EUROPEAN
COMMISSION

Brussels, 10.7.2014
SWD(2014) 236 final

Joint Review Report 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

Accompanying

the 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) 458 final}

TABLE OF CONTENTS

1. BACKGROUND AND PROCEDURAL ASPECTS OF THE JOINT REVIEW

Australian legislation empowers the Australian Customs and Border Protection Service (ACBPS) to require 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 requirements of the Australian authorities are based on section 64AF of the Customs Act 1901 of the Commonwealth (Cth), the Customs Administration Act (1985 (Cth), the Migration Act 1958 (Cth), the Crimes Act 1914 (Cth), the Privacy Act 1988 (Cth) and the Freedom of Information Act 1982 (Cth).

Obtaining PNR data electronically in advance of a flight's arrival significantly enhances the ability of ACBPS, through its Passenger Analysis Unit (PAU), to conduct efficient and effective advanced risk assessment of passengers and to facilitate bona fide travel, thereby enhancing the security of Australia. In the financial year 2012/2013, a total number of 19.779.882 passengers and crew members arrived in Australia by air travel. ACBPS is responsible for undertaking risk assessment and clearance of all passengers arriving to and departing from Australia. Under mandate from the Australian Government, ACBPS functions extend to the prevention and detection of terrorism as well as other serious crimes that are transnational in nature.

In order to enhance and encourage cooperation to effectively prevent and combat terrorism and serious transnational crime, while fully respecting fundamental rights and freedoms, in particular privacy and the protection of personal data, the European Union and Australia concluded an Agreement on the processing and transfer of PNR data by air carriers to the ACBPS (herein after "the Agreement").[1] The Agreement entered into force on 1 June 2012.

According to Article 24(2) of the 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. In line with this requirement, the first joint review of the Agreement was carried out in Canberra on 29/30 August 2013. Under the terms of Article 24(3) of the Agreement, the EU would be represented by the European Commission, and Australia would be represented by ACBPS. The EU Commissioner for Home Affairs delegated this task to Reinhard Priebe, Director for Internal Security in DG Home Affairs, while the ACBPS Chief Executive Officer Michael Pezzullo delegated this task to Roman Quaedvlieg, ACBPS Deputy Chief Executive Officer for Border Enforcement. Both officials nominated teams to assist them in their tasks. A full list of the members of both teams appears in Annex B. It is noted that the EU team included one expert to assist it in its tasks, namely a data protection expert.

The following methodology was applied in the joint review exercise:

- The EU team was composed of three Commission officials, two representatives of the EU Delegation in Canberra and one data protection expert from a national data protection authority.
- The Commission sent out a questionnaire to ACBPS in advance of the joint review. This questionnaire contained specific questions in relation to the implementation of the Agreement by ACBPS. ACBPS provided written replies to the questionnaire prior to the joint review (see Annex A).
- The EU team was granted access to ACBPS premises and carried out a side visit to the ACBPS Passenger Analysis Unit.

[1] OJ L 186, 14.7.2012, p. 4–16.

- The EU team was given the opportunity to watch the databases being operated in real time with the results shown and explained on screen by senior analysts.
- The EU team had the opportunity to have direct exchanges with ACBPS 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 ACBPS. The EU team also had the opportunity and the time to raise further questions with ACBPS officials and address all the various parameters of the Agreement.
- The EU team had detailed discussions with representatives of the Office of the Australian Information Commissioner, namely the Australian Privacy Commissioner and the Assistant Commissioner.
- Prior to the joint review, ACBPS provided the EU team with detailed documentation on the processing of PNR data by ACBPS, including a PNR control framework setting out a complete inventory of automated systems and manual controls for the processing of PNR data, other internal operational documents, a PNR privacy impact assessment, and recent audit reports by the Office of the Australian Privacy Commissioner. Upon request by the EU team, further documentation was made available during and after the joint review, including all remaining reports of formal audits conducted by the Office of the Australian Information Commissioner on PNR data processing by ACBPS and an internal operational document setting out the depersonalisation of PNR data under Article 16(2) of the Agreement.
- At the request of ACBPS, all members of the EU team signed a copy of a non-disclosure agreement as a condition for their participation in this review exercise.
- ACBPS had the opportunity to ask questions to the EU team about the status of the Commission proposal for an EU PNR Directive.[2]
- For the preparation of this report, the EU team used information contained in the written replies that ACBPS provided to the EU questionnaire, information obtained from its discussions with ACBPS, other Australian personnel and at the side visit, information contained in the aforementioned documentation received before, during and after the joint review, as well as information contained in other publicly available ACBPS documents.

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 Restricted. The present report should be read in the light of these limitations, as well as in the light of the fact that all members of the EU team had to sign non-disclosure agreements exposing them to criminal and/or civil sanctions for breaches.

It has to be noted that the joint review is not an inspection of the processing of PNR data by ACBPS and that the EU team had no investigative powers.

In spite of such limitations, before, during and after the review there has been an exchange of views with a remarkable openness and in a very constructive spirit, covering all the questions of the EU team. Therefore, the EU team would like to acknowledge the excellent cooperation on the part of all ACBPS and other Australian personnel and express its gratitude for the way in which the questions of the EU team have been replied to.

[2] COM(2011) 32 final.

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

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

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

2. THE OUTCOME OF THE JOINT REVIEW

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

Notwithstanding Article 24(4) on a joint evaluation of the Agreement four years after its entry into force, a preliminary assessment of the question of whether PNR serves the purpose of supporting the fight against terrorism and other serious crimes that are transnational in nature showed that the processing of PNR data provided ACBPS with the possibility of carrying out effective pre-departure risk assessments of all passengers up to 72 hours before departure. ACBPS processes PNR data to assess passenger information against targeting rules that can include several risk indicators. In case the assessment with risk indicators points to a potential high-risk traveller, PNR data is further processed by an analyst in conjunction with other law enforcement information to determine whether a traveller poses a high risk, in order to assist in identifying those travellers that require an intervention upon arrival. The early identification of passengers who may pose a high risk enables ACBPS to prepare the necessary responses upon arrival and better target their interventions, while facilitating the travel of legitimate travellers due to minimal interventions. According to ACBPS, the analysis of PNR data in conjunction with other information plays a critical role in the ability of ACBPS to identify, ahead of arrival, high risk travellers in the context of combatting terrorism, drugs trafficking, identity fraud, trafficking in human beings and other serious transnational crimes. ACBPS provided examples of the use of PNR data in Australia that appear in Annex C. PNR data is also processed by ACBPS to build and refine risk indicators. Moreover, ACBPS analyses PNR data trends, and results from the processing of PNR data, to enhance risk assessment based on PNR and to minimise unnecessary interventions with passengers. Finally, the Passenger Analysis Unit also responds to requests for PNR data from other areas of ACBPS, from other Australian government agencies and from specific authorities from other countries (including EU Member States) in individual cases related to terrorism or serious transnational crime.

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

2.1. Main findings

2.1.1 Geographical scope (Article 2(d))

According to 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. This is the case for thirteen airlines that represent approximately 30% of the passenger movements into and out of Australia.

There are no non-stop flights between the EU and Australia, i.e. any air travel between the EU and Australia includes a stop-over in a third country. Due to the geographical distance between the EU and Australia, and the distinct feature of air travel that results from it, the scope of the Agreement is not defined by a reference to passenger flights between the EU and Australia. This approach is different as compared to PNR Agreements that refer to passenger flights between the EU and the respective contracting party. The PNR Agreement with Australia, instead, applies to all flights to, from or through Australia operated by airlines that process PNR data in the territory of an EU Member State. This includes the PNR data of passengers whose travel neither departs from nor arrives to the EU, as the Agreement also applies to flights between third countries and Australia that are operated by airlines that process PNR data in the territory of an EU Member State.

In accordance with this geographical scope, ACBPS explained that it applied the rules and safeguards laid down in the Agreement to all PNR data provided by airlines that operate air transportation to, from and through Australia and that process PNR data in the territory of an EU Member State.

ACBPS clarified that it only collected PNR data for flights operating to, from or through Australia, i.e. not for flights that depart from the territory of an EU Member State but do not have a stop-over or the final destination in Australia. This was confirmed by both the Association of European Airlines and the service provider Amadeus whose reservation system is used by the thirteen airlines.

As the scope of the Agreement is defined by the nexus of PNR data processing in the territory of an EU Member State, it does not cover all possible ways of air travel between the EU and Australia. If a passenger travels from the EU to Australia with a stop-over in a third country using an airlines that does not process PNR data in a reservation system located in the EU, the Agreement does not apply. However, ACBPS explained that based on an internal policy directive, the rules and safeguards contained in the Agreement are applied to all PNR data, irrespective of whether it was provided by an airline that processed PNR data in the EU or not. Consequently, the level of data protection guaranteed by the Agreement applies to all air travel between the EU and Australia. The only exception to this is the method of transfer (see below point 2.1.13.). While all air carriers covered by the Agreement transfer PNR data to ACBPS exclusively on the basis of the "push" method, ACBPS explained that some airlines that were not covered by the Agreement still used the "pull" method, i.e. ACBPS had direct access to the reservation system of these airlines. At the time of the joint review visit, ACBPS was actively working with airlines that were not covered by the Agreement to transit to the PNRGOV "push" method. Subsequent to the joint review, ACBPS informed the EU team that it had stopped receiving PNR data via the "pull" method in January 2014.

Conclusion: ACBPS applies the rules and safeguards of the Agreement to all flights that are covered by its scope. Due to the distinct feature of air travel between the EU and Australia (there are no non-stop flights), the Agreement does not cover all possible ways of air travel between the EU and Australia. Irrespective of that, ACBPS applies the rules and safeguards contained in the Agreement to all PNR data it received, and the level of data protection guaranteed by the Agreement therefore applies to all air travel between the EU and Australia.

2.1.2. Scope of application (Article 3)

Article 3 of the Agreement sets out the purpose limitation of the processing of PNR data under the Agreement. Regarding the use of PNR data, ACBPS explained that there had been no difficulties in applying the definition of terrorism as set out in Article 3(2) of the Agreement. Regarding the definition of serious transnational crime as set out in Article 3(3) of the Agreement, ACBPS explained that the application of the definition could at times be difficult when the transnational element of a serious crime was less common or obvious than in cases such as drugs trafficking or trafficking in human beings. ACBPS provided examples for such cases, including cases where an individual act of serious crime is part of a broader investigation of a number of connected serious offences with a transnational dimension. In such cases, ACBPS undertakes additional efforts to clarify the individual matter and to consider its circumstances in order to establish whether the transnational dimension as defined in the Agreement is given or not.

ACBPS assesses PNR data against risk indicators in a very targeted way that minimises the access to personal data. ACBPS currently applies defined targeting rules composed of several risk indicators to produce alerts that point to a potential high-risk traveller. ACBPS explained they defined their targeting rules in a narrow way to only get a low volume of matches that could adequately be followed-up. In these cases, PNR data is further processed by an analyst in the Passenger Analysis Unit in conjunction with other information to determine whether a traveller poses a high risk. If a person is determined to be a high risk-traveller, this information is forwarded to an ACBPS border official at the airport. It is the sole responsibility of the border official at the airport to decide whether and how to intervene upon the arrival of the high-risk traveller. The analysis provided by the ACBPS Passenger Analysis Unit only points to a potential risk. ACBPS provided the EU team with statistical information on the number of targeting rules it applied and the number of alerts produced per day by these rules. These figures illustrated the very targeted way in which ACBPS applies the risk assessment of PNR data. Due to the classified nature of the information provided, these figures cannot be made public.

In addition to risk assessment based on targeting rules, ACBPS checks PNR data against a dedicated watch list that is limited to the purposes of Article 3(2) and Article 3(3) of the Agreement and that focuses on counter-terrorism and national security matters. PNR data is not checked against the general customs watch list applied by ACBPS.

Co-located with the ACBPS Passenger Analysis Unit is the so-called Tactical Support Unit (TSU), a small team of targeting specialists from the Australian Department of Immigration and Border Protection (DIBP). The TSU officers act under the control of ACBPS and have appropriate authorisations under section 64AF(5) of the Customs Act to access and processes PNR data in compliance with the Agreement to detect cases of document fraud, which is a serious crime under Australian criminal law. In the financial year 2012/13, through a narrowly targeted risk assessment of PNR data, the TSU identified 80 travellers attempting improperly documented travel to Australia. This reflects again the the very targeted way in which ACBPS applies the risk assessment of PNR data.

In compliance with Article 18 of the Agreement on the sharing of PNR data with other government authorities of Australia, the Tactical Support Unit shares PNR data with the Australian Department of Immigration and Border Protection, in particular the Department's Airline Liaison Officers located at international airports that have direct flights to Australia. Airline Liaison Officers provide advice and assistance to airline staff in relation to confirming the travel documentation and identity of a passenger.

ACBPS explained that no PNR data had been processed for the protection of the vital interest of an individual, such as risk of death, serious injury or health. However, ACBPS argued that the possibility of processing PNR data for such purposes under Article 3(4) of the Agreement remained important, and referred to theoretical cases of urgency where the contact information provided in PNR data would need to be used. These fictitious examples included the case of a suspected pandemic health situation where ACBPS would need to notify travelling companions or fellow passengers.

ACBPS did not process any PNR data under Article 3(5) of the Agreement for the facilitation of redress or sanctions for misuse of data. ACBPS provided PNR data for supervision purposes to the Office of the Australian Information Commissioner in its role as an independent auditor and in line with its competences under Australian law to receive access to PNR data stored by ACBPS.

Conclusion: ACBPS uses PNR data in full compliance with the Agreement. The very targeted way in which ACBPS applies the risk assessment of PNR data usefully minimises the access to personal data.

2.1.3. Provision of PNR data (Article 4)

Article 4 of the Agreement regulates the provision of PNR data. ACBPS has mechanisms in place that electronically remove and delete data beyond the elements listed in Annex 1 of the Agreement prior to being loaded to the database of the PNR system, the so-called PNR data store. The process to ensure that only the data elements listed in Annex 1 of the Agreement are stored was subjected to internal testing by ACBPS as part of the quality assurance associated with the implementation of the PNR system.

ACBPS indicated that it had neither identified any PNR data elements that were no longer required, nor was it aware of any additional PNR data elements that were required for the purposes of the Agreement.

In response to questions raised by the EU team about the necessity of processing all PNR data types listed in the Annex to the Agreement, ACBPS provided a list demonstrating the operational value of all PNR data types listed in the Annex of the Agreement. Due to the classified nature of the information contained in this list, it cannot be made public.

Conclusion: In accordance with its commitments under the Agreement, ACBPS removes and deletes any PNR data elements that it receives which are outside the 19 data elements listed in the Annex to the Agreement.

2.1.4. Non-discrimination (Article 7)

According to Article 7 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, in particular on the basis of nationality or country of residence or physical presence in Australia. ACBPS 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. This is required by both the Agreement and Australia's robust privacy law, as the Australian Privacy Act applies equally to all persons whose PNR data is processed by ACBPS. In order to ensure equal treatment and non-discrimination in practice, ACBPS put in place a risk mitigation strategy in the form of a PNR control framework that documents the safeguards implemented by ACBPS in compliance with the Agreement and the Australian Privacy Act. Moreover, ACBPS performed a privacy impact assessment which considers the application of the data protection safeguards under the Agreement and the Australian Privacy Act. Both the PNR control

framework and the privacy impact assessment were made available to the EU team, and both documents attest that the safeguards applicable to the processing of PNR data under the Agreement indeed apply to all passengers without discrimination.

Conclusion: ACBPS fully complies with the obligation of non-discrimination.

2.1.5. Sensitive data (Article 8)

According to Article 8 of the Agreement, any processing by ACBPS of sensitive PNR data shall be prohibited. ACBPS confirmed that it had never used sensitive data held in PNR data obtained under the Agreement. ACBPS explained that there had been some difficulties in the filtering out and deletion of sensitive data from PNR obtained under the Agreement, as sensitive data could be contained in free-text fields (the general remarks field and historical changes to the general remarks field) in a way that they are difficult to be identified. Therefore, ACBPS applies a combination of several layers of automated and manual controls to identify and delete sensitive data. There is an automated filtering over Special Service Requests (SSR), such as meal types and wheel chair requirements, as part of the general remarks field (point 17 in Annex 1of the Agreement). ACBPS provided a list of SSR meal codes that are filtered out from PNR data. Likewise, salutations (such as 'Mr/Mrs') are automatically removed from the name field (point 4 in Annex 1 of the Agreement), based on a list of known salutations that have been selected based on observation of the data. In addition to these automated controls, authorised officers in the Passenger Analysis Unit undertake manual checks prior to disclosing relevant PNR data elements to ensure that no sensitive data is disclosed. Moreover, there is no risk assessment or watch list processing applied to data fields that may contain sensitive data.

ACBPS is actively seeking ways to further improve the automatic identification of sensitive data. ACBPS is developing and testing new technical solutions to detect sensitive data by way of key words checks in free-text fields. ACBPS is also engaged in attempts to further structure the message format of PNR data in order to reduce the amount of information to be put in free-text fields. ACBPS explained that its analysis revealed that there was very little sensitive data contained in PNR data.

ACBPS explained that for technical reasons, PNR data first had to be loaded into the PNR system before sensitive data could be identified and deleted. This is in compliance with the Agreement. ACBPS set out that it was not possible to identify and delete sensitive data before it was received by ACBPS.

ACBPS explained that it had no operational need to access sensitive data in PNR.

Conclusion: ACBPS fully complies with the obligation under the Agreement concerning sensitive data. Moreover, ACBPS is actively seeking to further improve the automated identification and deletion of sensitive data.

2.1.6. Data security (Article 9)

Article 9 of the Agreement sets out the requirements on data security. ACBPS reported that there were comprehensive electronic and physical security systems in place to protect PNR data and to ensure it was isolated from other data retained in the general ACBPS environment. ACBPS explained that the data security safeguards in the Agreement had been analysed and incorporated into each PNR system capability as it had been developed and implemented. The PNR system is supported by a PNR control framework that provides a complete inventory of the security safeguards and the automated and manual controls in place over PNR data. The PNR control framework was made available to the EU team, and it allowed the EU team to get an overview of the variety of data security measures in place in the PNR system.

The Passenger Analysis Unit is located in a secure area with restricted access, and a layered level of logins is required to access the information technology systems. In its reply to the EU questionnaire, ACBPS set out a number of key controls that had been implemented to comply with the Agreement. For instance, user access controls are in place requiring users to seek approval from the ACBPS Chief Executive Officer. Every access to PNR data is logged (user, work location of the use, date and time of access, content of the query, number of records returned). The audit record provides the ability to generate reports of users who have accessed the system, allowing internal and external audits of the access to the PNR system. Specific systems based audits are performed, e.g. quarterly user access reviews. This includes audits conducted by a team with a governance role, and audits performed by divisions of ACBPS that are independent of the Passenger Analysis Unit, such as the ACBPS Security, Risk and Assurance Division. In addition, the Office of the Australian Information Commissioner conducts independent audits of ACBPS management, use and disclosure of PNR data against compliance with Australian privacy laws and the Agreement (see point 2.1.7.).

ACBPS reported that there had been no breaches of data security. Therefore, although there are mechanisms in place to report any breach of data security to the Office of the Australian Privacy Commissioner, no such breach has been reported.

Conclusion: ACBPS complies with its data security obligations under the Agreement.

2.1.7. Oversight and accountability (Article 10)

According to Article 10 of the Agreement, compliance with data protection rules by the Australian government authorities processing PNR data shall be subject to the oversight by the Australian Information Commissioner. During the joint review, meetings with representatives of the Office of the Australian Information Commissioner – the Australian Privacy Commissioner and the Assistant Commissioner – as well as documentation made available to the EU team indicate a high level of independent oversight of the processing of PNR data under the Agreement. Representatives of the Office of the Australian Information Commissioner also provided the EU team with a general overview of Australia's robust privacy law, including a reform of the Australian Privacy Act adopted in 2012 that will further strengthen the role of the Australian Information Commissioner by March 2014.

As required under Article 10(2) of the Agreement, ACBPS has arrangements in place under the Privacy Act for the Australian Information Commissioner to undertake regular formal audits of all aspects of PNR data processing by ACBPS under the Agreement. ACBPS and the Office of the Australian Information Commissioner have a Memorandum of Understanding in place setting out that the Office of the Australian Information Commissioner will conduct one audit per year related to the processing of PNR data by ACBPS under the Agreement, and provide advice with respect to privacy impact assessments or other policy advice.

At the point of the joint review, the Office of the Australian Information Commissioner had undertaken one formal audit since the entry into force of the Agreement (undertaken in October/November 2012, with a final report issued in June 2013). This report was made available to the EU team, as was the case with the reports of five formal audits previously undertaken by the Office of the Australian Information Commissioner on the processing of PNR data by ACBPS under the 2008 EU-Australia PNR Agreement.[3] 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 ACBPS had processed PNR data. Subsequent to the joint review, ACBPS informed the EU team that the Office of the

[3] OJ L 213, 8.8.2008, p. 47–57.

Australian Information Commissioner had notified ACBPS of another intended audit, with a final report expected in 2014.

The Office of the Australian Information Commissioner had also provided advice during the drafting of the privacy impact assessment on the processing of PNR data under the Agreement that was made available to the EU team. The document provides for a thorough assessment by mapping out all information flows for the PNR system, potential privacy risks and issues requiring clarification, as well as mitigations to such potential privacy risks in order to increase privacy protection.

As regards the existing right of any individual – including persons not present in Australia – to lodge a claim with the Australian Information Commissioner concerning the protection of his or her rights and freedoms with regard to the processing of personal data, the Assistant Commissioner of the Office of the Australian Information Commissioner confirmed that there had been no claim lodged by any individual with the Australian Information Commissioner concerning the processing of PNR data.

As regards the rights of any individual – including persons not present in Australia – to lodge a complaint with the Commonwealth Ombudsman regarding his or her treatment by ACBPS, ACBPS explained that the Commonwealth Ombudsman had not referred any such complaints related to the Agreement.

In addition to independent external oversight, ACBPS has internal audit and oversight mechanisms in place for its PNR system. This includes quality assurance processes implemented by the ACBPS Strategy and Policy Section (e.g. review of the enforcement of instructions and guidelines for PNR and the PNR controls framework), systems monitoring by the ACBPS IT division, reviews of user access and audit logs, and further internal audits.

Conclusion: ACBPS fully complies with the obligations concerning oversight and accountability.

2.1.8. 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. In its reply to the questionnaire, ACBPS referred to the information on the collection, processing and purpose of the use of PNR data that was made available on the ACBPS website, on air tickets and on the website of airline operators. On its general website on privacy matters,[4] ACBPS provides a link to a detailed description of its collection of PNR data.[5] The description provides passengers with clear and meaningful information on the purpose of collection of PNR data, on the protection of PNR data, and on how to request access, correction or administrative redress. It includes contact details if the public want to submit a Freedom of Information (FOI) request, as well as links to the websites of the Office of the Australian Information Commissioner[6] and the Commonwealth Ombudsman[7] to seek redress.

ACBPS also works together with airlines to ensure that passengers are provided with information on the processing and use of PNR data. ACBPS provided some examples of how airlines informed passengers about the collection of PNR data and its use for security purposes. ACBPS has Memoranda of Understanding in place with airlines that include sections on transparency. Examples of such Memoranda of Understanding were shown to the

[4] http://www.customs.gov.au/privacy/default.asp.
[5] http://www.customs.gov.au/webdata/resources/files/PNRPrivacyStatement.doc.
[6] http://www.oaic.gov.au/.
[7] http://www.ombudsman.gov.au/.

EU team. This allowed the EU team to conclude that ACBPS had taken the necessary steps with airlines to ensure transparency for passengers.

Conclusion: ACBPS fully complies with the obligations to ensure transparency.

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

2.1.9.1. Right of access (Article 12)

According to Article 12 of the Agreement, any individual shall have the right to access his or her PNR data, following a request made to ACBPS. In its reply to the questionnaire, ACBPS explained it had not received any request or application for access to information where the scope included PNR data. ACBPS is subject to the Australian Freedom of Information Act that requires ACBPS to release documents to any person – including persons not present in Australia – that requests access to these documents, subject to the provisions in the Freedom of Information Act.

Any request for access to information made to ACBPS falls under the Freedom of Information Act (FOI) and is handled as a FOI request. All FOI requests at ACBPS are processed through the ACBPS Legal Services Branch. The scope of each request is clarified with the individual before processing the request in a case management system. In the financial year 2011/2012, ACBPS received a total number of 116 FOI requests, 20 of which were assigned to its Passenger branch. According to ACBPS, none of these requests related to PNR data. In the financial year 2012/2013, ACBPS received a total number of 146 FOI requests, 32 of which were assigned to its Passenger branch. According to ACBPS, none of these requests related to PNR data.

The privacy impact assessment made available to the EU team indicates that ACBPS has procedures in place to respond to FOI requests within 30 days.

The Assistant Commissioner of the Office of the Australian Information Commissioner confirmed that there had been no complaints lodged by individuals with the Australian Information Commissioner against a decision by ACBPS to refuse or restrict access to PNR data.

Conclusion: ACBPS fully complies with the obligation to provide the right of access.

2.1.9.2. Right of rectification and erasure (Article 13)

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 ACBPS where the data is inaccurate. In its reply to the questionnaire, ACBPS explained it had not received any request seeking the rectification of PNR data.

The privacy impact assessment made available to the EU team indicates that ACBPS has procedures in place to respond to a request for rectification within 30 days, to correct personal information free of charge, and to provide, in case of refusing a correction request, the individual with written reasons for the refusal and with information on the available complaint mechanism.

The Assistant Commissioner of the Office of the Australian Information Commissioner confirmed that there had been no complaints lodged by individuals with the Australian Information Commissioner against a decision by ACBPS to refuse rectification or erasure of PNR data.

ACBPS underlined the operational need to ensure the accuracy of the PNR data processed, and referred to problems that could be caused by inaccurate PNR data. According to ACBPS,

accuracy of the data is a pre-condition to get an increased level of certainty from the processing of PNR data about the relative risk travellers may represent, and to allow law enforcement to make timely and risk-based decisions about how to respond and how to deploy resources. Therefore, ACBPS has control mechanisms in place that mitigate the risk of receiving incomplete or inaccurate PNR data from airlines.

Conclusion: ACBPS fully complies with the obligation to provide the right of rectification and erasure.

2.1.9.3. Right of redress (Article 14)

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, ACBPS explained any person aggrieved by any administrative action or decision relating to the collection or disclosure of PNR data – including persons not present in Australia – has measures available to seek administrative or judicial redress without discrimination. ACBPS stated that no individual had sought administrative or judicial redress in cases related to the rights referred to in the Agreement.

Concerning administrative redress, the Australian Privacy Commissioner explained that on the basis of the Australian Privacy Act, any person – including persons not present in Australia – has access to the Australian Privacy Commissioner and his office to seek redress for any breach of legislative requirements. The Australian Privacy Commissioner confirmed that he had received no request 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 administration can submit a complaint to the Office of the Ombudsman to seek redress. This avenue of redress is also open for complaints to appeal against a decision taken by the Office of the Australian Information Commissioner in a complaints process.

Concerning judicial redress, the Australian Privacy Commissioner referred to the Australian Decisions (Judicial Review) Act that enables any individual – including persons not present in Australia – to apply to the Federal Court of Australia for an order of judicial redress by way of judicial review of administrative decisions taken by Australian Government authorities, including ACBPS.

Conclusion: ACBPS fully complies with the obligation to provide the right of redress.

2.1.10. Automated processing of PNR data (Article 15)

According to Article 15 of the Agreement, ACBPS shall not take any decision significantly affecting a passenger solely on the basis of the automated processing of PNR data. Documentation provided by ACBPS to the EU team sets out that ACBPS has processes in place to ensure that an analysis is performed by ACBPS staff before any decision is made on the basis of the result of the automated processing of PNR data.

Moreover, a side visit to the Australian Passenger Analysis Unit, including a demonstration of real time use of PNR data, and further discussions with analysts demonstrated that the processing of PNR data by ACBPS was a highly manual process with no automated interventions with passengers. The automatic processing of PNR data elements – i.e. the assessment of passenger information against risk indicators combined in targeting rules – draws out for further scrutiny the selected PNR data of potential high-risk traveller. This selected PNR data is manually processed by an analyst in conjunction with other information

to determine whether a passenger poses a high risk and requires an intervention upon arrival. If the analyst comes to the conclusion that a passenger poses a high risk, the analyst issues a recommendation to intervene in an electronic system called PACE (Passenger Analysis Clearance & Evaluation System). Any PACE alert originating in the Passenger Analysis Unit (so-called 'PAU alerts') needs to include a justification for both the assessment made and the recommendation to intervene. ACBPS underlined that it was at the discretion of the border official at the airport to decide whether or not to follow the PACE system recommendation and intervene with the passenger, e.g. by way of referral to a secondary inspection. The analysis provided by the ACBPS Passenger Analysis Unit only points to a potential risk. Consequently, there are at least two steps of human decision-making involved in an intervention by ACBPS based on the analysis of PNR data.

Conclusion: ACBPS fully complies with the obligation under the Agreement concerning the automated processing of PNR data.

2.1.11. 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. ACBPS retains PNR data obtained under the Agreement separate from other systems and data it collects and stores. In compliance with the Agreement, ACBPS 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 on a daily basis, counting from the date of initial receipt. PNR data pushes received for different segments of a passenger's journey (i.e. for outbound flight and possible connecting/return flight) are treated individually for deletion purposes.

ACBPS applies the data retention and depersonalisation requirements of Article 16 only to PNR data retained in the database of the PNR system, the so-called PNR data store. The data retention and depersonalisation requirements of Article 16 PNR are not applied to PNR data that was identified as relating to a person of interest and extracted from the PNR data store for the purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious transnational crime (see below point 2.2.1.).

Access to PNR data is limited to a restricted number of officials within ACBPS who are specifically authorised by the ACBPS Chief Executive Officer under Section 64AF of the Australian Customs Act. In the reply to the questionnaire, ACBPS stated that there were 132 ACBPS officials who held a delegation to access PNR data. This includes officers who have access to PNR data for undertaking risk assessment activity as well as officers who are responsible for systems development and maintenance activity.

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). ACBPS is currently developing and implementing the measures necessary to ensure the masking out after three years of all data elements which could serve to identify the passenger to whom PNR data relates. According to Article 27 of the Agreement, no data is required to be masked out before 1 January 2015. ACBPS appears to be well on track to meet this obligation. ACBPS provided the EU team with internal documentation setting out how ACBPS is addressing the depersonalisation requirements. ACBPS will mask out PNR data after three years from its initial receipt by preventing access to the PNR data elements listed in Article 16(2) of the Agreement. The documentation provided by ACBPS also includes a detailed list of database columns of the PNR records that will be masked out in order to prevent an individual being identified or re-identified. ACBPS explained that it would use masked data to enable longer term trend analysis, pattern recognition and risk profile development, consistent with the

purpose limitation of the Agreement. It is foreseen that a group of eight ACBPS officials – the so-called Advanced Analytics team – will be authorised by the ACBPS Chief Executive Officer to access masked data. Full access to masked data will require permission by a member of the Senior Executive Service of ACBPS, and will only be possible if necessary and only for a specific case of terrorism or serious transnational crime.

Conclusion: ACBPS retains and deletes PNR data in full compliance with the Agreement, except for PNR data used in a specific investigation (see below point 2.2.1.). ACBPS is preparing the technical requirements to be able to mask out PNR data by 1 January 2015 as required under the Agreement.

2.1.12. Domestic sharing and onward transfers (Articles 18-19)

2.1.12.1.Sharing with other government authorities of Australia (Article 18)

Article 18 of the Agreement regulates the onward transfer from ACBPS to other government authorities of Australia. ACBPS 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. This also applies to the sharing of PNR data between the Tactical Support Unit – as part of the Passenger Analysis Unit – and the Australian Department of Immigration and Border Protection. ACBPS can only share PNR data if the receiving government authority provides a written undertaking that it will use PNR data received by ACBPS only for the purposes for which it was shared, and that the information will not be passed on to a third party unless specifically required by Australian law in a specific case. ACBPS explained that it was not aware of any case where a government authority further transferred PNR data, or analytical information containing PNR data, to a third party outside Australia.

ACBPS explained that all disclosures of PNR data included a caveat governing the use, storage and further disclosure of PNR data disclosed by ACBPS. 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 Passenger Analysis Unit. ACBPS explained that in order to ensure that only the minimum amount of data possible was shared, instructions and guidelines at ACBPS set out the matters that are to be taken into consideration when determining whether and to what extent PNR data elements were to be disclosed in a specific case.

ACBPS maintains a log of incoming requests and shared information. In the financial year 2012/2013, the Passenger Analysis Unit responded to 1646 requests – received both from other areas of ACBPS and from other Australian government authorities – that were related to PNR data obtained under the Agreement. ACBPS explained that most requests for information concerned real-time PNR data, i.e. PNR data of a person that is about to arrive to or leave Australia. Historical data of past travels, instead, are hardly requested by other government authorities.

ACBPS explained that under Australian law, ACBPS could theoretically receive a subpoena referring to PNR data, in which case ACBPS would be legally obliged to provide the data. In practice, however, there has never been a subpoena that sought PNR data. The Agreement does not explicitly provide for the disclosure of PNR data in order to comply with a subpoena.

ACBPS informed the EU team that Australia would seek to request a modification of the list of authorities set forth in Annex 2 of the Agreement according to Article 18(2) of the Agreement.

Conclusion: The domestic sharing of PNR data with other government authorities of Australia takes place in compliance with the Agreement.

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

Article 19 of the Agreement regulates the onward transfer from ACBPS to authorities of third countries. ACBPS set out that it had not transferred any PNR data received under the Agreement to authorities of a third country. ACBPS explained that it instead exchanged risk profiles (e.g. certain travel patterns used by drugs traffickers) that were derived from the analysis of PNR data, from detections based on PNR data, and from other sources, but which did not contain any PNR data of a specific person. ACBPS explained that there was no need to disclose any PNR data of a specific person and their travel when sharing risk profiles with third countries as well as Member States (see also point 2.2.2. on police, law enforcement and judicial cooperation). The sharing of risk profiles takes place on the basis of Memoranda of Understanding and in compliance with Australia's robust data protection regime based on the Australian Privacy Act. The risk profiles, when adjusted to the geographical situation of the receiving country and its specific context, can feed into targeting rules used by the receiving country for risk assessment based on PNR data.

ACBPS explained that it has Memoranda of Understanding in place with third countries that in principle allows for the transfer of PNR data received under the Agreement in compliance with Article 19 of the Agreement. The safeguards used in the domestic transfer of PNR data, such as the caveats or the rules minimising the amount of PNR data to be shared, will also apply if ACBPS eventually shares PNR data or analytical information containing PNR data with a third country. ACBPS however stated that in such a case, the obligation under Article 19(1)(f) of the Agreement – i.e. to inform the competent authorities of a Member State in case PNR data of a national or resident of the latter had been transferred – could lead to operational difficulties. Australia does not have direct information exchange channels in place with each EU Member State. ACBPS is therefore considering ways to establish a reporting mechanism through Europol in order to be prepared to meet its obligations under Article 19(1)(f) if it eventually transfers PNR data to a third country. The obligation to inform the competent authorities of a Member State in case PNR data of a national or resident of the latter had been transferred is an important element of the Agreement, as reflected in the joint declaration annexed to the Agreement.

Conclusion: ACBPS is in full compliance with the obligations under Article 19 of the Agreement. Although allowed under strict conditions, ACBPS has not shared PNR data or analytical data containing PNR data with a third country. The Agreement does not set any limitations on the sharing of risk profiles that do not include any PNR data. ACBPS is requested to set up a reporting mechanism that will enable ACBPS to inform Member States according to Article 19(1)(f) if PNR data received under the Agreement, or analytical information containing such data, is eventually shared with a third country. ACBPS should be supported in setting up this reporting mechanism.

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

Articles 20 and 21 of the Agreement regulate the method and frequency of PNR data transfers. ACBPS explained 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. This was confirmed by the Association of European Airlines and the service provider Amadeus. This currently applies to 13 airlines, all of which use the service provider Amadeus. ACBPS receives PNR data from Amadeus via a secure VPN channel that provides a direct link between Amadeus and ACBPS. PNR data is currently pushed in the

Amadeus SBRRes message format. This is an Amadeus proprietary message and ACBPS is progressing the transition to the PNRGOV message during 2014 for Amadeus hosted airlines. The PNRGOV message is a standardized electronic message for the transmission of PNR data, developed by a working group of the International Air Transport Association (IATA) and endorsed jointly by the World Customs Organisation (WCO), the International Civil Aviation Organization (ICAO) and IATA. Australia is a forerunner in the development, implementation and improvement of the PNRGOV standard message, seeking to achieve global standardisation for the transmission of PNR data in its engagement with individual airlines and in the framework of WCO, ICAO and IATA.

In its reply to the EU questionnaire, ACBPS explained that in cases of technical failure, i.e. where the connection between Amadeus and ACBPS had been disrupted, there was no alternative data process. Once the disruption is rectified, the PNR data transfer resumes.

At the time of the joint review, airlines that did not have reservation systems or data processing in the territory of an EU Member State – and that were therefore not covered by the Agreement – provided PNR data via the "pull" method, i.e. ACBPS had direct access to the reservation system of these airlines. PNR data received by ACBPS via the "push" method was physically separated from pull data. At the time of the joint review, ACBPS was actively seeking to apply the "push" method for all airlines flying to Australia. ACBPS was actively working with airlines that were not covered by the Agreement to transit to the "push" method. Subsequent to the joint review, ACBPS informed the EU team that it had stopped receiving PNR data via the "pull" method in January 2014. Although outside the scope of the Agreement, it is welcomed that ACBPS applies the "push" method – as the more privacy-friendly transmission format compared to "pull" access – to all airlines.

ACBPS 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. This was confirmed by the Association of European Airlines and Amadeus. PNR data transmitted 24 hours, two hours and one hour before departure may contain only changes to previously transmitted data as agreed between the airline and ACBPS.

ACBPS explained that in four cases since July 2010, it had required an air carrier to provide PNR data prior to the first scheduled transfer according to Article 21(2) of the Agreement; in 50 cases, it had required an air carrier to transfer PNR data in between regular transfers. In all of these cases, these ad-hoc data transfers were requested in order to determine the exact whereabouts of known persons, in order to support the off-shore decision-making of Australian authorities tasked to provide a safe return for these persons from high-risk places. In all of these cases, the ad-hoc PNR data transfer took place via the "push" method, in the form of a manual process undertaken by Amadeus in the framework of a 24/7 support capability.

Conclusion: ACBPS fully complies with the Agreement and is to be commended for the way it applies and promotes the “push” method. It is welcomed that Australia extended the application of the “push” method to all airlines not covered by the Agreement.

2.2. Issues to be further addressed

Two issues need to be further addressed.

2.2.1. Retention of data – data used in a specific investigation (Article 16)

According to Article 16(3) of the Agreement, PNR data required for a specific investigation, prosecution or enforcement of penalties for terrorist offences or serious transnational crime

may be processed for the purpose of that investigation, prosecution or enforcement of penalties until the relevant investigation or prosecution is concluded or the penalty enforced. ACBPS explained that for a specific case of terrorism or serious transnational crime, PNR data identified as relating to a person of interest is extracted from the so-called PNR data store of the PNR system. This specific PNR data related to a person of interest is then analysed and combined with other information or intelligence in an investigation file and stored in the protected ACBPS National Intelligence System (NIS). Moreover, in line with Article 18 of the Agreement on the sharing of PNR data with other government authorities of Australia, PNR data may be extracted from the PNR data store and provided to other government authorities of Australia for a specific case of terrorism or serious transnational crime. The receiving authorities combine the extracted PNR data with other information or intelligence and store it in a record in their relevant law enforcement database.

ACBPS explained that in such cases, all obligations under the PNR Agreement are applied to extracted PNR data except for the data retention and depersonalisation requirements of Article 16 of the Agreement. Instead, the extracted PNR data becomes subject to the retention and deletion requirements applicable to the ACBPS National Intelligence System or to the law enforcement database of the receiving authority. The general retention period of the ACBPS National Intelligence System is ten years, while the general retention periods of relevant law enforcement databases of other government authorities of Australia vary. ACBPS explained that other government authorities of Australia that received extracted PNR data and stored it in their relevant law enforcement database were under a legal obligation to retain the data in accordance with the general retention requirements for that law enforcement database (e.g. to allow a defendant to appeal). The Australian Privacy Act, including provisions on access, correction and redress, also applies to extracted PNR data.

ACBPS underlined the impracticality of applying the data retention and depersonalisation requirements of Article 16 of the Agreement to investigation files or records stored in law enforcement databases that contained, amongst other information, elements of PNR data extracted from the PNR data store.

Recommendation: 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.

2.2.2. Police, law enforcement and judicial cooperation (Article 6)

According to Article 6 of the Agreement, ACBPS shall ensure the availability, as soon as practicable, of relevant and appropriate analytical information obtained from PNR data received under the Agreement to Member States' police or judicial authorities, Europol or Eurojust. Moreover, Member States' police or judicial authorities, Europol and Eurojust may request access to PNR data or analytical information obtained from PNR data that had been received by ACBPS under the Agreement. ACBPS set out that it had provided analytical information obtained from PNR data to Europol in eight cases related to drugs trafficking to Australia. In addition to case-related information shared with Europol, Australia exchanged PNR based risk indicators (such as specific travel patterns) with EU Member States. As an example for this, ACBPS referred to the sharing of risk indicators based on PNR data related to drug trafficking with the United Kingdom, France and Germany on ten occasions in the first half of 2013, which resulted in the detection of over 40 kilograms of drugs and the arrest of eleven persons.

ACBPS explained that for the time being, the process of identifying relevant analytical information that needed to be shared with the EU was highly manual. ACBPS is currently developing system capabilities to automatically identify such relevant analytical information, and these capabilities should enable the efficient sharing with the EU of analytical information obtained from PNR data that is relevant for the combating of terrorism and serious transnational crime. In this context, ACBPS referred to difficulties in identifying the contact persons in Member States and the appropriate communication channel to share analytical information obtained from PNR data received under the Agreement.

ACBPS explained that it had received one request for PNR data from a Member State under Article 6(2) of the Agreement, in a case related to drugs trafficking. The request was made through the ACBPS Counsellor at the Australian Embassy in Belgium, and ACBPS provided the requested information. In general, Member States make very limited use of the possibility to request information under Article 6(2) of the Agreement, which might be due to a lack of awareness of the means for police, law enforcement and judicial cooperation under the Agreement. In those cases where Europol and a Member State received analytical information obtained from PNR data, the feedback provided to ACBPS on the use of this information and the results achieved was very limited. This should be improved.

Recommendation: The EU team welcomes the efforts made by ACBPS to improve the sharing with the EU of analytical information obtained from PNR data 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 notes 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 is 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.

3. CONCLUSIONS

The joint review mechanism enabled the EU team to witness how the data is used in practice and to have direct exchanges with targeters, analysts and other officials who use PNR data.

The overall finding is that Australia has fully implemented the Agreement in line with the conditions set out therein. 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 in the Agreement. 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. 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, it is noted that law enforcement cooperation based on the sharing of analytical information obtained from PNR data requires more attention. 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. At the same time, recipients of such information on the EU side should provide adequate feedback to ACBPS on the use of this information and the results

achieved. Australia is also requested to set up a reporting mechanism that will enable Australia to inform Member States if PNR data received under the Agreement, or analytical information containing such data, is eventually shared with a third country. Moreover, Australia should continue to ensure that the safeguards set out in the Agreement are also afforded to extracted PNR data that is shared with other areas of ACBPS or other Australian government authorities.

Australia is to be commended for the way it applies the PNRGOV “push” method. Although outside the scope of the Agreement, it is welcomed that Australia extended the application of the "push" method to all airlines not covered by the Agreement. Moreover, Australia is a forerunner in the development and promotion of the PNRGOV standard messaging format worldwide, seeking to achieve global standardisation for the transmission of PNR data in its engagement with individual airlines and in the framework of WCO, ICAO and IATA.

It is envisaged to combine the next joint review of the Agreement with the joint evaluation of the Agreement in mid-2016.

ANNEX A
EU QUESTIONNAIRE AND ACBPS REPLIES

1. QUESTIONS OF A GENERAL NATURE

Q1: *Has the transition from the 2008 Agreement to the 2012 Agreement given rise to any particular difficulties?*

The transition from the 2008 Agreement to the 2012 Agreement has not given rise to any particular difficulties. The change in the Agreement regarding the requirement to depersonalise PNR after 3 years rather than archive after 3.5 years was the main area of change impacting the implementation of the PNR system for the Australian Customs and Border Protection Service (ACBPS). This requirement has been considered as part of the design of the PNR system. No other difficulties due the transition were noted.

Q2: *Are all mechanisms required to properly implement the Agreement, in particular those aimed at implementing the safeguards, in place and operating satisfactorily?*

The safeguards outlined in the Agreement were analysed and incorporated into each PNR System capability as it was developed and implemented by ACBPS. These technical safeguards are further complemented by Policy Directions, Practice Statements and Instructions and Guidelines that provide policy and procedural guidance to support the operational processing of PNR data.

The safeguards and controls (systems and procedural) are outlined in the ACBPS PNR Control Framework. System based controls have been validated by ACBPS as part of the quality assurance over the development of the PNR system.

An internal quality assurance framework is also being designed and implemented which includes specific measures to ensure the on-going application of the safeguards required in the Agreement, including for example, PNR System user access monitoring and review.

Q3: *Have any specific incidents occurred during the first year of implementation of the Agreement?*

No.

2. GENERAL PROVISIONS

2.1 Article 2 – definitions

2.1.1 Article 2(d)

Q1: *Does Australia obtain 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 flights that depart from the territory of an EU Member State but do not have a stop-over or the final destination in Australia, and to delete related PNR data obtained by Australia?*

ACBPS uses the OAG Flight Schedule 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.

2.2 Article 3 – scope of application

2.2.1 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.

2.2.2 Article 3(3)

Q2: *Have there been any difficulties in applying of the definition of serious transnational crime?*

No. Article 3 clearly outlines the definition of transnational crime and generally the interpretation of this definition for operational purposes is in most cases, straightforward. The application of the definition can at times be difficult where the serious transnational crime for which the PNR is processed is less common than most cases. This does not prevent the ability to apply the definition, but rather makes the process less straightforward.

Q3: *How do officers of the Australian Customs and Border Protection Service determine if a crime is transnational in nature?*

The definitions of 'transnational' outlined in Article 3 of the Agreement are used to determine if the crime is transnational. ACBPS are yet to determine a case where the processing of PNR has defined transnational outside of these definitions.

2.2.3 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?*

Nil.

Q5: *What are specific examples of such cases?*

N/A

2.2.4 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.

Q7: *What are specific examples of such cases?*

N/A

2.3 Article 4 – ensuring provision of PNR data

2.3.1 Article 4(3)

Q1: *Is there a mechanism in place to filter out and delete PNR data beyond those listed in Annex 1 of the Agreement?*

Currently PNR data is received by ACBPS in the two data formats outlined below:

a) SBRRES/PRL EDI format PNR data from Amadeus is received via a secure channel which provides a direct link between Amadeus (the airline service provider) and ACBPS. EDI Messages from Amadeus are received via the ACBPS Gateway and Customs Connect Facility (CCF). PNR data beyond those listed Annex 1 of the Agreement is removed within CCF prior to the PNR data being loaded into the PNR Data Store.

b) PNRGOV format PNR data is also received via the ACBPS Gateway and Customs Connect Facility (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.

Overall for both formats, data beyond the elements listed in Annex 1 of the Agreement are removed and deleted prior to being loaded in the PNR data store.

Q2: *Has this mechanism been audited and if so, which conclusions have been drawn?*

Overall for both SBRRES/PRL EDI and PNRGOV format, data outside the elements listed in Annex 1 of the Agreement are 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.

Q3: *Has the Australian Customs and Border Protection Service become aware of any additional type of PNR information that may be available and required for the purposes set out in Article 3 and if so, which?*

No, ACBPS is not aware of any additional PNR data elements. 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.

Q4: *Has the Australian Customs and Border Protection Service become aware of any type of PNR information that is no longer required for the same purposes and if so, which?*

No, ACBPS has not identified any PNR data elements that are not required.

Q5: *Has the Australian Customs and Border Protection Service ever used information held in PNR obtained under the Agreement beyond those listed in Annex 1 of the Agreement, including sensitive information, and if so, how many times and for what reasons?*

No, any data that may be provided beyond Annex 1 of the Agreement cannot be collected by the PNR system, therefore cannot be processed.

2.4 Article 6 – police and judicial cooperation

2.4.1 Article 6(1)

Q1: *In how many cases did the Australian Customs and Border Protection Service provide analytical information obtained from PNR data to police or judicial authorities of EU Member States, Europol or Eurojust?*

ACBPS provided analytical information obtained from PNR data to Europol in relation to eight cases.

Currently ACBPS is developing technical capabilities to enable the efficient delivery of reports obtained from PNR data. As these capabilities are implemented, ACBPS will be able to review the dimensions of the output and examine analytical information that is relevant and appropriate for disclosure to the authorities stipulated in the Agreement.

Q2: *What are specific examples of such cases?*

All cases related to the importation to Australia of prohibited substances including illicit drugs, illicit precursor chemicals and Performance and Image enhancing drugs (PIEDs). Further detail relating to each case can be provided if required.

Q3: *What criteria does the Australian Customs and Border Protection Service apply to define 'as soon as practicable' in order to provide analytical information obtained from PNR data?*

ACBPS is developing system capabilities to automatically identify cases. As the current processes are highly manual, they are completed periodically as resources allow.

Q4: *What information exchange channels have been used to provide analytical information obtained from PNR data to police or judicial authorities of EU Member States, Europol or Eurojust?*

For the cases detailed in Q1 the information was transferred to Europol using existing information exchange processes with the Australian Federal Police via the ACBPS Counsellor in Brussels. The information was transferred with consideration to the security classification and the use of appropriate information exchange channels. ACBPS has an office that coordinates all international exchange of information, OSCORD (Overseas Co-ordination Unit).

2.4.2 Article 6(2)

Q5: *How many requests has the Australian Customs and Border Protection Service 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?*

To date, ACBPS has received one (1) request for PNR data or analytical output from PNR data by police or judicial authorities of EU Member States, Europol or Eurojust.

Q6: *In how many cases did the Australian Customs and Border Protection Service made such information available?*

On one (1) occasion, PNR data was made available in response to a request.

Q7: *What are specific examples of such cases?*

The specific matter related to the detection and prosecution of an individual for illicit drug importation into Australia. Further detail relating to this case can be provided if required.

3. SAFEGUARDS APPLICABLE TO THE PROCESSING OF PNR DATA

3.1 Article 7 – data protection and non-discrimination

3.1.1 Article 7(2)

Q1: *What measures are implemented to ensure that the safeguards applicable to the processing of PNR data under the Agreement and relevant national laws apply to all passengers without discrimination?*

In implementing the PNR System and supporting processes, ACBPS has put in place a risk mitigation strategy in the form of a 'PNR Control Framework' that documents the safeguards implemented by ACBPS applicable to processing PNR data under the Agreement, the

Australian Privacy Act 1988, Freedom of Information Act 1982 and the Australian Commonwealth Protective Security Policy Framework.

Further, as part of the implementation of the PNR System, ACBPS has performed a Privacy Impact Assessment which considers the application of the data protection and privacy safeguards under the Australian Privacy Act 1988 and the Agreement. It should be noted that the principles in the Australian Privacy Act 1988 provide individuals protection against the mishandling of their personal information, and apply equally to all individuals whose PNR data is processed by ACBPS.

The PNR Control Framework and Privacy Impact Assessment are aids to ensure that safeguards employed under the Agreement and relevant national laws are applied to all travellers to Australia without discrimination by the following mechanisms:

- all PNR data transferred to ACBPS is handled and safeguarded in the same fashion irrespective of the basis of nationality or country of residence or physical presence in Australia of the individuals to whom the PNR relates; and
- the objective of the PNR System (EPAC2 program) is to increase the level of certainty about the relative risk travellers represent earlier in the traveller pathway to enable border protection, law enforcement and intelligence agencies to make timely, well placed, risk based response and resource deployment decisions. Increased certainty around the identification of persons of interest reduces the privacy impact of the use of PNR data in relation to the general public travelling to or from Australia.

3.2 Article 8 – sensitive data

Q1: *How does the Australian Customs and Border Protection Service 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 ACBPS and therefore, sensitive data can not be filtered out until after the PNR data is received by ACBPS.

It is planned that the SBRRES/PRL format will be replaced by the PNRGOV format for PNR data. PNRGOV is a new Electronic Data Interchange (EDI) based industry standard message structure developed by IATA. This format will support a more effective way of organising data being pushed from airline reservation systems to ACBPS. The structure will support a XML-based message structure which will provide the ability to manage PNR data in a more effective and efficient manner, including the potential to remove and delete certain sensitive data should it be included in the PNR. The PNRGOV message format is not currently at a mature enough stage to allow this to occur and ACBPS sees this as a longer term goal.

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

- applies filters over Salutation and Special Service Requests (SSR) (i.e. meal types and special passenger requirements);
- 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 PNR Control Framework - refer to Control 41 page 59.

Q2: *Have there been any difficulties in the filtering out and deletion of sensitive data from PNR obtained under the Agreement?*

Yes. There have been some difficulties in the filtering out and deletion of sensitive data from PNR obtained under the Agreement. As noted under Q1 above, 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 ACBPS and therefore, sensitive data cannot be filtered out until after the PNR data is received by ACBPS.

Further, the message formats of both SBRRES/PRL and PNRGOV are such that sensitive data might be contained in free-text fields that are difficult to identify and delete. Therefore as outlined in Q1 a combination of system and manual processes are used to identify and delete sensitive data contained within PNR prior to use or disclosure.

Q3: *Has the Australian Customs and Border Protection Service ever used sensitive data held in PNR obtained under the Agreement?*

No. In order to filter out and delete sensitive data, ACBPS:

- applies filters over Salutation and Special Service Requests (SSR) (i.e. meal types and special requirements);
- applies 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 PNR Control Framework - refer to Control 41 page 59.

3.3 Article 9 - data security and integrity

Q1: *What technical and organisational measures have been implemented to protect personal data and personal information contained in PNR?*

In alignment with the implementation of the PNR System and supporting processes, ACBPS has also put in place a risk mitigation strategy in the form of a 'PNR Control Framework' that documents the safeguards implemented by ACBPS applicable to processing PNR data under the Agreement, the Australian Privacy Act 1988, Freedom of Information Act 1982 and the Australian Commonwealth Protective Security Policy Framework.

Further, as part of the implementation of the PNR system ACBPS has performed a Privacy Impact Assessment which considers the application of the Australian Privacy Act 1988 and the Agreement.

The following key controls have been implemented by ACBPS:

- clear definition and boundary of the PNR system that is used to manage user access and to separate PNR data from other Customs data;

- user access controls which require users to seek approval from the CEO to access PNR data and approval from the system owner's delegate to obtain access to PNR systems and data;
- built in functionality and systems controls that have implemented key requirements under the Agreement;
- implementation of Policy and Procedures with respect to the handling, management and disclosure of PNR data; and
- implementation of backup and recovery measures and disaster recovery plans.

In addition, the Office of the Australian Information Commissioner conducts independent biannual audits of ACBPS management, use and disclosure of PNR data against compliance with Australian privacy laws and the Agreement.

3.3.1 Article 9(1)

Q2: *What measures are in place to prevent accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any unlawful forms of processing?*

The following key controls have been implemented by ACBPS to prevent accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any unlawful forms of processing:

- clear definition and boundary of the PNR system that is used to manage user access and separate PNR data from other ACBPS data;
- user access controls which require users to seek approval from the CEO to access PNR data and approval from the system owner's delegate to obtain access to PNR systems and data;
- built in functionality and controls that have implemented key requirements under the Agreement i.e. with regard to user logging and purpose limitation requirements;
- implementation of Policy and Procedures with respect to the handling, management and disclosure of PNR data; and
- implementation of backup and recovery measures and disaster recovery plans.

PNR data cannot be altered using standard user access provided by the PNR system. All changes to PNR data must be made under strict change control measures implemented by ACBPS.

Backup and recovery processes implemented across ACBPS IT infrastructure, including PNR data, ensure that there is no accidental loss of data.

PNR data will be deleted by ACBPS in accordance with the data retention requirements outlined in the Agreement. ACBPS have designed automated processes to delete and depersonalise PNR data bases on these requirements.

3.3.2 Article 9(1)(d)

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

The safeguards outlined in the Agreement were analysed and incorporated into each PNR System capability as it was developed and implemented by ACBPS. These technical safeguards are further complemented by Policy Directions, Practice Statements and

Instructions and Guidelines that provide policy and procedural guidance to support the operational processing of PNR data.

The safeguards and controls (systems and procedural) are outlined in the ACBPS PNR Control Framework. System based controls have been validated by ACBPS as part of the quality assurance over the development of the PNR system.

An on-going quality assurance framework is also being implemented which includes specific measures to ensure the on-going application of the safeguards required in the Agreement, including for example, PNR System user access monitoring and review.

Specific systems based audit have been performed including:

- audit logging and monitoring of user access to the PNR system; and
- quarterly user access reviews that compare PNR users access to those staff approved to access PNR data under delegation from the Customs and Border Protection CEO.

3.3.3 Article 9(2)

Q4: *Has there been any breach of data security?*

No.

3.3.4 Article 9(3)

Q5: *Has the Australian Customs and Border Protection Service reported any breach of data security to the Office of the Australian Information Commissioner?*

No.

3.4 Article 10 – oversight and accountability

3.4.1 Article 10(2)

Q1: *How many formal audits of the Australian Customs and Border Protection Service's processing of PNR data have been conducted by the Australian Information Commissioner since the Agreement entered into force? What was the outcome of these audits?*

Since 2008, the Australian Information Commissioner has averaged two formal audits per year on ACBPS processing of PNR data.

The most recent two audits scope and outcomes were:

- November 2011 – post arrival processing of PNR at international airports. No breaches of the IPPs were identified and therefore no recommendations were made other than two best privacy practice suggestions on information management which were accepted by ACBPS.
- October 2012 – Request for PNR Information (RFPI) process

  Five recommendations were made and accepted by ACBPS. No breaches of the IPPs were identified and five recommendations were made related to potential future risks including:

  1) the finalisation of policy and procedural documents;

  2) a review of electronic storage arrangements;

  3) a systems audit of IT systems outside of the PNR systems to ensure compliance;

  4) a review of audit logs to improve monitoring; and

5) a review of identity verification procedures in the handling of verbal requests.

3.4.2 Article 10(3)

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

To date, the Australian Information Commissioner has not referred any complaints related to the Agreement.

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

3.4.3 Article 10(4)

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

To date, the Commonwealth Ombudsman has not referred any complaints related to 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.

3.5 Article 11 – transparency

3.5.1 Article 11(1)

Q1: *What measures are 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?*

Advice that ACBPS collects and uses PNR data which also outlines the purpose, authority, use and disclosure provisions relating to PNR data is contained on the ACBPS website at http://www.customs.gov.au/site/page6094.asp

Passengers are also 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.

3.5.2 Article 11(2)

Q2: *What measures are implemented to provide the public with information on the purpose of collection and use of PNR data by the Australian Customs and Border Protection Service?*

Advice that ACBPS collects and uses PNR data which also outlines the purpose, authority, use and disclosure provisions relating to PNR data is contained on the ACBPS website at http://www.customs.gov.au/site/page6094.asp

Passengers are also 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.

Q3: *How does Australia provide the public with information on how to request access, correction and redress under the Agreement?*

Advice on the ACBPS website at http://www.customs.gov.au/site/page6094.asp also provides the public with information on how to request access, correction and redress under the Agreement.

3.6 Article 12 – right of access

3.6.1 Article 12(1)

Q1: *How many requests from individuals for access to PNR data have been received by the Australian Customs and Border Protection Service?*

Nil. An individual may request access to any information, including PNR data, held by ACBPS. A Freedom of Information (FOI) request is processed through ACBPS's Legal Services Branch and the scope of the request is clarified with the individual before processing the request.

ACBPS has not received any requests or application for access to information under the Freedom of Information Act 1982 where the scope includes PNR data.

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

Nil.

Q3: *How many requests have been received by the Australian Customs and Border Protection Service for access to documents held by the Australian Customs and Border Protection Service 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?*

Nil. The request to access documents is provided under the Freedom of Information Act 1982 and ACBPS follows the same process as outlined in Q1.

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

Nil.

Q5: *What was the average response time by the Australian Customs and Border Protection Service to requests for access?*

N/A

3.6.2 Article 12(2)

Q6: *In how many cases was the disclosure of information limited and for what reasons?*

N/A

3.6.3 Article 12(3)

Q7: *How many refusals or restrictions of access have been set out in writing and provided to requesting individuals?*

N/A

Q8: *What was the average response time by the Australian Customs and Border Protection Service?*

N/A

Q9: *How many times have individuals lodged a complaint with the Australian Information Commissioner against a decision of the Australian Customs and Border Protection Service to refuse or restrict access to information?*

Nil.

3.6.4 Article 12(4)

Q10: *If individuals lodged such complaints with the Australian Information Commissioner, what was the outcome of the investigation of these complaints?*

N/A

3.7 Article 13 – right of rectification and erasure

3.7.1 Article 13(1)

Q1: *How many requests from individuals seeking the rectification of their PNR data have been received by the Australian Customs and Border Protection Service?*

Nil.

3.7.2 Article 13(3)

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

N/A

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 Customs and Border Protection Service to requests for rectification?*

N/A

3.7.3 Article 13(4)

Q5: *How many times have individuals lodged a complaint with the Australian Information Commissioner against a decision of the Australian Customs and Border Protection Service related to a request for rectification?*

Nil.

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

N/A

3.8 Article 14 – right of redress

3.8.1 Article 14(1)

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

Nil.

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

Nil.

Q3: *What was the outcome of these procedures?*

N/A

3.8.2 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.

3.8.3 Article 14(3)

Q5: *What measures are implemented 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 following measures have been implemented to provide all individuals with the right to seek effective administrative and judicial redress:

Office of Ombudsman

The Ombudsman Act 1976 (Cth) established the office of Ombudsman to function as a watchdog over the executive arm of government by investigating complaints relating to actions relating to matters of administration taken by a department or prescribed authority and making recommendations to the administrator whose action is being investigated and to the responsible Minister. The Ombudsman may investigate such actions in response to complaints made or of his own motion. This avenue of redress is open to all individuals aggrieved by any actions taken by departments or prescribed authority regardless of whether the individual is an Australian citizen.

Privacy Commissioner

The Privacy Act 1988 provides protection of an individual's personal information in regard to its collection and disclosure. PNR information is protected under this legislation and government departments and agencies are required to comply with certain requirements to ensure that PNR information is collected in a lawful manner and disclosed only under strict controls. All persons including non-citizens have access to the Privacy Commissioner and his office to seek redress of any breach of legislative requirements.

Judicial Review

The Administrative Decisions (Judicial Review) Act 1977 was enacted to provide a simple procedure of application by any individual including non-citizens for an order of judicial review of administrative decisions taken by and conduct of administrators of Government departments and authorities. The Federal Court may either:

- set aside the decision;
- make an order referring the matter to which the decision relates to the person who made the decision for further consideration, subject to such directions as the court thinks fit;
- make an order declaring the rights of the parties in respect of any matter to which the decision relates;

- make an order directing any of the parties to do, or to refrain from doing, any act or thing the doing, or the refraining from the doing, of which the court considers necessary to do justice between the parties.

Any person aggrieved by any administrative action or decision relating to the collection or disclosure of PNR may have available to him/her any or all of the above measures to seek administrative or judicial redress without discrimination.

3.9 Article 16 – retention of data

3.9.1 Article 16(1)(a)

Q1: *How many officials of the Australian Customs and Border Protection Service are authorised to access PNR data from the initial receipt to three years?*

At this time there are 132 ACBPS officers who hold a Delegation to access PNR data under section 64AF of the Customs Act 1901. These include officers who have access to the PNR system for undertaking risk assessment activity as well as officers who are responsible for systems development and maintenance activity.

3.9.2 Articles 16(1)(b)

Q2: *What 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?*

ACBPS is designing and implementing the following measures:

- masking out 3 years after receipt of the data of all PNR data fields identified as potentially containing personal data elements which could serve to identify the passenger to whom the data relates. This will be performed by the use of access roles that mask access at the database table and field level for those elements potentially containing personal PNR data;
- general PNR system users will not have access to any personalised data after 3 years from receipt of the data; and
- Advanced Analytics users will have access to depersonalised data after 3 years.

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

The main difficulty is the scope of the application of data retention and depersonalisation requirements which raised both the operational efficiency and cost effectiveness of these measures. In response to these difficulties, ACBPS developed a policy direction to clarify the scope of the PNR data retention and depersonalisation requirements in Article 16 of the PNR Agreement.

The policy direction which sets out the operational difficulties and rationale for the clarification of the scope of Article 16 can be provided.

Q4: *How many officials of the Australian Customs and Border Protection Service are authorised to access depersonalised PNR data from three years after initial receipt to the end of the five and a half year period?*

This has been identified as the Advanced Analytics team which is currently a group of eight (8) users.

3.9.3 Article 16(3)

Q5: *Has paragraph 16(3) of the Agreement been applied in practice yet?*

No records have yet been flagged as being required to be retained until the relevant investigation or prosecution is concluded or penalty enforced.

As noted ACBPS is currently implementing automated data retention and depersonalisation functionality into the PNR systems and there will be functionality provided to PNR system users to flagged PNR records that are required to be retained.

3.10 Article 17 – logging and documentation of PNR data

3.10.1 Article 17(1)

Q1: *Which logging and documentation procedures are applied by the Australian Customs and Border Protection Service for the purpose of verification of lawfulness of the data processing, self-monitoring and ensuring appropriate data integrity and security of data processing?*

ACBPS employs the following audit logging in relation to PNR data:

- audit logging of all user access in particular read access as this is only access provided;
- audit logging at the PNR database level; and
- logging of all information disclosures to other Australian government authorities.

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

3.11.1 Article 18(1)(a)

Q1: *How does the Australian Customs and Border Protection Service guarantee that receiving government authorities afford to PNR data the safeguards as set out in the Agreement?*

ACBPS cannot provide a guarantee, however Government authorities provide a written undertaking that they will only use information given to them by ACBPS 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 agency 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.

3.11.2 Article 18(1)(d)

Q2: *How does the Australian Customs and Border Protection Service ensure that only the minimum amount of data possible is shared?*

Policy documentation, including Practice Statements, Instructions and Guidelines and Associated Documents 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.

3.11.3 Article 18(3)

Q3: *How does the Australian Customs and Border Protection Service ensure that the safeguards in Article 18 of the Agreement are respected when transferring analytical information containing PNR data obtained under the Agreement?*

Safeguards as outlined in Q1 & Q2 above.

3.12 Article 19 – transfers to authorities of third countries

3.12.1 Article 19(1)(a)

Q1: *How does the Australian Customs and Border Protection Service determine whether the receiving third country authority has agreed to afford to the data transferred the same safeguards as set out in the Agreement?*

A formal Memoranda of Understanding must be in place between ACBPS and the third country/international agency. Consideration of the third country policies and safeguards are a consideration for the development of the Memoranda of Understanding.

All requests for PNR data or the output of analysis come through OSCORD (overseas Co-ordination unit), or via our International Overseas Diplomatic representatives (Counsellor or First Secretary).

3.12.2 Article 19(1)(e)

Q2: *How does the Australian Customs and Border Protection Service ensure that only the minimum amount of data possible is shared?*

Policy documentation, including Practice Statements, Instructions and Guidelines and Associated Documents 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 are shared.

3.12.3 Article 19(1)(f)

Q3: How many times has the Australian Customs and Border Protection Service 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?

Nil.

Q4: *How did the Australian Customs and Border Protection Service inform the competent authorities of a Member States of the fact that data of a national or a resident of that Member State had been transferred?*

N/A

Q5: *Did the competent authorities of the Member State react to this sharing of information?*

N/A

Q6: *Have there been situations in which the competent authorities of a Member State were not informed about the fact that data of a national or a resident of that Member State had been transferred and if so, why?*

N/A

3.12.4 Article 19(1)(h)

Q7: *How does the Australian Customs and Border Protection Service 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 ACBPS 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.

Q8: *How does the Australian Customs and Border Protection Service ensure that the safeguards in Article 19 of the Agreement are respected when transferring analytical information containing PNR data obtained under the Agreement?*

Currently ACBPS is developing technical capabilities to enable the efficient delivery of reports obtained from PNR data. As these capabilities are implemented, ACBPS will be able to review the dimensions of the output and assess the analytical information for its relevance and appropriateness for disclosure to the authorities stipulated in the Agreement.

4. MODALITIES OF TRANSFERS

4.1 Article 20 – the method of transfer

Q1: *How does Australia ensure that air carriers transfer PNR data to the Australian Customs and Border Protection Service exclusively on the basis of the push method?*

ACBPS actively engages with airlines with a team responsible for maintaining the on-going provision of passenger data. Through active engagement, airlines or service providers advise ACBPS of system changes and ACBPS communicates the requirements under the Australia-EU PNR Agreement. ACBPS has a strong working relationship with Amadeus and communicates regularly on any changes to airlines transitioning to and from any EU hosted service. ACBPS is actively working with airlines who do not host data in the EU to transition PNR data transfer to the 'Push' method.

Q2: *Does Australia obtain PNR data from air carriers that have reservation systems and/or PNR data processed in the territory of the EU and operate passenger flights in international air transportation to, from or through Australia exclusively on the basis of the push method?*

Yes, the 'Push' method is the exclusive method of transfer for air carriers that have a reservation and check-in system in member states of the EU.

4.1.1 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 cases where the connection between Amadeus and ACBPS has been disrupted. This has been due to communication or system outages at either end. The current secure connection from Amadeus to ACBPS was upgraded in June 2013.

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

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

4.2 Article 21 – the frequency of transfer

4.2.1 Article 21(1)

Q1: *How many times per flight do air carriers have to transfer PNR data to the Australian Customs and Border Protection Service?*

There is a requirement for air carriers to provide 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 departure time.

4.2.2 Article 21(2)

Q2: *Have there been cases in which the Australian Customs and Border Protection Service required an air carrier to provide PNR data prior to the first scheduled transfer?*

Yes. There have been a total of 4 cases since July 2010 where PNR data for a specific flight was requested prior to the first scheduled transfer.

Q3: *What are specific examples of such cases?*

In all cases, PNR data was requested for risk assessment purposes prior to the first scheduled transmission of PNR data.

4.2.3 Article 21(3)

Q4: *Have there been cases in which the Australian Customs and Border Protection Service required an air carrier to provide PNR data in between or after regular transfers?*

Yes. There have been 50 cases since July 2010 where PNR data for a specific flight was requested in between the regular transfer.

Q5: *What are specific examples of such cases?*

Updated PNR data were requested for risk assessment purposes prior to the next scheduled transmission of PNR data.

ANNEX B
COMPOSITION OF THE REVIEW TEAMS

The members of the EU team were:

– Reinhard Priebe, Director, European Commission, DG Home Affairs – Head of the EU delegation

– Julian Siegl, European Commission, DG Home Affairs,

– Liene Balta, European Commission, DG Justice,

– Péter Kimpián, expert on data protection in the law enforcement area from the Hungarian data protection authority

– Bruno Scholl, EU Delegation in Canberra

– Lynne Hunter, EU Delegation in Canberra.

The members of the Australian team were:

– Roman Quaedvlieg, Deputy Chief Executive Officer for Border Enforcement, Australian Customs and Border Protection Service (ACBPS) – Head of the Australian delegation

– Rachel Noble, National Director Intelligence Division and Chief Information Officer, ACBPS

– Teresa Conolan, Chief of Staff, National Manager Executive Coordination, ACBPS

– John Gibbon, National Manager, National Border Intelligence and Targeting Centre Capability Branch, Intelligence Division, ACBPS

– Timothy Pilgrim, Privacy Commissioner, Office of the Australian Information Commissioner

– Angelene Falk, Assistant Commissioner, Office of the Australian Information Commissioner

– Neil Smail, European Union Section, Department of Foreign Affairs and Trade

– Sally Macourt, Director, Strategy and Policy, Intelligence Division, ACBPS

– Angela Black, Director, Passenger Analysis Unit, Intelligence Division, ACBPS

– Michael Odgers, Director, Industry Engagement, Intelligence Division, ACBPS

– Steven Kouparitsas, Compliance, Intelligence Division, ACBPS.

ANNEX C
PNR CASE STUDIES

Recent PNR Case Studies – counterterrorism

PNR data is used to support law enforcement and national security investigations within the purpose limitations of the Agreement. For example, PNR was used to link the association of two suspected terrorists, both of whom were convicted of terrorist related offences in Europe and Australia.

Recent PNR Case Studies – drugs trafficking

29 August 2013: Pre-arrival risk assessment based on PNR data identified a traveller of interest (Traveller X) due to arrive at Melbourne Airport. Further analysis of the traveller's PNR and other data identified a number of risk indicators. Intervention was undertaken on arrival and 6kg of heroin was located in Traveller X's possession. On the basis of this information further analysis was undertaken using PNR data which identified that Traveller Y had similar characteristics of travel. An alert was placed on Traveller Y resulting in a further detection of 5.5 kg of heroin at Perth Airport.

19 August 2013: A 43 year old German national matched a risk indicator profile based on PNR data targeting European nationals travelling to Australia for the purpose of importing drugs. Further analysis of the PNR data and other data identified a range of risk associated with a number of illicit drug detections. An alert was placed on the traveller and the resulting examination by Customs and Border Protection officers at Perth Airport detected 5.2 kilograms of Crystal Methamphetamine concealed in the lining of the traveller's suitcase.

13 August 2013: A 71 year old Canadian citizen matched a pre arrival risk assessment profile based on PNR data targeting high risk travellers with travel originating in Central and South America. Further analysis of PNR and other data resulted in the placement of an alert. Examination by Customs and Border Protection officers at Sydney Airport detected 2 kilograms of cocaine concealed in the lining of the traveller's suitcase.

9 August 2013: A 41 year old UK national matched a pre-arrival risk assessment profile based on PNR data which was deployed in support of Customs and Border Protection Intelligence and Targeting activity surrounding a syndicate of UK nationals responsible for organising the importation of illicit drugs via the air passenger stream. Further analysis of the traveller's PNR data and other data identified a number of risk indicators. Intervention was undertaken on arrival and the passenger was found to be internally concealing cocaine.

24 March 2013: A 42 year old citizen and resident of the United States of America matched a pre arrival risk assessment profile based on PNR data which targets individuals travelling to Australia who are assessed as high risk for internally concealing illicit drugs. Further analysis of PNR and other data resulted in the placement of an alert. The resulting examination by Customs and Border Protection officers at Perth Airport detected 3.8 kilograms of Crystal Methamphetamine concealed in items within the traveller's luggage.

19 March 2013: A 64 year old German national matched a pre-arrival risk assessment profile based on PNR data targeting European nationals travelling to Australia for the purpose of importing drugs. Further analysis of PNR and other data resulted in the placement of an alert. An examination by Customs and Border Protection officers at Sydney Airport detected 5 kilograms of Crystal Methamphetamine concealed in the lining of the traveller's suitcase.

22 December 2012: A 27 year old Canadian national and resident of Hong Kong matched a pre-arrival risk assessment profile based on PNR data targeting high risk travellers from Hong Kong. Further assessment of PNR and other data resulted in the placement of an alert. An examination by Customs and Border Protection officers at Sydney Airport detected 4 kilograms of Crystal Methamphetamine concealed under the clothing the traveller was wearing.

6 April 2013: PNR data enabled the identification of further criminal syndicate members after a targeted cargo importation led to the arrest of a Hong Kong and a Canadian national and the detection of more than 365 litres of liquid methamphetamine imported in a shipping container in a joint law enforcement operation involving ACBPS, federal and state police.

January to October 2013: A risk based assessment using PNR data was successful in identifying travellers disguising their travel intentions. Twenty-three confirmed drug couriers with a total of 84.87 kilograms of illicit drugs seized was directly attributable to the use of PNR data and this risk based assessment process

Recent PNR Case Studies - possession of child pornography or exploitation material

During the **financial year 2012/13**, ACBPS finalised 28 cases involving the possession of child pornography or exploitation material which were originally transported by the passenger or detected in the passenger's baggage. Of these cases there were 17 individuals successfully prosecuted.

Recent PNR Case Studies – identity fraud

15 July 2013: Pre-departure flight screening identified a passenger of interest attempting travel from Vienna to Perth via Doha. Further analysis of the traveller's PNR data and other data identified a number of risk indicators. The passenger was referred for passport and face to passport assessment prior to boarding. The referral resulted in the detection of an Iranian using a fraudulent passport.

17 July 2013: Through targeted analysis of PNR, two passengers of interest were identified attempting travel from Paris to Melbourne via Dubai. The passengers matched the profile targeting travellers utilising counterfeit and altered European passports to travel to Australia in conjunction with other risk indicators identified through PNR data. The passengers were referred for assessment prior to boarding. The Greek passports presented were assessed as counterfeit and the travellers' nationality was confirmed as Albanian.

Recent PNR Case Studies – money laundering

January 2014: A risk based assessment and further analysis of a passenger's PNR data identified a number of risk indicators and the traveller was referred for examination into Melbourne airport. As a result of the examination, the examining officer did not locate any items of interest, but referred their ongoing suspicions of the traveller to an investigative team. Two days later the traveller and two travel companions were arrested with between $700,000AUD and $1,000,000AUD of laundered money following the referral.