10031/03/EN
WP 85

Opinion 1/2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines

Adopted on 16th January 2004

OPINION 1/2004 OF THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

On the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1], and in particular Articles 29 and 30 paragraph 1 (b) thereof,

Having regard to the Rules of Procedure of the Working Party[2], and in particular Article 12 and 14 thereof,

Whereas:

The Government of Australia requested[3] the Commission to find that Australia ensures an adequate level of protection for the transmission of Passenger Name Record data (hereafter 'PNR') from airlines within the meaning of Article 25 of the Directive,

The European Commission sought the Opinion of the Working Party in this regard,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

Australian border protection legislation empowers Australian Customs to risk assess international airlines' Passenger Name Record (PNR) data prior to passenger arrival in Australia. This legislation aims at enhancing the security of the Australian border and serves in particular to implement the Government's 2001 election programme to increase national security.

Customs access to, use and disclosure of PNR data to any third party is regulated in Australian Law by the Customs Act 1901, the Customs Administration Act 1985, the Privacy Act 1988 and an Undertaking by Customs to Parliament with respect to PNR data non-retention.

---

1 OJ L 281, 23.11.1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 Adopted by the Working Party at its third meeting held on 11.9.1996.

3 Meeting between Australian FM Downer and EU Commissioner Patten on 26 January 2003. Repeated at the meeting between Australian Attorney General Williams and EU Commissioner Bolkestein on 1 October 2003 and at the Ministerial Troika meeting held in Rome on 2 October 2003.

Airlines are under an obligation to provide Customs with access to certain of the PNR data they hold. Compliance with the Australian requirements by the airlines may create problems in respect of Directive 95/46/EC on data protection. The Commission has thus entered into negotiations with Australia in order to establish the conditions that would allow it to adopt a decision recognising adequate protection on the basis of Article 25(6) of Directive 95/46/EC. The Commission has updated the Working Party on these negotiations. In particular, the Working Party has received from the Commission a document containing the Australian Customs' Undertaking to the Australian (Federal) Parliament in relation to access to airline passenger information and non-retention of such information, as well as the Senate's findings in relation to this issue.[4]

The Working Party notes that the transfer of PNR data by airlines to authorities outside the European Union raises public concern and has broad and sensitive implications in international, political and legal terms. In order to meet these concerns a full picture of the relevant Australian regulatory framework should be included as an annex to any Commission Decision. The Working Party also recommends that in the Commission Decision a provision should be made for a mechanism that ensures that any change in the relevant legislation is communicated to the Commission.

2. AUSTRALIAN LAW ON PASSENGER NAME RECORD DATA

The Working Party notes the explanations provided by the Australian Government on this issue. According to these, the Australian Law on PNR data covers the following situations:

- ***The Customs Act 1901 as amended***

Schedule 7 of the Border Security Legislation Amendment (Terrorism) Act 2002, amending the Customs Act 1901 (hereafter "the Customs Act") was implemented on 2 August 2002 and authorises Customs to obtain airline passenger information on the request of the Chief Executive Officer of Customs (hereafter "the CEO"). In this respect Section 64AF of the Customs Act makes it mandatory for the operator of an international passenger air service to provide Customs with access to PNR data if requested to do so by the CEO. Section 64AF Clause (1) (a) states that the request from the CEO to an airline operator for access to passenger information is done in a "particular manner and form". Once the request is executed by the CEO, it becomes a formal legal instrument that on receipt by an operator becomes the binding requirement for provision of passenger data.

The Working Party notes that the obligation to provide access must be complied with even though the information concerned is personal information as defined in Australia's Privacy Act 1988. Section 273GAB of the Customs Act authorises disclosure of passenger data to Customs even if the information is personal information as defined in the Privacy Act and such disclosure would otherwise be regulated by the Privacy Act.

The Working Party notes that, by imposing a penalty for non-compliance, the Australian government has determined its intent that the CEO is required to exercise the power prescribed by Section 64AF. The CEO has no discretion regarding exemption of any airline from application of Section 64 AF. However, this section allows the CEO

[4] Reply from Australia of November 2003 to issue raised during a video conference held on 27 October 2003 between representatives of the Commission and the Australian Government.

discretionary power in respect to timing of the request and for prescribing the "particular manner and form" of access to the operators' passenger information.

According to the Australian authorities the "manner and form" of the request is a legally binding document that prescribes the detail of system access and data provision.

- ***The Customs Administration Act 1985***

Section 16 of the Customs Administration Act 1985 (hereafter "the Customs Administration Act") regulates the recording and disclosure *of "protected information"*. Any PNR data that is accessed by Customs is "protected information" within the meaning of this section and recording and disclosure of this information will have to be undertaken in accordance with this section. Protected information *"means information that directly or indirectly comes to the knowledge of, or in the possession of, a person while he or she is performing his or her duties (whether the information is related to those duties or not)."*

The Customs Administration Act prohibits the unauthorised recording and disclosure of certain information held by Customs, provides for exceptions in relation to the prohibition and makes particular provision in relation to the authorised disclosure of *"personal information"*. [5] The Customs Administration Act takes as its starting point the prohibition to record or disclose protected information unless so authorised by Section 16, or as required or authorised by any other law or in the course of performing the person's duties.[6]

The Customs Administration Act applies to the CEO as well as to a limited group of officials defined in its subsection 1AA.

- ***The Privacy Act 1988***

The Commonwealth Government enacted a Privacy Act in 1988, the so-called Commonwealth Privacy Act 1988 (hereafter "the Privacy Act"). This Act primarily covers the activities of Federal Government departments and agencies, subjecting them to a set of Information Privacy Principles (hereafter "IPPs") based on the 1980 OECD Guidelines governing the protection of privacy and transborder flows of personal data, under the supervision of a Privacy Commissioner.[7] As a Commonwealth Government agency, Customs is subject to the public sector provisions of the Privacy Act (see Annex A containing a summary of this Act). Most of the IPPs apply to records containing personal information, but not to the information itself. The Working Party understands that the definition of record confirms that databases for example are covered by the Privacy Act.

The Working Party notes that any PNR information that is retained by Customs is also *"personal information"* within the meaning and for the purpose of the Privacy Act 1988. Customs is therefore obliged to handle information in accordance with this Act, including in relation to the collection, use, retention and dissemination of any such data.

---

5 "Personal information" as defined in the Privacy Act 1988 to which subsection 1A of the Customs Administration Act refers.

6 Section 16, subsection 2.

7 Set out in Section 14 of the Act. See also http://www.privacy.gov.au/

The IPPs place obligations on Commonwealth Government agencies to deal with personal information appropriately in the following areas:

- collection and solicitation of personal information (IPPs 1 to 3);
- storage and security (IPP 4);
- identification of personal information held (IPP 5);
- access by an individual to his personal information (IPP 6);
- rights of correction (IPP 7);
- a requirement that personal information be accurate, up to date and complete (IPP 8);
- a requirement that personal information should be used only for a relevant purpose (IPP 9);
- limitations on the use of personal information (IPP 10), and
- limitations on the disclosure of personal information (IPP 11).

According to the Australian Government, the Privacy Commissioner conducts audits of Commonwealth government agencies to ensure their compliance with the IPPs. According to the same Government, Customs has put in place formal processes for audit of access to passenger information by both the Privacy Commissioner and Customs Internal Audit. A proposal to amend the Privacy Act to allow the Privacy Commissioner to conduct an audit of Customs to ensure the non-retention of identifiable PNR data is being put to the Attorney General for his consideration.

3. OPERATION AND FEATURES OF THE CUSTOMS PNR ACCESS ARRANGEMENTS

The Working Party notes the explanations provided by the Australian authorities on this issue. According to these, Customs PNR access arrangements consist of the following features and operate in the way described below.

- ***Processing and retention of PNR data***

Access to PNR data through SITA is described in an Annex to this Opinion, which forms part of the present Opinion. The PNR accessed does not include historical data, but only PNR for current flights.

The first stage of processing of PNR data by Customs consists of an automated risk assessment using a software interrogation system. This means that certain data contained in airline PNR (passenger reservation and check-in data) are subjected to automated profile analysis software. This software screens out 95% to 97% of passengers on average on a particular flight whose PNR is assessed as not conforming to a risk profile. The PNR of these passengers is not viewed or downloaded by Customs and there is no further action in respect of accessing or assessing their PNR.

The first time a human intervention takes place is when Customs officers review the PNR data of the remaining 3% to 5% of passengers (on average on a particular flight) selected by the automated profile analysis software. The PNR of these passengers is visually examined by a Customs officer assigned to the Passenger Analysis Unit ("PAU") located in Canberra who undertakes a threat analysis. If, after further analysis there remains sufficient reason to consider the passenger a risk, he or she may be referred for interception on arrival at the Australian border. This sub-set accounts for 0.05% to 0.1% of passengers on average on a particular flight. Customs at the border (airport) make a further and final determination of whether to intercept the passenger.

Regarding retention of PNR data, there is no statutory obligation on Customs to retain PNR data. Likewise there is no statutory prohibition on Customs to store these data. The PNR data of passengers assessed via the automated profile analysis software and assessed as low risk (95% to 97% of passengers) are not retained and no record is kept of their PNR information. So Customs applies a general policy of non retention for these data.

For those 0.05% to 0.1% of passengers who are referred to Customs for further evaluation, the airline PNR data are temporarily retained, but not stored, pending resolution of the border evaluation. After resolution, their PNR data are erased from the PC of the Customs PAU officer concerned and are not entered into Australian databases.

Customs will retain personal data that is accessed from the PNR, only if the passenger has committed an offence against a border protection Act administered by Customs. Where an offence is alleged, the data will be temporarily held during investigation of the alleged offence. If the investigation does not result in prosecution or no offence is proven, the PNR data are destroyed.

The policy of non-retention of PNR data as described above is embedded in an undertaking made by Customs to the Australian (federal) Parliament at the time the Senate Legal and Constitutional Legislation Committee made inquiries into the Security legislation Amendment (Terrorism) Bill 2002 (No 2) and related Bills.[8] In seeking the agreement of the Australian Parliament to compel airlines to disclose PNR data through legislation and in recognition of the Federal Privacy Commissioner's concerns about storage of personal data, Customs made the following undertaking to the Parliament in which they gave assurance on not storing PNR data: "*Customs does not retain or store any passenger information unless the passenger has been identified undertaking an illegal activity or the information is needed as intelligence to assist in investigation of a suspected offence*."[9] The Senate committee's findings and Parliament's expectations of Customs in relation to access to PNR data are reflected in paragraphs 4.80 through 4.87 of the committee's report of May 2002.

According to the explanations given by the Australian authorities, this undertaking is of a binding nature. Regardless of whether the CEO of Customs or the Minister changes, a breach of the undertaking would occur if the conditions were altered. The CEO is therefore bound to observe this commitment as otherwise he would be in contempt of Parliament by acting contrary to the intent of Section 64 AF. On the basis of this undertaking Customs has developed stringent operational procedures that govern the use of PNR data which specifically prevent data retention. Likewise, the computer system that is used for PNR analysis has been built so as to not have the capability to retain the data.

The Working Party understands that the Australian system prevents a general and prolonged storage and subsequent processing of PNR data and notes the explanations and assurances provided by the Australian Government. As mentioned earlier, a passenger's PNR data are retained only when a passenger is found to have committed an offence against a border protection Act administered by Customs. Where an offence is alleged, the data will be temporarily held during investigation of the alleged offence. If the

[8] Reply from Australia of November 2003, page 2.
[9] Reply from Australia of June 2003, pages 9-10; reply from Australia of November 2003, page 10.

investigation does not result in prosecution or no offence is proven, the PNR data are destroyed. In all other cases no record is kept of the PNR information. In addition, Customs no longer has access to any data for a particular flight after it is deleted from the airlines' systems – 24 to 48 hrs. after the landing of the flight. Thus, from the perspective of data protection, the Working Party notes that this system presents an important and fundamental difference compared with the US approach, where PNR data are downloaded from the airlines databases and stored in a separate database for subsequent processing.

The Working Party also notes that the Australian system involves systematic communication of PNR data from airlines to the Australian authorities. At the same time, each communication from an airline concerns a particular flight only and each PNR created for such a flight is specific to that flight. Thus, the PNR accessed does not include historical data. The Working Party therefore bases its position on the interaction between systematic communication of PNR data, the fact that such data are specific to each flight and the general policy of non-retention of PNR data applied by the Australian authorities.

- ***Customs purpose for accessing PNR data***

The Working Party notes that according to the Australian authorities, Customs' purpose for accessing passenger's PNR data is "*to implement the Australian government's decision that all PNR data of passengers on flights to or from Australia be assessed in order that border protection is improved through identification of those passengers who may pose a threat of terrorism or related criminal activity*."[10] Access is restricted to those flights defined as Australian International Flights in Section 64 AF Clause (6) of the Customs Act, i.e. those flights involving travel to, through or departure from Australia.[11]

- ***PNR data elements accessed***

The PNR data that are collected for processing by Customs consists of information contained in the airline Passenger Name Record held in various areas of the Reservation and Check-in components of the airline Computer Reservation System (hereafter "the CRS") for an individual on a flight to or from Australia.[12]

According to the Australian authorities, the initial computer-based scanning of passenger data focuses on a limited group of PNR data elements, i.e. 18 PNR data elements. Of those elements none focuses on sensitive data which Customs agree may be filtered out, or on data like frequent flyer data.

The Working Party assessed the 18 PNR data elements used by Customs automated profile analysis software system against the PNR data elements listed in its Opinion 4/2003 of 13 June 2003.[13] The Working Party notes that out of the 18 PNR data elements, 7 PNR data elements[14] do not form part of the PNR data elements considered

---

10 Reply from Australia of November 2003, page 1.
11 Reply from Australia of May 2003, Issue 3, pages 3 and 4.
12 Attachment D to the reply from Australia of November 2003.
13 Page 8 of this opinion.
14 All forms of payment information (without details thereof); travel agency; travel agent; code share information; split/divided PNR information; OSI information and SSR information.

not excessive in its Opinion 4/2003. Moreover, 4 PNR data elements[15] have not been assessed earlier by the Working Party.

If, as a result of the automated profile analysis, a passenger is assessed as a possible risk, further PNR data elements may be inspected by a authorised Customs officer; 5 of these elements[16] do not form part of the data elements considered not to be excessive in the abovementioned Opinion, 2 data elements[17] have not been assessed by the Working Party in its Opinion 4/2003.

The Working Party notes that Customs may assess the entire PNR including sensitive data in cases of suspicion of high risk. This may occur for 0.05% to 0.1% of passengers (on average on a particular flight) selected by the automated profile software as presenting a possible risk.

- ***Manner and Form of access to PNR data***

Custom's automated risk assessment software access to the PNR data elements identified above is permitted in so far as it is being conducted in a particular manner and form referred to in Section 64AF clause (1) (a) of the Customs Act and described in a special Manner and Form document. According to the Australian authorities, any other form of access is unlawful under Australian law. In addition to the Manner and Form Document, a System Access Arrangement document describes the procedures allowing the management of Customs' access to airline passenger information in accordance with the Customs Act, the Customs Administration Act and the Privacy Act.

The manner of access is described as a continuous, real time, on-line electronic access to the CRS components of the airline's computer system or systems used to store passenger information.

Access is read-only (also specified in Clause 2.3 under c of the System Access Arrangement providing for Customs' access to airlines passenger information) and is available only to limited number of Customs officials authorised by the CEO. The access rights are provided by the airline.

The form of access specifies Custom specially designed computer software. This software resides on a Customs computer system that is connected to the airline's system via a network called SITA. The technical process for accessing PNR information through SITA is described in a technical annex to this opinion.

- ***Initial recipient of PNR data***

The Working Party notes that Customs is the only administration that accesses the PNR data transmitted by airlines. Access in Customs is restricted to a small group of officers assigned to the Passenger Analysis Unit located in Customs headquarters at Canberra. Before accessing passengers' information each officers must be authorised by instrument

---

The PNR data considered not excessive are dates of reservation; dates of intended travel; all travel initerary for specific PNR; no show history; number of bags; bag tag numbers and go show.

15 Ticket issue city; nationality; year of birth and ticket purchase date.

16 Number of travellers on PNR; seat information; contact telephone number; travel status; general remarks and collected apis/api.

17 Date of birth and travellers full name.

of the CEO of Customs under subsection 64AF(1) of the Customs Act. This subsection states that the operator of an international passenger air service receives a request from the CEO to allow authorised officers ongoing access to the operator's passenger information. The Manner and Form document specifying access to airline passenger information states that "*the Chief Executive Officer of Customs will authorise a number of officials who occupy certain positions to access your system. Details of officers filling these positions will be communicated to you by means of the registration/application form for a user login code and password that you have provided.*"

Reference to 'authorised officers' is also made in the System Access Arrangement specifying the computer system access arrangements between Customs and airlines. It states that only authorised officers from Customs can access the airline's system (clause 2.2) while it also mentions that Customs will notify the airline concerned who the authorised officers are and indicates that access to the airline computer system is restricted to those authorised officers (or nominated computer addresses used for automated system access and PNR information analysis) (clause 2.3).

- ***Onward transfers***

PNR data accessed by Customs may be provided to certain third parties only in the following circumstances:

a) Where Customs is required by order of a court of law to disclosure information to the court.

b) To the Australian Federal Police (hereafter "the AFP") for further investigation and prosecution of an offence under Australian law, where a person who has arrived at the Australian border is alleged by Customs to have committed an offence. Customs does not pass the entire PNR to the AFP but may provide in some circumstances specific data that led to the passengers' apprehension. Access to credit card and telephone records may only be given on the basis of a search warrant.

Under ministerial arrangements between Customs and the AFP, all major offences (e.g. terrorism and drug importations that are encountered by Customs at the border) are passed by Customs to the AFP for investigation and prosecution.

The AFP, being a Commonwealth government agency, is subject to the Privacy Act. IPP 11 of this Act specially provides that an agency which receives information from Customs shall not use or disclose the information for a purpose other than the purpose for which the information was given to the agency.

In addition, Section 60A of the Australian Federal Police Act 1979 imposes a secrecy obligation on all members of the AFP. Under this section, current and former members of the AFP must not directly or indirectly record or disclose information obtained in the course of their duties except as authorised by the section, as required by any other law or in the course of performing their duties as a member of the AFP. A breach of Section 60 attracts a penalty of imprisonment for a period of up to 2 years.

With regard to the onward transfer of PNR data, Customs is subject to the IPP 11 as set out in Section 14 of the Privacy Act. This IPP imposes specific restrictions on the disclosure of personal information. A record-keeper (similar to a data controller within

the meaning of the Directive), shall not disclose personal information for a secondary purpose subject to some specified exceptions. These include: the consent of the individual concerned, the disclosure is required or authorised by law and for a purpose reasonably necessary for enforcement of the criminal law, a law imposing a pecuniary penalty or the protection of the public revenue.

In addition, Customs officers who are authorized to access passenger information are bound by the requirements of Section 16 of the Customs Administration Act 1985, which contains rules on record and disclosure of protected information such as PNR data.

According to the Australian authorities, there are no other provisions for personal data to be passed to third parties.[18]

- ***Security***

According to the Australian authorities multiple layers of security have been installed in relation to access to PNR data.

The safeguards include limiting access to only a small group of authorised Customs offices. Furthermore, comprehensive physical and electronic securities measures have been taken that isolate passenger information from the general Customs environment. In this respect the most important measures are the following. Airline information is viewed via a dedicated LAN that is isolated physically and electronically from all other Customs systems. The workstations located in the Passenger Analysis Unit of Customs are in a secured, limited access computer space. There are three layers of login ID/passwords needed to access the airline information, i.e. LAN access, PNR analysis software access and airline provided system access (e.g. airline sonic ID/password). According to representatives from the network provider SITA, the Australian system is not linked to the flow of data for visa control by Customs officials outside the PAU and the two flows of data are insulated from each other. The Australian authorities have confirmed that APIS data for visa control is kept entirely separate from the flow of PNR data.

- ***Sensitive data***

According to the Australian Government all personal information is accorded an equal level of protection by Customs, which does not profile against sensitive data (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or data concerning health)[19].

- ***Information***

In order to inform passengers adequately, the Working Party stresses that they should be clearly and precisely informed about their rights, in particular their right of access, rectification and the available redress mechanisms. Ideally such information should be available when a ticket is purchased.

- ***Right of access and rectification***

[18] Reply from Australia of May 2003, Issue 1, page 2.
[19] Ibidem, Issue 10, page 7.

As Customs is subject to the Privacy Act, it is required to handle PNR data in conformity with the IPPs 6 and 7 which provide explicit rights of access, rectification and objection.

IPP 6 provides that an individual has a right of access to his or her personal information except to the extent that a record-keeper is authorised or required by a law, which itself provides for access to documents, to refuse to provide access. These laws are the Freedom of Information Act 1982 (the FIO) and the Archives Act 1983. The FIO obliges an agency to release requested documents (whether or not they contain personal information) to a member of the public who requires them unless those documents fall within certain exceptions categories. The Archives Act provides that records more than 30 years old held by the National Archives of Australia are open to public access.

IPP 7 enables an individual in case a record-keeper is not willing to amend a record, to require the record-keeper to take reasonable steps to attach a statement in respect of that.

The Working Party notes that PNR data are only stored in cases where an offence has been committed against the border protections Acts administered by Customs or during investigation of a suspected offence against these Acts. In addition to the statutory rights mentioned above, a person charged with an offence may seek access to information held about them throughout the court process in order to assist in the defence case.

- ***Enforcement mechanisms***

The Privacy Act establishes the independent Office of the Federal Privacy Commissioner. The Privacy Commissioner[20], appointed as a statutory officer[21], has a statutory obligation to investigate complaints from individuals about interference with privacy under the Privacy Act and related legislation. The Privacy Commissioner is appointed for fixed terms. In order to guarantee his independence, he/she can only be removed from office on very serious grounds such as misbehaviour or incapacity.

The Working Party notes that under Section 52 of the Privacy Act, the Privacy Commissioner can make determinations declaring that certain practices are an interference with privacy and that they should cease; that the respondent should redress any loss or damage suffered by the complainant and that the latter is entitled to a specified amount of money as compensation. Sections 58 to 60 of the Privacy Act oblige agencies to comply with the terms of a Section 52 determination. Should an agency not comply with a determination, either the complainant or the Privacy Commissioner may commence proceedings in a federal court to enforce it.

At present, subsection 41(4) of the Privacy Act restricts the Privacy Commissioner's ability to investigate complaints from non-Australian citizens or residents in relation to IPP 7 (rectification). This is currently under review with a view to have this restriction taken away. The Working Party notes that there is no limitation on the Privacy Commissioner's ability to investigate complaints from non-Australian citizens or residents in relation to any of the other IPPs.

In addition, the Working Party notes that all passengers have the right to complain to the Commonwealth Ombudsman regarding the treatment by Customs during Border processing on the basis of the Ombudsman Act 1976.

---

[20] Part V.

[21] Part IV Division 1.

4. THE SCOPE OF THE PRESENT OPINION

The scope of the present Opinion concerns the protection of fundamental rights and freedoms regarding the processing of personal data in the context of PNR data transferred from airlines to Australian authorities in relation to those flights defined as Australian International Flights in Section 64 AF Clause (6) of the Customs Act, i.e. those flights involving travel to, through or departure from Australia.

This Opinion is given by the Working Party after having assessed the adequacy of the level of protection provided for by Australia of Passenger Name Record data from airlines. This protection is provided together by the Australian Customs Act 1901, the Customs Administration Act 1985, the Privacy Act 1988 and Customs Undertaking to Parliament as described above. The present Opinion is thus issued with reference to the level of protection ensured by Australia after the requested transmission by airlines of personal data concerning their passengers and crewmembers on the basis of the above-mentioned laws and Customs Undertaking to Parliament. In particular, the Working Party has taken into account the explanations and assurances given by the Australian authorities as to how the provisions of these Acts as well as Customs Undertaking to Parliament are to be interpreted and as to what situations fall within the scope of these Acts and Undertaking.

The Working Party also notes that the Australian system access arrangements through SITA can best be qualified as "pull". The present Opinion is therefore given on the basis of the current understanding as described in the Annex to this Opinion of how the system access arrangements through SITA work.

The present Opinion is also given on the condition that the restriction laid down in subsection 41(4) of the Privacy Act as regards the Privacy Commissioner's ability to investigate complaints from non-Australian citizens or residents in relation to IPP 7 (rectification) will be taken away.

The Working Party also reserves the general right to supplement the present Opinion by a further opinion should this Opinion not be adequately taken into account or if substantial changes in the legislation are made in the course of future negotiations.

Additionally, if the guarantees provided by the Australian administration are not correctly implemented, re-evaluation of the situation will be necessary. For this reason, it is essential that the Commission submits a regular report on the actual use of the data and implementation of the protection in Australia. This should allow for the verification of the conditions of processing in Australia, to ensure that the underlying assumptions, which justified the Commission's decision, still hold well.

5. TRANSITIONAL NATURE OF THE ADEQUACY FINDING

The scope of data flows is related to recent serious circumstances at the international level. The Working Party recommends that periodical re-evaluations of the situation shall be made to assess if the necessity for such flows remains. Should the international circumstances alter, it would be necessary to review the situation. The Working Party recommends the Commission to include clauses in its decision providing for 'sunset' limitation and review the situation after 3 years in any event.

6. RESULTS OF THE ASSESSMENT

The Working Party stresses that, in order to carry out the present assessment on the Australian Law on PNR data, the Australian Government has provided information on how the relevant provisions of the Customs Act 1901, the Customs Administration Act 1985, the Privacy Act 1988 and Customs Undertaking to Parliament are to be interpreted, and has given assurances that the Australian rules on PNR data are being implemented in line with such interpretation. The Working Party has therefore based its analysis upon such information and assurances of the Australian Government, and this Opinion is thus dependent on these elements provided by the Australian Government being confirmed in the actual implementation of the rules on PNR data in Australia. In particular, as regards the scope of the Australian Law on PNR data, the Working Party has taken into account the explanations and assurances given by the Australian Government as to how the relevant provisions of the Customs Act 1901, the Customs Administration Act 1985 and Customs Undertaking to Parliament are to be interpreted and as to what situations fall within the scope of the Privacy Act 1988. Furthermore, the Working Party has based its position on the interaction between the PNR data elements accessed by the Australian Customs service, the purpose for accessing these data and the general policy of non-retention thereof. According to the Working Party this interaction has led to a globally balanced approach by the Australian authorities. The present Opinion is also given on the condition that the Australian authorities proceed with a review of subsection 41(4) of the Privacy Act, which restricts the Privacy Commissioner's ability to investigate complaints from non-Australian citizens or residents in relation to rectification and that this review will result in this restriction being taken away. The present Opinion has been drafted on the basis of these assumptions, explanations and conditions.

In conclusion, on the basis of the above mentioned findings and subject to the issues mentioned in paragraphs 3, 4 and 5 being taken into account, the Working Party assumes that Australia ensures an adequate level of protection within the meaning of Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of Passenger Name Record data from airlines to Australian authorities in relation to those flights defined as Australian International Flights in Section 64 AF Clause (6) of the Customs Act, i.e. those flights involving travel to, through or departure from Australia.

Done at Brussels, on 16th January 2004

For the Working Party
The Chairman
Stefano RODOTA