many refusals or restrictions of access have been set out in writing and provided to requesting individuals?

Nil cases.

Q9: What was the average response time by the Australian Competent Authority?

N/A.

Q10: How many times have individuals lodged a complaint with the Australian Information Commissioner against a decision of the Australian Competent Authority to refuse or restrict access to information?

Nil times.

Article 12(4):

Q11: If individuals lodged such complaints with the Australian Information Commissioner, what was the outcome of the investigation of these complaints?

N/A.

e) Article 13 – right of rectification and erasure

Article 13(1):

Q1: How many requests did the Australian Competent Authority receive from individuals seeking the rectification of their PNR data?

Nil requests.

Article 13(3):

Q2: In how many cases did requests for rectification result in the rectification of PNR data?

Individuals have a right to request correction of their own personal information under Australian Privacy Principle (APP) 13, contained in Schedule 1 of the *Privacy Act 1988* and section 48 of *the Freedom of Information Act 1982*.

The Department has not received any requests under APP 13 seeking correction of personal information.

Q3: In how many cases did requests for rectification result in the erasure of PNR data?

N/A.

Q4: What was the average response time by the Australian Competent Authority to requests for rectification?

N/A.

Article 13(4):

Q5: How many times have individuals lodged a complaint against a decision of the Australian Competent Authority related to a request for rectification?

Nil times.

Q6: If individuals lodged such complaints with the Australian Information Commissioner, what was the outcome of the investigation of these complaints?

N/A.

f) Article 14 – right of redress

Article 14(1):

Q1: How many times have individuals sought administrative redress in cases related to the rights referred to in the Agreement?

Nil times.

Q2: How many times have individuals sought judicial redress in cases related to the rights referred to in the Agreement?

Nil times.

Q3: What was the outcome of these procedures?

N/A.

Article 14(2):

Q4: How many times have individuals applied for remedies in cases related to the processing of PNR data under the Agreement or the rights referred to in the Agreement?

Nil times.

Article 14(3):

Q5: Is the Australian Competent Authority undertaking any additional measures than the ones reported during the prior review to ensure that the right to effective administrative and judicial redress and the right to apply for effective remedies are afforded to all individuals without discrimination?

The Department is committed to maintaining the privacy of all personal information it collects and ensures it is accurate, up to date and complete. The Department notes its commitment to privacy obligations on its website at the following link:

https://www.homeaffairs.gov.au/access-and-accountability/our-commitments/privacy

The Department is bound by legislative provisions under the *Privacy Act 1988* and the *Freedom of Information Act 1982* and internal policies, procedures and regular reviews.

g) Article 16 – retention of data

Article 16(1)(a):

Q1: How many officials of the Australian Competent Authority are authorised to access PNR data from the initial receipt to three years?

There are 259 officers who are authorised officers with access to PNR data.

Of that, 140 fall within the scope of Information Technology, who perform different roles in the maintenance of the PNR System and the development of new and improved capabilities or the replacement of existing capabilities.

Articles 16(1)(b):

Q2: As reported during the prior review, has the Australian Competent Authority designed and implemented that measures are in place to ensure the masking out after three years of all data elements which could serve to identify the passenger to whom the PNR data relate?

Yes, the Department implemented the measures to mask out data after three years. An automated process runs daily to identify those records that have reached three years since receipt. A summary of results are emailed to the PNR mailbox. These records are masked from view.

Q3: Have there been any additional difficulties related to the operational efficiency or cost effectiveness of these measures?

There has only been one time where this job did not successfully finish due to technical and system issues. However, in this case, the script (automated process) was re-run and this saw the process finish and successfully mask the data.

There have been no additional difficulties to those raised at the prior review.

Q4: Has the policy direction developed (as stated by the Australian Competent Authority during the prior review), been implemented, used and found efficient? In what ways?

Yes, the policy direction continues to remain in force. It provides clarity on where the data retention and depersonalisation requirements are to be applied. PNR data extracted from the PNR system may be stored in Departmental protected systems or provided to partner authorities. Any extracted PNR data kept in Departmental systems is treated with the same stringent data protection controls as other Departmental information and in accordance with the Privacy Act. Any PNR data disclosed to partner authorities includes a caveat that outlines the conditions for disclosure and is subject to the same controls and maintained in appropriate

protected systems or files.

PNR data, when added with other Departmental information, provides immense intelligence value in identifying persons of interest. To maintain the integrity of the analysis, it is essential that the PNR data remains with the key linking information.

The policy direction was implemented due to the operational and administrative overhead it would take to effectively manage and track disclosures. Once the PNR data has been disclosed, to actively monitor and identify the location of the PNR data and to apply the data retention and depersonalisation measures, would divert valuable human resources unnecessarily. This is where the efficiencies are found.

Q5: How many officials of the Australian Competent Authority are authorised to access depersonalised PNR data from three years after initial receipt to the end of the five and a half year period?

There are 259 officers who are authorised officers, by the Comptroller-General of Customs, which enables access to PNR data.

Of that, 140 fall within the scope of Information Technology, who perform different roles in the maintenance of the PNR System and the development of new and improved capabilities or the replacement of existing capabilities.

Q6: Has the Australian Competent authority undertaken any additional measures to ensure the masking out after three years of all data elements which could serve to identify the passenger to whom the PNR data relate?

No, as the current process successfully does this.

Q7. How many cases of re-personalisation of PNR records have there been?

The Department manages the retention of personalised data for investigation by manually 'flagging' the PNR data in the PNR System. There have been 144 cases were data has been flagged for 'under investigation'.

Q8: Do you have an update on the number of officials that will be / are specifically authorised to access the dormant database?

There are 140 authorised officers whom fall within the scope of Information Technology, who perform different roles in the maintenance of the different applications within the PNR

System, and the development of new and improved capabilities or the replacement of existing capabilities. These officers are only authorised to access the PNR database to perform their duties associated with these purposes.

Article 16(3):

Q9: What measures are in place to ensure that PNR data has been required for the purposes of a specific investigation, prosecution or enforcement is permanently deleted once is no longer needed?

The user/work area that marked the record in the system unmarks the record, then the nightly automated deletion process picks it up and it is deleted if it has been 5½ years since receipt.

Q10: How does the Australian Competent Authority ensure that the safeguards set out in the Agreement are afforded to the extracted PNR data?

There are various protocols in place, such as roles-based access controls, audit / event logging, restricting transmission of the data out of the PNR Data Store, etc.

For the deletion/depersonalisation process, if the confirmation email is not received or the nightly automated batch job is unsuccessful, an internal IT Service Request is submitted to investigate and rectify.

Departmental officers are bound by secrecy and disclosure provisions under Part 6 of the *Australian Border Force Act 2015* and the *Privacy Act 1988*. Information sharing of PNR data must meet these disclosure provisions in addition to the conditions of the PNR Agreement, and an appropriate caveat is applied to the extracted data.

Q11: In case of PNR data disclosed to other law enforcement bodies for the purposes of a specific investigation, prosecution or enforcement what measures are in place to ensure the deletion of PNR data after it is no longer needed?

The Department includes a specific caveat on the extraction when PNR data is disclosed to partner law enforcement agencies.

h) Article 17 – logging and documentation of PNR data

Article 17(1):

Q1: Which logging and documentation procedures are applied by the Australian Competent Authority for the purpose of verification of lawfulness of the data processing, self-monitoring

and ensuring appropriate data integrity and security of data processing?

The Department employs the following audit logging in relation to PNR data:

1. Audit logging of all users access
2. Audit logging at the PNR database level
3. Logging and record-keeping of all information disclosures to other government authorities

i) Article 18 – sharing of PNR data with other government authorities of Australia

Article 18(1)(a):

Q1: What measures are in place to ensure that the data is shared under this provision only with those government authorities listed in Annex 2 of the Agreement?

Mandatory online learning, which covers disclosure provisions, must be undertaken before an officer is authorised and provisioned access to PNR data. Secrecy and disclosure training sessions continue on a regular basis thereafter.

The Department works on a centralised operating model for officers who may access PNR through a Request for Information process and disclosure PNR data to partner agencies. This ensures that all requests are processed centrally, and a consistent and compliant approach is undertaken at all times.

Regular internal assurance activities are undertaken by internal business areas (that is internal audit or PNR Policy area), to measure the effectiveness of the training, gauge officer knowledge and identify any irregularities in disclosure processes.

Q2: What measures are in place, to guarantee that the receiving government authorities afford to PNR data the 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.

Article 18(1)(d):

Q3: How does the Australian Competent Authority ensure that only the minimum amount of data possible is shared?

In addition to the mandatory online training, which covers the provisions of the PNR Agreement, there are various policy documents that set out the matters that must be taken into consideration when determining whether to disclose PNR data elements, and the extent to which PNR data is shared.

The centralised operating model also supports compliance with the disclosure provisions, to ensure that only the minimum amount of data possible is shared commensurate with the request and requirements.

Article 18(3):

Q4: How does the Australian Competent Authority ensure that the data are shared only for the purposes stated in Article 3?

The same controls as outlined in Q1, Q2 and Q3 apply to the scope of the Agreement.

Q5: How does the Australian Competent Authority ensure that the safeguards in Article 18 of the Agreement are respected when transferring analytical information containing PNR data obtained under the Agreement?

The same safeguards as outlined in Q1, Q2 and Q3 apply to analytical information that contains PNR data obtained under the Agreement.

j) Article 19 – transfers to authorities of third countries

Article 19(1)(a):

Q1: How does the Australian Competent Authority determine whether the receiving third country authority has agreed to afford to the data transferred the same safeguards as set out

in the Agreement?

All requests for PNR data come through the Tactical Intelligence (centralised operating work area) for determination as to whether PNR data will be transferred to the 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.

In addition, the Department is obligated under the Privacy Act and Australian Privacy Principle 8 – Cross-border data flows. The Department must be satisfied that the third-party overseas recipient is subject to laws providing substantially similar protection as the APPs, unless certain exceptions apply, including obtaining the individual's consent to the transfer of information or if there is a serious threat to life, health or safety or to public health or safety. Under Australian Privacy Principle 8, if the Department discloses personal information to an overseas recipient, we are accountable for any acts or practices of the overseas recipient in relation to the information that would breach the Australian Privacy Principles.

Q2: Are the Australian authorities aware of any instances, in which the requesting third country did not apply the relevant safeguards?

No.

Article 19(1)(e):

Q3: How does the Australian Competent Authority ensure that only the minimum amount of data possible is shared?

The same controls are in place for the access, use and disclosure to third countries as for domestic authorities.

This includes mandatory training and policy documentation, which set out the matters that must be taken into consideration when determining whether to disclose PNR data elements and the extent to which PNR data elements can be shared. Appropriateness and proportionally

is always included in each case-by-case assessment of any requests.

Article 19(1)(b):

Q4: How does the Australian Competent Authority ensures that the third country's authority is directly related to the prevention, detection, investigation and prosecution of terrorist offences and/or serious transnational crime?

As outlined in Q1, a Memorandum of Understanding needs to be in place before the exchange of PNR data can take place. The Memorandum of Understanding would outline the scope of the authority's remit. PNR data would not be provided if the Memorandum of Understanding, or the any specific request, did not directly relate to the prevention, detection, investigation and prosecution of terrorist offences and/or serious transnational crime.

Article 19(1)(f):

Q5: Please describe the reporting mechanism put in place to ensure that when PNR data of a national or resident of a Member State is shared with a third country that the competent authorities of that Member State are informed at the earliest opportunity.

The disclosure of information to a Member State would follow the Departmental information disclosure procedures as outlined in the relevant information disclosure policy documentation.

Q6 How many times has the Australian Competent Authority informed the competent authorities of a Member States of the fact that data of a national or a resident of that Member State was transferred to a third country?

Nil times.

Q7: Have the competent authorities of a Member State reacted to this sharing of information?

N/A.

Article 19(1)(h):

Q8: How does the Australian Competent Authority determine whether the receiving third country authority has agreed not to further transfer PNR data?

International authorities provide a written 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 another party unless required to do so by law. The undertaking is a requirement before an agency can be approved for an ongoing authorisation. Ongoing authorisations

outline specific circumstances where specific classes of information can be released for a specific purpose.

All PNR data is disclosed in accordance with the Agreement and a caveat is provided outlining the conditions of which it is disclosed, including further transfer of data.

Article 19(2):

Q9: How does the Australian Competent Authority ensure that the safeguards in Article 19 of the Agreement are respected when transferring analytical information containing PNR data obtained under the Agreement?

The same safeguards at Q8 would apply to analytical information shared to third countries.

III. Modalities of transfers

a) Article 20 – the method of transfer

Q1: How does Australia continue to ensure that air carriers transfer PNR data to the Australian Competent Authority exclusively on the basis of the push method?

All carriers 'push 'data to the Department. The Department has transitioned exclusively to receive PNR via the push method. No pull capability is available.

Q2: Does Australia receive or have access to any PNR data other than using the push method from airlines?

No.

Article 20(a):

Q3: Have there been cases of technical failure in the transfer of PNR data and if so, of what kind?

Yes, there have been unplanned system outages due to technical issues. There have also been data validation failures affecting individual messages or records, where PNR data is received but not stored.

Q4: How were PNR data transferred in such cases of technical failure?

There is currently no alternative transfer process. Once the outage was rectified, the PNR data transfer was resumed with no loss of data.

b) Article 21 – the frequency of transfer

Article 21(1):

Q1: How many times per flight, do air carriers have to transfer PNR data to the Australian Competent Authority?

There is a requirement for air carriers to provide up to five (5) scheduled transfers of PNR data, starting at 72 hours prior to scheduled departure time. Subsequent transfers are at 24 hours prior, two (2) hours prior, one (1) hour prior and at the time of departure.

Other than the first and last push, if no changes are made to the relevant PNR data, then a push is not required.

Article 21(2):

Q2: Have there been cases in which the Australian Competent Authority required an air carrier to provide PNR data prior to the first scheduled transfer?

No.

Q3: What are specific examples of such cases?

N/A.

Article 21(3):

Q4: Have there been cases in which the Australian Competent Authority required an air carrier to provide PNR data in between or after regular transfers?

No.

Q5: What are specific examples of such cases?

N/A.

ANNEX B

Composition of the review 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)