EUROPEAN COMMISSION

Brussels, XXX
2011/HOME/035
[...](2011) XXX draft

RESTREINT UE

Proposal for a

COUNCIL DECISION

on the conclusion 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

EXPLANATORY MEMORANDUM

- Australian legislation empowers the Australian Customs Service to require each air carrier operating passenger flight to and from Australia to provide it with electornic 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).

- This legislation aims at obtaining PNR data electronically in advance of a flight's arrival and therefore significantly enhances the Australian Customs Sercice's ability to conduct efficient and effective advance risk assessment of passenger and to facilitate bona fide travel, thereby enhancing the security of Aystralia. The European Union in cooperating with Australia in the fight against terrorism and other serious transnational crime views the transfer of data to Australia as fostering international police and judicial cooperation which will be achieved though the transfer of analytical information flowing from PNR data by Australia to the competent Member States authorities as well as Europol and Eurojust within their respective competences.

- PNR is a record of each passenger' travel requirements which contains all information necessary to enable reservations to be processed and controlled by air carriers. As far as necessary to enable reservations to be processed and controlled by air carriers. As far as the current recommendation is concerned, PNR data covers data collected and contained in the air carrier's automated reservation and departure control systems.

- Air carriers are under an obligation to provide the Australian Customs Service with access to certain PNR data to the extent it is collected and contained in the air carrier's automated reservation and departure control systems.

- The data protection laws of the EU do not allow European and other carriers operating flight from the EU to transmit the PNR data of their passengers to third countries which do not ensure an adequate level of protection of personal data without adducing appropriate safeguards. A solution is required that will provide the legal basis for the transfer of PNR data from the EU to Australia as a recofnition of the necessity and importance of the use of PNR data in the gight against terrorism and other serious transnational crime, whilst avoiding legal uncertainty for air carriers. In addition, this solution should be applied homogenously throughout the European Union in order to ensure a legal certainty for air carriers and respect of individuals' rights to the protection of personal data as well as their physical security.

- The European Union signed an agreement in 2008 with Australia on the transfer and processing of PNR data based on a set of commitments by the Australian Customs Service in relation to the application of its PNR programme.[1]

---

1 OJ L 213, 8.8.2008, p.47.

- The European Parliament issued a resolution criticising various aspects of the agreement.[2]

- Following the entry into force of the Lisbon Treaty and pending the conclusion of the agreement, the Council sent the 2008 Australia Agreement to the European Parliament for its consent for the conclusion. The European Parliament adopted a resolution[3] in which it decided to postpone its vote on the requested consent and requesting a renegotiation of the Agreement on the basis of certain criteria. Pending such renegotiation, the 2008 Agreement would remain provisionally applicable.

- On 23 September 2010, the Council received three recommendations from the Commission to authorise the opening of negotiations for an Agreement between the European Union and Australia for the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crime.

- On 11 November 2010, the European Parliament adopted a resolution on the Recommendation from the Commission to the Council to authorise the opening of the negotiations.

- On 02 December 2010, the Council adopted a Decision, together with a negotiation directive, authorising the Commission to open negotiations on behalf of the European Union. Following negotiations between the parties, the Agreement was initialled on .... May 2011.

- This Agreement takes into consideration and is consistent with the general criteria laid down in the Communication from the Commission on the Global Approach to the transfer of Passenger Name Record (PNR) data to third countries[4] and the negotiating directives given by the Council.

- PNR has proven to be a very important tool in the fight against terrorism and serious crime. The Agreement has secured several important safeguards for those whose data will be transferred and processed, for example by giving individuals the right to access, correction and redress and the right to information. The data will be transferred using exclusively the 'push' method and the use of sensitive data is prohibited.

- The Article 218(2) of the Treaty on the Functioning of the European Union states that the Council shall authorise the signing of international agreements.

- The Commission therefore proposes to the Council to adopt a decision to conclude the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) by air carriers to the Australian Customs and Border Protection Service.

---

2 P7_TA(2010)0144.
3 P7_TA-(2010)0144, 5.5.2010
4 COM(2010)492.

Proposal for a

COUNCIL DECISION

on the conclusion 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

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 87(2)(a) and 88 (2), in conjunction with Article 218 (6)(a) thereof,

Having regard to the proposal from the European Commission,

Having regard to the consent of the European Parliament[5],

Acting in accordance with a special legislative procedure,

Whereas:

(1) On 02 December 2010, the Council adopted a Decision, together with negotiation directives, authorising the Commission to open negotiations on behalf of the European Union between the European Union and Australia for the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and other seious transnational crime.

(2) In accordance with Council Decision 2010/XXX of []6 the Agreement between the European Union and Australia for the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and other seious transnational crime was signed on …., subject to its conclusion at a later date.

(3) The Agreement has not yet been concluded. The procedures to be followed to that end by the European Union are governed by Article 218 of the Treaty on the Functioning of the European Union.

(4) The Agreement should be concluded.

(5) This Agreement respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union,

---

5 OJ C , , p. .
6 OJ L , , p. .

notably the right to private and family life, recognised in Article 7 of the Charter, the right to the protection of personal data, recognised in Article 8 of the Charter and the right to effective remedy and fair trial recognised by Article 47 of the Charter. This Agreement should be applied in accordance with those rights and principles.

(6) [In accordance with Article 3 of the Protocol 21 on the Position of the United Kingdom and Ireland in respect of the area of Freedom, Security and Justice annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, the United Kingdom and Ireland take part in the adoption of this Decision.]

(7) In accordance with Articles 1 and 2 of the Protocol 22 on the Position of Denmark annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Decision and is not bound by the Agreement or subject to its application.

HAS ADOPTED THIS DECISION:

Article 1

The Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record data from the European Union to Australia for purposes of the Passenger Name Record data is hereby concluded.

The text of the Agreement to be concluded is attached to this Decision.

Article 2

The President of the Council shall designate the person empowered to proceed, on behalf of the European Union, to the exchange of the instruments of approval provided for in Article 22 of the Agreement, in order to express the consent of the European Union to be bound by the Agreement.

Article 3

This Decision shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

Article 4

This Decision is addressed to the Member States in accordance with the Treaties.

Done at Brussels,

For the Council
The President

ANNEX

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

THE EUROPEAN UNION,

of the one part, and

AUSTRALIA,

of the other part,

Together hereinafter referred to as 'the Parties',

DESIRING to prevent and combat terrorism and serious transnational crime effectively as a means of protecting their respective democratic societies and common values;

SEEKING to enhance and encourage cooperation between the Parties in the spirit of the EU-Australian partnership;

RECOGNISING that information sharing is a fundamental component of the fight against terrorism and serious transnational crime, and in this context the use of Passenger Name Record (PNR) data is an essential tool;

RECOGNISING the importance of preventing and combating terrorism and serious transnational crime, while respecting fundamental rights and freedoms, in particular, privacy and the protection of personal data;

MINDFUL of Article 6 of the Treaty on European Union on respect for fundamental rights, the right to privacy with regard to the processing of personal data as stipulated in Article 16 of the Treaty on the Functioning of the European Union, the principles of proportionality and necessity concerning the right to private and family life, the respect for privacy, and the protection of personal data under Article 8 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, Council of Europe Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional Protocol 181, Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and Article 17 of the International Covenant on Civil and Political Rights on the right to privacy;

RECOGNISING that, in 2008, Australia and the EU signed the Agreement Between the European Union and Australia on the Processing and Transfer of European Union – Sourced Passenger Name Record (PNR) Data by Air Carriers to the Australian Customs Service which had provisional application from the time of signature but has not entered into force;

NOTING that the European Parliament decided on 5 May 2010 to postpone the vote on the request for consent to that Agreement and by its Resolution of 11 November 2010 welcomed the recommendation from the European Commission to the Council of the European Union to negotiate a new agreement;

RECOGNISING the relevant provisions of the Australian *Customs Act 1901* (Cth) (the Customs Act), and in particular section 64AF thereof whereby, if requested, all international passenger air service operators, flying to, from or through Australia, are required to provide the Australian Customs and Border Protection Service with PNR data, to the extent that they are collected and contained in the air carrier's reservations and departure control systems, in a particular manner and form;

RECOGNISING that the *Customs Administration Act 1985* (Cth), the *Migration Act 1958* (Cth), the *Crimes Act 1914* (Cth), the *Privacy Act 1988* (Cth), the *Freedom of Information Act 1982* (Cth), the *Auditor-General Act 1997* (Cth), the *Ombudsman Act 1976* (Cth) and the *Public Service Act 1999* (Cth) provide for data protection, rights of access and redress, rectification and annotation and remedies and sanctions for misuse of personal data;

NOTING the commitment of Australia that the Australian Customs and Border Protection Service processes PNR data strictly for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crime in strict compliance with safeguards on privacy and the protection of personal data, as set out in this Agreement;

STRESSING the importance of sharing of analytical data obtained from PNR by Australia with police and judicial authorities of Member States, and Europol or Eurojust, as a means to foster international police and judicial cooperation;

AFFIRMING that this Agreement does not constitute a precedent for any future arrangements between Australia and the European Union, or between either of the Parties and any State, regarding the processing and transfer of PNR data or any other form of data and noting that, in the future, similar arrangements may be considered for sea passengers;

HAVE AGREED AS FOLLOWS:

CHAPTER I

GENERAL PROVISIONS

Article 1

Purpose of Agreement

To ensure the security and safety of the public this Agreement provides for the transfer of EU-sourced PNR data to the Australian Customs and Border Protection Service. This Agreement stipulates the conditions under which such data may be transferred and used, and the manner in which the data shall be protected.

Article 2

Definitions

For the purposes of this Agreement:

a) 'Agreement' shall mean this Agreement and its Annexes, and any amendments thereto;

b) 'personal data' shall mean any information relating to an indentified or identifiable natural person: an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

c) 'processing' shall mean any operation or set of operations which is performed upon PNR data, whether or not by automatic means, such as collection, recording, organisation,

retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission or transfer, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

d) 'air carriers' shall mean 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;

e) 'reservation systems' shall mean an air carrier's reservation system, departure control system or equivalent systems providing the same functionalities;

f) 'Passenger Name Record data' or 'PNR data' shall mean the information processed in the EU by air carriers on each passenger's travel requirements as listed in Annex 1 which contains the information necessary for processing and control of reservations by the booking and participating air carriers;

g) 'passenger' shall mean passenger or crew member including the captain;

h) 'sensitive data' shall mean any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or health or sex life.

Article 3

Scope of application

1. Australia shall ensure that the Australian Customs and Border Protection Service processes PNR data received pursuant to this Agreement strictly for the purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious transnational crime:

2. Terrorist offences shall include:

a) acts of a person that involve violence, or are otherwise dangerous to human life or create a risk of damage to property or infrastructure, and which, given their nature and context, are reasonably believed to be committed with the aim of:

(i) intimidating or coercing a population;
(ii) intimidating, compelling, or coercing a government or international organisation to act or abstain from acting;
(iii) seriously destabilising or destroying the fundamental political, constitutional, economic, or social structures of a country or an international organisation;

b) assisting, sponsoring or providing financial, material or technological support for, or financial or other services to or in support of, acts described in a);

c) providing or collecting funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the acts described in a) or b); or

d) aiding, abetting, or attempting acts described in a), b) or c).

3. Serious transnational crime shall mean any offence punishable in Australia by a custodial sentence or a detention order for a maximum period of at least four years or a more serious penalty and as they are defined by the Australian law, if the crime is transnational in nature. A crime is considered as transnational in nature in particular if:

a) it is committed in more than one country;
b) it is committed in one country but a substantial part of its preparation, planning, direction or control takes place in another country;
c) it is committed in one country but involves an organised criminal group that engages in criminal activities in more than one country; or
d) it is committed in one country but has substantial effects in another country.

4. In exceptional cases, PNR data may be processed by Australia where necessary for the protection of the vital interests of any individual, such as risk of death, serious injury or threat to health.

5. In addition, for the purpose of supervision and accountability of public administration and the facilitation of redress and sanctions for the misuse of data, PNR data may be processed on a case-by-case basis where such processing is specifically required by Australian law.

Article 4

Ensuring provision of PNR data

1. Air carriers shall provide PNR data contained in their reservation systems to the Australian Customs and Border Protection Service. They shall not be prevented by any provision of the law of either Party from complying with relevant Australian law which obliges them to so provide the data.

2. Australia shall not require air carriers to provide PNR data elements which are not already collected or held in their reservation systems.

3. Should PNR data transferred by air carriers include data beyond those listed in Annex 1, the Australian Customs and Border Protection Service shall delete it.

Article 5

Adequacy

Compliance with this Agreement by the Australian Customs and Border Protection Service shall, within the meaning of relevant EU data-protection law, constitute an adequate level of protection for PNR data transferred to the Australian Customs and Border Protection Service for the purpose of this Agreement.

Article 6

Police and judicial cooperation

1. The Australian Customs and Border Protection Service shall ensure the availability, as soon as practicable, of relevant and appropriate analytical information obtained from PNR data to police or judicial authorities of the Member State concerned, or to Europol and Eurojust, within the remit of their respective mandates, and in accordance with law enforcement or other information sharing agreements or arrangements between Australia and any Member State of the European Union, Europol or Eurojust, as applicable.

2. A police or judicial authority of a Member State of the European Union, or Europol or Eurojust, within the remit of their respective mandates, may request access to PNR data or relevant and appropriate analytical information obtained from PNR data which is necessary in a specific case to prevent, detect, investigate, or prosecute within the European Union a

terrorist offence or serious transnational crime. The Australian Customs and Border Protection Service shall, in accordance with the agreements or arrangements referred to in 1, make such information available.

CHAPTER II

SAFEGUARDS APPLICABLE TO THE PROCESSING OF PNR DATA

Article 7

Data protection and non- discrimination

1. PNR data shall be subject to the provisions of the *Privacy Act 1988* (Cth) (Privacy Act) which governs the collection, use, storage and disclosure, security and access and alteration of personal information held by most Australian Government departments and agencies.

2. Australia shall ensure that the safeguards applicable to the processing of PNR data under this 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.

Article 8

Sensitive data

Any processing by the Australian Customs and Border Protection Service of sensitive PNR data shall be prohibited. To the extent that the PNR data of a passenger which is transferred to the Australian Customs and Border Protection Service include sensitive data, the Australian Customs and Border Protection Service shall delete it.

Article 9

Data security and integrity

1. To prevent accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any unlawful forms of processing:

a) PNR data-processing equipment shall be held in a secure physical environment, and maintained with high-level systems and physical intrusion controls;

b) PNR data shall be stored separately from any other data. For the purpose of matching, data may flow to the PNR system, but not from the PNR system to other databases. Access to the PNR system shall be limited to a restricted number of officials within the Australian Customs and Border Protection Service who are specifically authorised by the Chief Executive Officer to process PNR data for the purpose of this Agreement. These officials shall access the PNR system in secure work locations that are inaccessible to unauthorised individuals;

c) Access to the PNR system, by the officials described in b) shall be controlled by security access systems such as layered logins using a user ID and password;

d) Access to the network of the Australian Customs and Border Protection Service and any data contained in the PNR system shall be audited. The audit record generated shall contain the user name, the work location of the user, the date and time of access, the content of the query and the number of records returned;

e) All PNR data shall be transferred from the Australian Customs and Border Protection Service to other authorities in a secure manner;

f) The PNR system shall ensure fault detection and reporting;

g) PNR data shall be protected against any manipulation, alteration or addition or corruption by means of malfunctioning of the system;

h) No copies of the PNR database shall be made, other than for disaster recovery back-up purposes.

2. Any breach of data security, in particular leading to accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any unlawful forms of processing shall be subject to effective and dissuasive sanctions.

3. The Australian Customs and Border Protection Service shall report any breach of data security to the Office of the Australian Information Commissioner, and notify the European Commission that such a breach has been reported.

Article 10

Oversight and accountability

1. Compliance with data protection rules by the government authorities processing PNR data shall be subject to the oversight by the Australian Information Commissioner who, under the provisions of the Privacy Act, has effective powers to investigate compliance by agencies with the Privacy Act, and monitor and investigate the extent to which the Australian Customs and Border Protection Service complies with the Privacy Act.

2. The Australian Customs and Border Protection Service has arrangements in place under the Privacy Act for the Australian Information Commissioner to undertake regular formal audits of all aspects of Australian Customs and Border Protection Service's EU-sourced PNR data use, handling and access policies and procedures.

3. The Australian Information Commissioner will, in particular, hear claims lodged by an individual regardless of their nationality or country of residence, concerning the protection of his or her rights and freedoms with regard to the processing of personal data. The individual concerned will be informed of the outcome of the claim. The Australian Information Commissioner will further assist individuals concerned with exercising their rights under this Agreement, in particular rights of access, rectification and redress.

4. Individuals also have the right to lodge a complaint with the Commonwealth Ombudsman regarding their treatment by the Australian Customs and Border Protection Service.

Article 11

Transparency

1. Australia shall request air carriers to provide passengers with clear and meaningful information in relation to the collection, processing and purpose of the use of PNR data. Preferably this information will be provided at the time of booking.

2. Australia shall make available to the public, in particular on relevant government websites, information on the purpose of collection and use of PNR by the Australian Customs and Border Protection Service. This shall include information on how to request access, correction and redress.

Article 12

Right of access

1. Any individual shall have the right to access his or her PNR data, following a request made to the Australian Customs and Border Protection Service. It shall be provided without undue constraint or delay. This right is conferred by the *Freedom of Information Act 1982* (Cth) (Freedom of Information Act) and the Privacy Act. The right of access shall further extend to the ability to request and to obtain documents held by the Australian Customs and Border Protection Service as to whether or not data relating to him or her have been transferred or made available and information on the recipients or categories of recipients to whom the data have been disclosed.

2. Disclosure of information pursuant to paragraph 1 may be subject to reasonable legal limitations applicable under Australian law to safeguard the prevention, detection, investigation, or prosecution of criminal offences, and to protect public or national security, with due regard for the legitimate interest of the individual concerned.

3. Any refusal or restriction of access shall be set out in writing to the individual within thirty (30) days or any statutory extension of time. At the same time, the factual or legal reasons on which the decision is based shall also be communicated to him or her. The latter communication may be omitted where a reason under paragraph 2 exists. In all of these cases, individuals shall be informed of their right to lodge a complaint against the decision of the Australian Customs and Border Protection Service. This complaint will be lodged with the

Australian Information Commissioner. They shall be further informed of the means available under Australian law for seeking administrative and judicial redress.

4. Where an individual submits a complaint to the Australian Information Commissioner as referred to in paragraph 3, individual shall be formally advised of the outcome of the investigation of the complaint. He or she shall at least receive a confirmation whether his or her data protection rights have been respected in compliance with this Agreement.

5. The Australian Customs and Border Protection Service shall not disclose PNR data to the public, except to the individuals whose PNR data have been processed or their representatives.

Article 13

Right of rectification and erasure

1. Any individual shall have the right to seek the rectification of his or her PNR data processed by the Australian Customs and Border Protection Service where the data is inaccurate. Rectification may require erasure.

2. Requests for the rectification of PNR data held by the Australian Customs and Border Protection Service may be made directly to the Australian Customs and Border Protection Service pursuant to the Freedom of Information Act or the Privacy Act.

3. The Australian Customs and Border Protection Service shall make all necessary verifications pursuant to the request and without undue delay inform the individual whether his or her PNR data have been rectified or erased. Such notification shall be set out to the individual in writing within thirty (30) days or any statutory extension of time and provide information on a possibility of a complaint against the decision of the Australian Customs and Border Protection Service to the Australian Information Commissioner and otherwise on the means available under Australian law for seeking administrative and judicial redress.

4. Where an individual lodges a complaint to the Australian Information Commissioner as referred to in paragraph 3, the individual shall be formally advised of the outcome of the investigation.

Article 14

Right of redress

1. Any individual shall have the right to effective administrative and judicial redress in case any of his or her rights referred to in this Agreement have been violated.

2. Any individual who has suffered damage as a result of an unlawful processing operation or of any act incompatible with rights referred to in this Agreement shall have the right to apply for effective remedies, which may include compensation from Australia.

3. The rights referred to in paragraphs 1 and 2 shall be afforded to individuals regardless of their nationality or country of origin, place of residence or physical presence in Australia.

Article 15

Automated processing of PNR data

1. The Australian Customs and Border Protection Service or other government authorities listed in Annex 2 shall not take any decision which significantly affects or produces an adverse legal effect on a passenger solely on the basis of the automated processing of PNR data.

2. The Australian Customs and Border Protection Service shall not carry out the automated processing of data on the basis of sensitive data.

Article 16

Retention of data

1. PNR data shall be retained not longer than five and a half years from the date of the initial receipt of PNR data by the Australian Customs and Border Protection Service. During this period PNR data shall be retained in the PNR system only for the purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious transnational crime, and in the following manner:

a) From the initial receipt to three years, all PNR data shall be accessible to a limited number of the Australian Customs and Border Protection Service's officials specifically authorised by the Chief Executive Officer of the Australian Customs and Border Protection Service to identify passengers who may be potential persons of interest;

b) From three years after initial receipt to the end of the five and a half year period, PNR data shall be retained in the PNR system but all data elements which could serve to identify the passenger to whom PNR data relate shall be masked out. Such depersonalized PNR data shall be accessible only to a limited number of Australian Customs and Border Protection Service officials specifically authorised by the Chief Executive Officer of the Australian Customs and Border Protection Service to carry out analyses related to terrorist offences or serious transnational crime. Full access to PNR data shall be permitted only by a member of the Senior Executive Service of the Australian Customs and Border Protection Service if it is necessary to carry out investigations for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crimes.

2. To achieve depersonalization, the following PNR elements shall be masked out:

a) name(s);

b) other names on PNR, including number of travellers on PNR;

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

d) general remarks including other supplementary information (OSI), special service information (SSI) and special service request (SSR) information, to the extent that it contains any information capable of identifying a natural person; and

e) any collected advance passenger processing (APP) or advance passenger information (API) data to the extent that it contains any information capable of identifying a natural person.

3. Notwithstanding paragraph 1, 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. PNR data may be retained until the relevant investigation or prosecution is concluded or the penalty enforced.

4. Upon the expiry of the data retention period specified in paragraphs 1 and 3, PNR data shall be permanently deleted.

Article 17

Logging and documentation of PNR data

1. All processing, including accessing and consulting or transfer of PNR data as well as requests for PNR data by the authorities of Australia or third countries, even if refused, shall be logged or documented 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.

2. Logs or documentation prepared under paragraph 1 shall be used only for oversight and auditing purposes including investigation and resolution of matters pertaining to unauthorised access.

3. Logs or documentation prepared under paragraph 1 shall be communicated on request to the Australian Information Commissioner. The Australian Information Commissioner shall use this information only for the oversight of data protection and for ensuring proper data processing as well as data integrity and security.

Article 18

Sharing PNR data with other government authorities of Australia

1. The Australian Customs and Border Protection Service may share PNR data only with those government authorities of Australia which are listed in Annex 2 and only pursuant to the following safeguards:

a) Receiving government authorities shall afford to PNR data the safeguards as set out in this Agreement.

b) Data shall be shared strictly for the purposes stated in Article 3;

c) Data shall be shared only on a case-by-case basis unless the data has been depersonalized;

d) Prior to the sharing, the Australian Customs and Border Protection Service shall carefully assess the relevance of data to be shared. Only those particular PNR data elements which are clearly demonstrated as necessary in particular circumstances shall be shared. In any case, the minimum amount of data possible shall be shared.

e) Receiving government authorities shall ensure that the data is not further disclosed without the permission of the Australian Customs and Border Protection Service, which

permission shall not be granted by the Australian Customs and Border Protection Service except for the purposes stated in Article 3 of the Agreement.

2. The list of authorities set forth in Annex 2 may be amended by exchange of diplomatic notes between the Parties, to include:

a) any successor departments or agencies of those which are listed in Annex 2; and

b) any new departments and agencies established after the entry into force of this Agreement whose functions are directly related to preventing, detecting, investigating or prosecuting terrorism or serious transnational crime; and

c) any existing departments and agencies whose functions become directly related to preventing, detecting, investigating or prosecuting terrorism or serious transnational crime.

3. When transferring analytical information containing PNR data obtained under this Agreement, the safeguards applying to PNR data in this Article shall be respected.

4. Nothing in this article prevents the disclosure of PNR data where necessary for the purposes of Article 3 (4) and (5) and Article 10.

Article 19

Transfers to authorities of third countries

1. The Australian Customs and Border Protection Service may transfer PNR data only to specific third country authorities pursuant to the following safeguards:

a) The Australian Customs and Border Protection Service is satisfied that the receiving third country authority has agreed to afford to the data transferred the same safeguards as set out in this Agreement;

b) Only a third country authority whose functions are directly related to preventing, detecting, investigating and prosecuting terrorist offences or serious transnational crime may receive PNR data;

c) Data shall be transferred for the exclusive purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious transnational crime as defined in Article 3;

d) Data shall be transferred only on a case-by-case basis;

e) Prior to the transfer, the Australian Customs and Border Protection Service shall carefully assess the relevance of data to be transferred. Only those particular PNR data elements which

are clearly demonstrated as necessary in particular circumstances shall be transferred. In any case, the minimum amount of data possible shall be transferred;

f) Where the Australian Customs and Border Protection Service is aware that data of a citizen or a resident of a Member State is transferred, the competent authorities of the concerned Member State shall be informed of the matter at the earliest appropriate opportunity;

g) the Australian Customs and Border Protection Service is satisfied that the receiving third country authority has agreed to retain PNR data only until the relevant investigation or prosecution is concluded or the penalty enforced or are no longer required for the purposes set out in Article 3(4), and in any case no longer than necessary;

h) the Australian Customs and Border Protection Service is satisfied that the receiving third country authority has agreed not to further transfer PNR data;

i) The Australian Customs and Border Protection Service shall ensure, where appropriate, that the passenger is informed of a transfer of his or her PNR data.

2. When transferring analytical information containing PNR data obtained under this Agreement, the safeguards applying to PNR data in this Article shall be respected.

3. Nothing in this article prevents the disclosure of PNR data where necessary for the purposes of Article 3 (4).

CHAPTER III

MODALITIES OF TRANSFERS

Article 20

The method of transfer

For the purpose of this Agreement, the Parties shall ensure that air carriers transfer to the Australian Customs and Border Protection Service PNR data exclusively on the basis of the push method and in accordance with the following procedures:

a) Air carriers shall transfer PNR data by electronic means in compliance with technical requirements of the Australian Customs and Border Protection Service or, in case of technical failure, by any other appropriate means ensuring an appropriate level of data security.

b) Air carriers shall transfer PNR data using an agreed messaging format.

c) Air carriers shall transfer PNR data in a secure manner using common protocols required by the Australian Customs and Border Protection Service.

Article 21

The frequency of transfer

1. The Parties shall ensure air carriers transfer to the Australian Customs and Border Protection Service all requested PNR data of passengers as described in Article 20 at a maximum of five scheduled points in time per flight, with the first point being up to 72 hours before scheduled departure. The Australian Customs and Border Protection Service shall communicate to air carriers the specified times for the transfers.

2. In specific cases where there is an indication that early access is necessary to respond to a specific threat related to terrorist offences or serious transnational crime, the Australian Customs and Border Protection Service may require an air carrier to provide PNR data prior to the first scheduled transfer. In exercising this discretion, the Australian Customs and Border Protection Service shall act judiciously and proportionately and use exclusively the push method.

3. In specific cases where there is an indication that access is necessary to respond to a specific threat related to terrorist offences or serious transnational crime, the Australian Customs and Border Protection Service may require an air carrier to transfer PNR data in between or after regular transfers referred to in paragraph 1. In exercising this discretion, the Australian Customs and Border Protection Service shall act judiciously and proportionately and use exclusively the push method.

CHAPTER IV

IMPLEMENTING AND FINAL PROVISIONS

Article 22

Non-derogation/Relationship to other instruments

1. This Agreement shall not create or confer any right or benefit on any person or entity, private or public. Each Party shall ensure that the provisions of this Agreement are properly implemented.

2. Nothing in this Agreement shall limit rights or safeguards contained in the laws of Australia.

3. Nothing in this Agreement shall derogate from existing obligations under any bilateral mutual legal assistance instruments between Australia and Member States of the European Union to assist with a request to obtain data for evidence in criminal proceedings concerning terrorism or serious transnational crime.

Article 23

Dispute resolution and suspension of the Agreement

1. Any dispute arising from the interpretation, application or implementation of this Agreement and any matters related thereto shall give rise to consultation between the Parties with a view to reaching a mutually agreeable resolution, including providing an opportunity for either Party to comply within a reasonable time.

2. In the event that consultations do not result in a resolution of the dispute, either Party may suspend the application of this Agreement by written notification through diplomatic channels, with any such suspension to take effect 120 days from the date of such notification, unless otherwise agreed.

3. Any suspension shall cease as soon as the dispute is resolved to the satisfaction of Australia and the EU.

4. Notwithstanding any suspension of this Agreement, all data obtained by the Australian Customs and Border Protection Service under the terms of this Agreement shall continue to be processed in accordance with the safeguards of this Agreement, including the provisions on retention and deletion of data.

Article 24

Consultation and review

1. The Parties shall notify each other, where appropriate before adoption, of any legislative or regulatory changes which may materially affect the implementation of this Agreement. References in this Agreement to Australian legislation shall be deemed to include any successor legislation.

2. The Parties shall jointly review the implementation of this Agreement and any matters related thereto one year after the entry into force of this Agreement and regularly thereafter within the duration of this Agreement and additionally as requested by either Party. The Parties agree that the review should in particular look into the mechanism of masking out data according to Article 16(1)(b), any difficulties related to the operational efficiency or cost effectiveness of the mechanism, and experience acquired with similar mechanisms in other mature PNR schemes, including the EU scheme. In the event that an operationally efficient and cost effective mechanism is not available, access to the data will instead be restricted by archiving, and may be accessed only in the way that depersonalized data is accessed under Article 16.

3. The Parties shall agree in advance of the joint review its modalities and shall communicate to each other the composition of their respective teams. For the purpose of the joint review, the European Union shall be represented by the European Commission and Australia shall be represented by the Australian Customs and Border Protection Service. The teams may include experts on data protection and law enforcement. Subject to applicable laws, any participants to the joint review shall be required to respect confidentiality of the discussions and have appropriate security clearances. For the purpose of the joint review, the Australian Customs and Border Protection Service shall ensure access to relevant documentation, systems and personnel.

4. The Parties shall evaluate the Agreement, in particular its operational effectiveness no later than four years after its entry into force.

5. Following the joint review, the European Commission shall present a report to the European Parliament and to the Council of the European Union. Australia shall be given an opportunity to provide written comments which shall be attached to the report.

6. Since the establishment of an EU PNR system could change the context of this Agreement, if and when an EU PNR system is adopted, the Parties shall consult to determine whether this Agreement would need to be adjusted accordingly.

Article 25

Termination

1. Either Party may terminate this Agreement at any time by written notification through diplomatic channels. Termination shall take effect 120 days from the date of receipt of such notification, or as otherwise agreed.

2. Notwithstanding any termination of this Agreement, all data obtained by the Australian Customs and Border Protection Service under the terms of this Agreement shall continue to be processed in accordance with the safeguards of this Agreement, including the provisions on retention and deletion of data.

Article 26

Duration

1. Subject to Article 25, this Agreement shall remain in force for a period of seven years from the date of entry into force.

2. Upon the expiry of the period set forth in paragraph 1, as well as any subsequent period of renewal under this paragraph, the Agreement shall be renewed for a subsequent period of seven years unless one of the Parties notifies the other in writing through diplomatic channels, at least twelve months in advance, of its intention not to renew the Agreement.

3. Notwithstanding the expiration of this Agreement, all data obtained by the Australian Customs and Border Protection Service under the terms of this Agreement shall continue to be processed in accordance with the safeguards of this Agreement, including the provisions on retention and deletion of data.

Article 27

PNR data received prior to the entry into force of this Agreement

Australia shall treat any PNR data held by the Australian Customs and Border Protection Service at the time of the entry into force of this Agreement in accordance with the provisions of this Agreement. However, no data shall be required to be masked out before 1 January 2015.

Article 28

Territorial application

1. Subject to paragraphs 2 to 4, this Agreement shall apply to the territory in which the Treaty on European Union and the Treaty on the Functioning of the European Union are applicable and to the territory of Australia.

2. This Agreement will only apply to Denmark, the United Kingdom or Ireland, if the European Commission notifies Australia in writing that Denmark, the United Kingdom, or Ireland has chosen to be bound by this Agreement.

3. If the European Commission notifies Australia before the entry into force of this Agreement that it will apply to Denmark, the United Kingdom or Ireland, this Agreement shall apply to the territory of such State on the same day as for the other EU Member States bound by this Agreement.

4. If the European Commission notifies Australia after the entry into force of this Agreement that it applies to Denmark, the United Kingdom, or Ireland, this Agreement shall apply to the territory of such State on the first day following receipt of the notification by Australia.

Article 29

Final Provisions

1. This Agreement shall enter into force on the first day of the month after the date on which the Parties have exchanged notifications indicating that they have completed their internal procedures for this purpose.

2. This Agreement replaces the Agreement between the European Union and Australia on the Processing and Transfer of European Union – Sourced Passenger Name Record (PNR) Data by Air Carriers to the Australian Customs Service done at Brussels on 30 June 2008, which will cease to apply upon the entry into force of this Agreement.

Done at..., on...; in two originals, in the English language. This Agreement shall be also drawn up in the Bulgarian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish languages, each version being equally authentic. In case of divergence between the language versions, the English version shall prevail.

FOR THE EUROPEAN UNION

++++++++++

FOR AUSTRALIA

++++++++++

Annex 1

PNR data elements referred to in Article 2 f) which air carriers are required to provide to the Australian Customs and Border Protection Service but only to the extent they already collect them:

1. PNR record locator code
2. Date of reservation/issue of ticket
3. Date(s) of intended travel
4. Name(s)
5. Available frequent flier and benefit information (i.e. free tickets, upgrades, etc.)
6. Other names on PNR, including number of travellers on PNR
7. All available contact information (including originator information)
8. All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)
9. Travel itinerary for specific PNR
10. Travel agency/travel agent
11. Code share information
12. Split/divided information
13. Travel status of passenger (including confirmations and check-in status)
14. Ticketing information, including ticket number, one-way tickets and Automated Ticket Fare Quote
15. All baggage information
16. Seat information, including seat number
17. General remarks including OSI, SSI and SSR information
18. Any collected APIS information
19. All historical changes to the PNR listed in numbers 1 to 18

Annex 2

List of other government authorities of Australia with whom the Australian Customs and Border Protection Service is authorised to share PNR data:

1. Australian Crime Commission;
2. Australian Federal Police;
3. Australian Security Intelligence Organisation;
4. Commonwealth Director of Public Prosecutions;
5. Department of Immigration and Citizenship;
6. Office of Transport Security, Department of Infrastructure and Transport.