ARTICLE 29 Data Protection Working Party



10037/04/EN WP 88

Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines

Adopted on 11th February 2004

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC.

The secretariat is provided by Directorate E (Services, Copyright, Industrial Property and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.

OPINION 3/2004 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 Canada for the transmission of Passenger Name Records (PNR) and Advanced Passenger Information (API) 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 data¹, and in particular Articles 29 and 30 paragraph 1 (b) thereof,

Having regard to the Rules of Procedure of the Working Party², and in particular Article 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

Canada has adopted a number of laws and regulations requiring airlines flying into its territory to transfer to Canada personal data relating to passengers and crew members flying to or from this country in order to secure the integrity of Canadian borders and the security of Canada. The Canadian API/PNR program was already under development long before the events of 11 September 2001, because it was considered part of the programs which could be used to better manage Canadian borders, allowing Canada to identify and focus resources on high-risk travellers, while facilitating the entry of low-risk individuals.

Compliance with the Canadian requirements by the airlines may create problems in respect of Directive 95/46/EC on data protection. The Commission thus entered into talks with Canada in order to establish the conditions that would allow the Commission to adopt a decision recognising the adequate protection on the basis of Article 25(6) of Directive 95/46/EC. The Commission has updated the Working Party on these talks.

The Working Party notes that the transfer of API/PNR data by airlines to Canada may raise public concern, as it already did in the case of the United States, and have broad and sensitive implications in international, political and legal terms.

OJ L 281, 23.11.1995, p. 31, available at:

http://europa.eu.int/comm/internal market/en/media/dataprot/index.htm

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

The collection of the data included in the databases of airlines as requested by Canada covers a large number of passengers which underlines the need for a cautious approach bearing in mind the possibilities this opens up for data mining affecting, in particular, European citizens and entailing the risk of generalised surveillance and controls by a third State. Therefore, the Canadian requirements for the transmission of PNR and API from airlines should be addressed with the utmost attention.

In addition, the Working Party is fully aware that similar flows from airlines have already been requested and/or proposed by several other third countries. This raises the issue of non-discrimination between third States and the necessity for a global approach, which might become a model solution for other countries that may receive similar requests. The Working Party reiterates its view that there is a need for an overall framework for personal information circulating throughout the world for purposes related to security in connection with air travel. In a previous opinion issued in October 2002³, the Working Party called for a common approach at the European Union level to be found.

2. SCOPE OF THE OPINION

The scope of the present Opinion concerns the protection of fundamental rights and freedoms regarding the processing of personal data in a field where the balance between security concerns and these rights and freedoms are at stake.

This Opinion is given by the Working Party with a view to assessing the legitimacy of the communication of personal data and the adequacy of protection provided by Canada with regard to envisaged Commission decisions or other legal instruments dealing with this issue. The Working Party reserves the right to supplement the present Opinion by a further opinion should this Opinion not be adequately taken into account or if substantial changes are made in the course of future negotiations.

The present Opinion is issued with reference to the level of protection ensured by Canada once airlines have transmitted personal data relating to their passengers and crewmembers to the Canadian authorities, on the basis of Canadian law and international commitments. In its assessment of the adequacy of protection afforded by Canadian law, the Working Party has been guided by the general criteria set forth in previous documents⁴ as well as in its Opinion on the subject of API/PNRS data required by the United States⁵.

3. TRANSITIONAL NATURE OF AN ADEQUACY FINDING

Concerns with regards to data flows are related to recent serious circumstances at the international level. The Working Party recommends that periodical short-term re-

³ Opinion 6/2002 issued 24 October 2002.

Working Document on "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive", WP 12 of the Working Party, issued 24 July 1998.

The Working Party also refers to its Opinion 2/2001 on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act.

Opinion 6/2002 of the Working Party on "transmission of Passenger Manifest Information and other data from Airlines to the United States", WP 66 of the Working Party, issued 24 October 2002. Opinion 4/2003 on the Level of protection ensured in the US for the Transfer of Passengers' Data, adopted 13 June 2003.

evaluations of the situation should be made to assess if the necessity for such flows remains. Should the international circumstances alter, or if other means of combating terrorism appear to be more appropriate, it would be necessary to review the situation. The Working Party recommends that the Commission should include clauses in its draft decision on the level of protection afforded by Canada with regard to the collection and processing of PNR/API data providing for a 'sunset' limitation and should review the situation after 3 years in any event.

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

4. ACTION AGAINST TERRORISM AND THE PROTECTION OF FUNDAMENTAL RIGHTS AND FREEDOMS

As the Working Party already stated in its Opinion 4/2003 in relation to the Unites States, the fight against terrorism is both a necessary and valuable element of democratic societies. However, whilst combating terrorism, respect for fundamental rights and freedoms of the individuals including the right to privacy and data protection must also be ensured⁶.

Such rights are protected in particular by Directive 95/46/EC, Article 8 of the European Convention on Human Rights⁷ and are enshrined in Article 7 and 8 of the Charter of Fundamental Rights of the European Union⁸. Moreover data protection is further recognised and expanded in the draft European Constitution prepared and discussed by the Convention on the future of Europe, and is increasingly recognised internationally.

The legitimate requirements of air transport security and internal security in Canada should not contradict these fundamental principles. Derogations and limitations to fundamental rights and freedoms regarding the processing of personal data in the European Union, in particular regarding the purpose principle, should only take place if necessary in a democratic society and for the protection of public interests provided for under European law⁹.

5. CANADIAN LAW ON API/PNR DATA

The Working Party considers that any Commission Decision recognising the provided protection as adequate as well as any other instrument(s) providing a legal framework for the data flows should be based on a clear-cut picture of primary and secondary Canadian legislation regulating purposes, mechanisms and rationale of data processing in Canada and the entities entitled to access such data.

See Opinion 10/2001 « on the need for a balanced approach in the fight against terrorism », adopted on 14 December 2001.

See also the relevant case-law of the European Court on Human Rights.

The European Commission has committed itself to respect the Charter. See Commission Communication on the Charter of Fundamental Rights of the European Union (COM (2000) 559 final).

⁹ See the interests listed in Article 13 of Directive 95/46/EC.

A full picture of the relevant Canadian regulatory framework, to meet openness and transparency requirements in respect of European citizens, should be included as an annex to any Commission Decision. In addition, provision should be made for a mechanism which ensures that any relevant legislative innovation is communicated to the Commission.

The Canadian Customs and Revenue Agency (hereafter the "CCRA") and the Citizenship Immigration Canada Agency (hereafter "CIC") have jointly set up an API/PNR program under the Customs Act (Bill S 23), which received Royal Assent on 25 October 2001 and the Immigration and Refugee Protection Act (hereafter "IRPA"). 10

CCRA's and CIC's access to, use and disclosure of API/PNR data to any third party is regulated in Canadian Law under the Customs Act, the Immigration and Refugee Protection Act (IRPA) and related Immigration Regulations, the Privacy Act, Passenger Information (Customs) Regulations as well as Customs Notices. Both the Passenger Information (Customs) Regulations and Customs Notices implement rules set by the CCRA. Together they constitute a common legal regime providing for the protection of passengers' data transferred from airlines to Canada¹¹.

• The Customs Act and Passenger Information (Customs) Regulations

With respect to information collected by the CCRA, access, use and disclosure of API/PNR information is governed by section 107.1 of the Customs Act. Paragraph 1 of said section provides that "the Minister may under prescribed circumstances and conditions, require any prescribed person or prescribed class of persons to provide, or provide access to, prescribed information about any person on board a conveyance in advance of arrival of the conveyance in Canada or within a reasonable time after that arrival." Furthermore, paragraph 2 of said section provides that "Any person who is required under subsection (1) to provide, or proved access to, prescribed information shall do so despite any restriction under the Aeronautics Act on the disclosure of such information."

API/PNR data must thus be provided in advance of the arrival of the airplane in Canada or within a reasonable time after that arrival.

The Passenger Information (Customs) Regulations bring into force the Advanced Passenger Information/Passenger Name Record (API/PNR) initiative introduced in the 2002-2004 Customs Action Plan. These Regulations were drafted under the authority of section 107.1 of the Customs Act and provide the legal basis for the API/PNR program.

On the basis of section 107.1, which mentions the notions of "the prescribed classes of persons" and "the prescribed information", the Regulations of October 2002 specify what type of information must be provided as well as who has to provide this kind of information.

In force as from 28 June 2002.

The Working Party notes that on 12 December 2003 CCRA and CIC have been merged into a newly created Canadian Border Services Agency. It urges the Commission to provide it with all the necessary information about the consequences of this new arrangement.

Article 2 of these Regulations defines the prescribed classes of persons as: "commercial carriers and charterers who undertake to carry persons and goods to Canada and the representatives of those carriers and charterers; travel agents; and finally owners and operators of a reservations system".

Article 3 defines the prescribed information in respect of a person on board a commercial conveyance and includes PNR and API data such as the passenger's surname, first name and any middle names; date of birth; gender; citizenship or nationality; the type of travel document that identifies the person, the name of the country in which the travel document was issued and the number on the travel document; the reservation record locator number, if any, in the case of a person in charge of the commercial conveyance or any other crew member without a reservation record locator number, notification of their status as a crew member and the information relating to the person in a reservation system.

The Regulations of 1 February 2003 govern the CCRA's collection of API/PNR data from airlines. The collection of API data began on 7 October 2002, whereas the collection of PNR data began on 8 July 2003.

• The Immigration and Refugee Protection Act (hereafter 'IRPA') and Immigration Regulations

According to the information provided by the Canadian authorities, Sections 148(1)(d) and 150 of the Immigration and Refugee Protection Act provide the CIC with legislative authority to enact Immigration Regulations. These Regulations define the terms used in the IRPA and provide operational details related to transporters' obligations under the Act, such as Section 269 of the Immigration Regulations which came into force on 28 June 2002. 12

• The draft legislation (Bill C-17)

Draft legislation (Bill C-17) concerns the collection and use of PNR by other Canadian governmental agencies and departments.

This Bill aims to clarify CIC's right to enter into information sharing agreements with other agencies and covers the collection and use of PNR data by other Canadian governmental agencies. The Bill states that the right to enter into agreements includes "the collection, retention, disposal and disclosure of information for the purposes of this Act" (Section 72 of the Bill amending the IRPA). According to the Canadian authorities the Bill's purpose is to make this right, which exists already, more explicit. The Bill also enables the CIC to adopt regulations in this respect which are passed by the Canadian Parliament. According to the Canadian authorities, the new Section 150.1(b) of the IRPA may provide a very limited extension of CIC's ability to disclose information for reasons related to security and anti-terrorism.

The Working Party notes that this Bill, if adopted, will give both the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) the authority to require certain passenger information.

¹² Canada Gazette Part II, Vol. 136, Extra of 14 June 2002.

6. OPERATION AND FEATURES OF THE CANADIAN API/PNR ACCESS ARRANGEMENTS

• Processing of API/PNR data

The Regulations of 1 February 2003¹³ and 2 July 2003 ¹⁴govern the CCRA's collection of API/PNR data from airlines.

Under the Canadian system, API/PNR relating to passengers on board flights to Canada are 'pulled' from the airlines reservation and departure control systems. Airlines provide the data via the SITA network to a specified address. The Canadian authorities then access these data and store them in the databanks of the CCRA.

The Working Party refers to its Opinion 4/2003 of 13 June 2003, in particular the issue of 'push' and 'pull'. The Working Party notes that the Canadian system is qualified by the Canadian authorities as a 'pull' system, i.e. a system whereby airline passengers data are directly accessed by the authorities concerned on a continuous basis. This raises problems under the Directive as described in this Opinion¹⁵. However, the Working Party welcomes the Canadian position that they have no difficulty in accepting a 'push' system. The Working Party requests that a 'push' system should substitute the present Canadian 'pull' system as soon as possible.

• Purposes for processing API/PNR data

According to the Canadian authorities, API/PNR information will be collected by CCRA for the purpose of identifying persons likely to import prohibited or strictly regulated goods, or any goods which threaten the health or safety of an individual, the environment or the national security or defence of Canada in accordance with the Immigration and Refugee Protection Act. API/PNR data are thus collected for the purposes of identifying persons who, through the import of the goods mentioned above, pose a risk to the health, safety and security of Canada. In addition the Working Party notes that the Canadian system will collect and retain API/PNR information concerning all passengers entering Canada rather than only those who pose a perceived risk

The Working Party refers in this respect to its Opinion 4/2003 of 13 June 2003 with regard to the level of protection ensured in the United States for the transfer of passengers' data and in particular page to 7 thereof. Here the Working Party states that "The purposes for which the data will be used should be limited to fighting acts of terrorism without expanding their scope to other unspecified "serious criminal offences"." These purposes are too widely defined, and in particular go well beyond the purpose of fighting acts of terrorism. Automatic access by customs and law enforcement authorities to personal and commercial data contained in airline passengers' information constitutes an unprecedented derogation to the right to collect data for commercial purposes and should only be justified on the basis of very serious concerns. As in the case of the United States, the Working Party requests that a clear and limited list of serious offences directly related to terrorism should be provided by the Canadian authorities, without prejudice to the possibility of performing additional specific and individual data exchanges on a case by case basis within the framework of judicial and

.

¹³ Canada Gazette, Part I, 1 February 2003.

¹⁴ Canada Gazette, Part II, 2 July 2003.

Heading 5, page 7.

police co-operation. Moreover, the Working Party requires that the different purposes for each data processing should be specified and defined individually. Stricter definitions of the purposes would facilitate the carrying out of proportionality tests with regard to each of the elements involved in the processing.

.

The Working Party has also noted the explanations given by the Canadian authorities in this respect, which indicate that in most cases the data kept after the initial 72 hour period, will not be associated with particular individuals since the names of the passengers will no longer be available. However, the Working Party is not convinced that the passenger's name no longer will be accessible, since certain officials still will have access to the data element 'name'. The Working Party refers to its remarks made below in this respect in the section on data retention time.

• Transferable Personal Data

38 API/PNR data elements have been identified by the Canadian authorities as being required by the CCRA and CIC for the above-mentioned purposes. According to the Canadian authorities API/PNR data elements relating to sensitive data are not collected.

The Working Party notes that this list of 38 API/PNR data elements is longer than the list of API/PNR data mentioned in its Opinion 4/2003 of 13 June 2003. The Working Party thus considers that the amount of data to be transferred to the Canadian authorities goes well beyond what could be considered adequate, relevant and not excessive within the meaning of Article 6 (1) c) of the Directive. The amount of data requested by Canadian Customs and Immigration officials therefore needs to be adapted to the different public interests at stake. The Working Party refers to the 17 API/PNR data elements ¹⁶ mentioned in its Opinion 4/2003 which it considers legitimate and not excessive to be transferred to the Canadian authorities.

A clear, exhaustive list of the data transferred on the basis of the Commission Decision should be attached as an annex to this Decision.

• Data Retention Time

All 38 elements are being collected for the purposes mentioned above. According to the Canadian authorities, access to and disclosure of particular data elements will be increasingly restricted as time progresses. Moreover, the purposes for which the officials use the information may also change. Canadian authorities add that only those particular data elements which are necessary and relevant will be disclosed in any particular situation.

Concerning the different retention periods, the Working Party notes the following:

These elements are: API/PNR record locator code, date of reservation, date(s) of intended travel, passenger name, other names on API/PNR, all travel itinerary, identifiers for free tickets, one-way tickets, ticketing field information, ATFQ (Automatic Ticket Fare Quote) data, ticket number, date of ticket issuance, no show history, number of bags, bag tag numbers, go show information, number of bags on each segment, voluntary/involuntary upgrades, historical changes to API/PNR data with regard to the aforementioned items.

During the first retention period (0-72 hours after arrival), a small number of Customs and Immigration officials will have access to the data. Information will be used to identify passengers who may potentially pose a high risk for immigration or customs purposes.

During the second retention period (72 hours till the end of 2 years), the data will be anonymized, i.e. the data subject's "name" will become inaccessible for most officials having access to the data. Only intelligence officers will have access to the data subject's "name" in specific circumstances. The anonymized data will be used to develop trends and calculate risk factors in order to identify future high-risk travellers who pose a risk of importing controlled goods or who may be refused access to Canada.

The Working Party observes that during this retention period, which by no means can be considered to be "short retention period", some officials will have access to all the data, including the data subject's "name". Therefore, contrary to the assumption made by the Canadian authorities that at this point the remaining data do not convey personal information about a particular passenger, the Working Party considers that it still remains possible to identify the passenger concerned and that such a situation cannot be considered as an anonymization of the data concerned.

During the third retention period (from the third year till the end of six years), personalization data elements such as "name", "date of birth", "address information" and "travel document number" will not be accessible unless in very exceptional circumstances. Again the remaining data will be used for trend analysis and the development of risk indicators that should enable the Canadian authorities to identify future passengers posing a potential risk of contravening the Immigration and Refugee Protection Act in terms of importing certain goods or who may be refused access to Canada.

The Working Party is of the opinion that there exists no essential difference between the second and third retention period. In both cases, data are being stored in order to develop trends and risk factors, which should enable the Canadian authorities to identify future passengers posing a risk of importing controlled goods or who may be refused access to Canada. Again, access to data enabling to identify the passenger to whom the API/PNR data relate remains possible. The Working Party therefore reiterates its remarks made with regard to the second retention period on anonymization.

Also, in line with its Opinion 4/2003, the Working Party is of the opinion that personal data should be kept for no longer than is necessary for the purposes for which they are collected. Thus, only retention of the transferred data in line with the announced purpose of controlling the entry to the Canadian territory with a view to the detection and prevention of terrorist acts may be accepted. Data should only be retained for a short period that should not exceed a few weeks or months following the entry to Canada. A period of 6 years cannot be considered to be a legitimate duration. This is obviously without prejudice to the possible need for the processing to continue on a transitional basis in individual cases where there are well-established, specific grounds to examine certain persons more closely, in view of taking measures related to their actual and/or potential involvement in terrorist activities within the framework of judicial and police co-operation.

• Data Disclosure/Onward Transfers

According to the Canadian authorities disclosure of API/PNR data will be carried out by the CCRA and CIC in very limited circumstances. According to the Canadian authorities, the disclosure should respect the following fundamental principles:

- 1. Disclosure of API/PNR data by the CCRA or CIC agencies shall be carried out under their discretion, on a case by case basis. Said agencies will disclose such information in accordance with administrative guidelines which restrict the circumstances in which this type of information will be disclosed and ensure that disclosures will only be made for purposes which are fully consistent with those for which the information was collected.
- 2. Prior to disclosing API/PNR information, CCRA or CIC agencies should carry out an individualized assessment of the relevance of information relating to a particular person. Only those particular API/PNR elements, which are clearly demonstrated as being required in the particular circumstances, may be provided. In all cases, only strictly necessary information may be provided.
- 3. Onward transfers will be restricted to cases where the recipients of the onward transfer (eg: other Canadian agencies or third countries) are also subject to rules affording an adequate level of protection.

According to the Canadian authorities disclosure of API/PNR information will become increasingly restrictive as time progresses, on the basis of the following timetable:

From the initial receipt until the end of two years, CCRA may disclose the data to law enforcement authorities where it relates to customs offences at the border. CCRA may also share the data with law enforcement authorities where it is necessary to prevent a threat to the life, health and safety of an individual or to the Canadian (or any other country's) environment. For all other purposes, law enforcement authorities or tax administrators will need a warrant to obtain the data. These restrictions reflect the requirements of the Canadian Charter of Rights and Freedoms. They should ensure that any disclosure of API/PNR information will be fully consistent with the customs purposes for which the information will have been collected.

Finally, from the initial receipt until the end of six years, CCRA may disclose the data to national security and defence agencies when there is reason to believe that said data relates to a real or potential threat to Canada's security or defence interests.

If Bill C-17 was to be enacted, CIC would be allowed to disclose API/PNR data on the grounds provided for under the Immigration and Refugee Protection Act as well as with a view to upholding national security and defence interests, and conducting international relations.

The Working Party observes that it is not clear in what concrete cases, under what circumstances and subject to what safeguards a disclosure to other agencies can take place. Disclosures will be made by decision-makers in said agencies on a discretionary basis, in accordance with administrative guidelines only. The Working Party wishes to be informed on which concrete cases and under which circumstances the CCRA and CIC are allowed by law to authorize third party disclosure. Moreover, the Working Party wishes to know what the consequences would be if CCRA and CIC failed to respect the administrative guidelines on data disclosure. The Working Party also wishes to be informed about possible sanctions in case a recipient agency that does not respect the third party rules on disclosure.

The Working Party further notes that the disclosure of information to other agencies or other countries is closely linked to the issue of purposes for processing API/PNR data.

The need for clarification as requested by the Working Party in relation to the purposes for which API/PNR data are being processed by CCRA and CIC also relates to the other agencies entitled to receive the data. In this respect, the Canadian authorities have indicated that provincial or territorial authorities will receive API/PNR information from the CCRA or CIC where, during the first two years after collection of the information, there is reason to suspect that it relates to a threat to the life, health and safety of an individual or the environment of Canada or any other country. However, the Working Party strongly believes that the data should only be communicated to other agencies in specific cases directly related to terrorism. This is in line with the position taken by the Working Party in its Opinion of 13 June 2003.¹⁷

On the issue of onward transfers, the Working party considers that disclosure of API/PNR information to third countries must be specifically restricted to cases where this information relates to persons travelling to these countries and may only be carried out if the destination country affords an equivalent level of protection. Moreover, the Working Party also refers to its position expressed in the above-mentioned opinion and reiterates that any direct or indirect transfers should be made on a case to case basis and made conditional upon acceptance of specific undertakings or conditions no less favourable than those to be provided to the Commission by the Canadian authorities in connection with protecting the transferred data.¹⁸

• Rights of the data subjects and enforcement

The Working Party refers to its Opinion of 13 June 2003, where it states that "one of the most basic principles of an adequate data protection regime is for the data subject to be provided with information and to be able to exercise his/her rights, in an easy, quick and effective manner".

1. Passenger's right to information

The Working Party considers that in its current notification to passengers, the Canada Customs and Revenue Agency is only partly transparent. Indeed, passengers are notified "all airlines are required by Canadian law to provide Canadian customs and immigration authorities with flight and reservation information concerning all passengers and crew on flights destined for Canada. This information will be used by Canadian customs and immigration authorities for authorized customs and immigration purposes. For further information please contact the Canada Customs and Revenue Agency (CCRA) by e-mail at mailto: API-IPVcra.adrc.gc.ca." " and that they may ask for further information. However, the Working Party believes that passengers should be provided with information as to the purpose of the processing and the identity of the data controller in the third country (in this case in Canada), and other information insofar as this is necessary to ensure fairness. In particular, the notice should indicate which personal details are being disclosed to Canadian authorities (name, address, phone number, travel document number, etc) as well as inform passengers about redress mechanisms. Further information should also be provided by Canadian embassies around the world, as it is not always possible for passengers flying to Canada to address their

Page 7 thereof.

Page 8 thereof.

queries directly to a public office in Canada. Finally, the Working Party considers that a final draft notice will have to be agreed between Canada and the European Union.

2. Passenger's right of access, rectification and opposition

The Canadian Privacy Act provides individuals with the rights of access, rectification and opposition with regard to any personal information relating to them, under the control of a Canadian supervisory authority. However, the Privacy Act currently requires that individuals be present in Canada in order to avail themselves of these rights. The Working Party welcomes the CCRA and CIC's commitment to administratively extend the rights of access, rectification and opposition to EU citizens who are not present in Canada. However, it remains to be seen how the execution of these rights will be realised in practice. The Working Party also welcomes the Canadian authorities' position to examine ways in which this commitment could be legally recognized so as to give rise to formal third party rights to EU citizens. The Working Party underlines the importance of non-discriminatory treatment of EU citizens in this respect and requests that the Privacy Act be amended accordingly, as soon as possible. It thus urges the Commission to take this point fully into account in its negotiations with the Canadian authorities. With regard to the enforcement of these rights, the Working Party would like to know what mechanisms, if any, exist under Canadian law, in order to ensure that the individuals' rights of access, rectification and opposition are upheld should a data controller refuse to cooperate.

Moreover, the Canadian Privacy Act confers investigation and reporting powers to the Privacy Commissioner and provides for recourse to the Federal Court. The Customs Act provides for sanctions in the case of unauthorised access, use or disclosure of customs information.

Role of the Privacy Commissioner: The Commissioner's functions are specifically set out in the federal Privacy Act. The Commissioner plays an essential role in monitoring the way in which federal government institutions comply with the basic principles set out in the Privacy Act. Indeed, he or she may receive complaints on any matter relating to the collection, retention or disposal of personal information by a government institution, on the use or disclosure of personal information under the control of a government institution and relating to an individual's request for access to personal information. In such a case, he or she may conduct investigations, but has no adjudicatory power. His or her role is limited to formulating recommendations to the institutions concerned and reporting to the Parliament. However, the Working Party would like to receive additional information enabling it to obtain a full picture of the role of the Privacy Commissioner in terms of his or her concrete powers with regard to the investigation of complaints and the extent to which he or she may intervene in practice, for example by posing sanctions or bringing a case before the courts.

Sanctions: Section 107(2) of the Customs Act forbids unauthorised access, use or disclosure of customs information. Any contravention is a criminal offence punishable by summary conviction with a maximum fine of \$50,000 or imprisonment up to six months, or both, or by indictment with a maximum fine of \$500,000 or imprisonment up to 5 years, or both. Whether or not sanctions exist for the unlawful processing of personal

data by the Citizenship and Immigration Canada agency remains unclear to the Working Party.

7. CONCLUSION

This Opinion sets out a number of the Working Party's concerns with regard to the level of protection of API/PNR data provided for under Canadian law, prior to the adoption by the Commission of a possible Decision on the management of API/PNR information. The overall objective is to establish as soon as possible a clear legal framework for any transfer of airline data from third countries to Canada in a way which is compatible with data protection principles. While recognising that ultimately political judgements will be needed, the Working Party urges the Commission to take its views fully into account in its negotiations with the Canadian authorities. Furthermore, the Working Party reserves the right to discuss the subject again should the matter be examined in a more global manner.

The Working Party is aware that a more global approach concerning the conditions of the use of air transport data for security purposes in a multilateral context might be necessary. The Working Party welcomes the willingness of Canada to work together with the EU with a view to develop such a global approach.

Done in Brussels, on 11th February 2004 For the Working Party *The Chairman* Stefano RODOTÀ