Canada Border Services Agency | Agence des services frontaliers du Canada

ISSN 2369-2391

Memorandum D1-16-3

Ottawa, May 31, 2016

Guidelines for the Access to, Use, and Disclosure of Advance Passenger Information (API) and Passenger Name Record (PNR) Data

In Brief

This memorandum has been revised to reflect changes made to the related regulations, policies, and procedures which govern the access and use of Advance Passenger Information (API) and Passenger Name Record (PNR) data to enable the Interactive Advance Passenger Information (IAPI) system.

This memorandum provides administrative guidelines on the access, use, and disclosure of API and PNR data within the Canada Border Services Agency (CBSA), as well as information regarding access and correction requests for this data.

Legislation

Customs Act
Privacy Act
Immigration and Refugee Protection Act
Passenger Information (Customs) Regulations
Immigration and Refugee Protection Regulations
Protection of Passenger Information Regulations

Guidelines and General Information

Advance Passenger Information (API)

1. API comprises basic information about a traveller and the flight they arrived in Canada upon. Commercial air carriers must provide this prescribed information about every person onboard of expected to be onboard the flight to the CBSA no later than the time of take-off from the last point of embarkation of persons before the conveyance arrives in Canada.

2. The required information about each traveller includes the following:

(a) their name, date of birth, citizenship or nationality, and gender;

(b) type and number of each passport or other travel document that identifies them, and the name of the country or entity that issued it;

(c) their reservation record locator number, if any; and

(d) a unique passenger reference number assigned to them for board/no-board purposes by the carrier or, in the case of a crew member, notification of their status as a crew member.

3. The required information about the flight includes:

(a) the date and time of take-off from the last point of embarkation before arriving in Canada, and the location of that last point of embarkation;

(b) the date and time of arrival at the first point of disembarkation in Canada, and the location of that first point of disembarkation; and

(c) the flight code identifying the commercial air carrier and the flight number.

4. The requirement to provide API comes from s. 5*(a)-(d)* and *(f)* of the *Passenger Information (Customs) Regulations* (PICR) and s. 269(1)*(a)-(d)* and *(f)* of the *Immigration and Refugee Protection Regulations* (IRPR).

Passenger Name Record (PNR)

5. PNR is the air transport industry term for reservation and departure control records created by air carriers or their agents for each journey booked by or on behalf of any passenger. This data is used by air carriers for their own business purposes, and depending upon the underlying transactions and systems responsible for the booking, may contain information including basic identity data about the traveller and their itinerary; contact, payment, and billing information; information about the travel agent that made the booking; check-in status; and seat and baggage information.

6. The CBSA collects a limited set of PNR data relating to all passengers seeking entry into Canada. However, the CBSA does not require any carrier to collect or provide additional elements that they do not already collect for their own business purposes.

7. The requirement to provide PNR comes from s. 5*(e)* of the PICR and s. 269(1)*(e)* of the IRPR.

Operational use of API and PNR Data

8. API may only be used by the CBSA for purposes authorized under the *Customs Act* or the *Immigration and Refugee Protection Act* (IRPA).

9. Per subsection 107(3) the *Customs Act*, where necessary, an official of the CBSA may use API:

(a) for the purposes of administering or enforcing the *Customs Act*, the *Customs Tariff*, the *Excise Act, 2001*, the *Special Import Measures Act* or Part 2 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, or

(b) for the purposes of any Act or instrument made under it that the Governor in Council or Parliament authorizes the Minister, the Agency, the President, or an employee of the Agency to enforce.

10. Per subsection 149*(a)* of IRPA, where necessary, an official of the CBSA may use API for the purposes of exercising the powers or performing the duties and functions of the Minister of Public Safety and Emergency Preparedness under that Act or to identify a person for whom a warrant of arrest has been issued in Canada. For greater certainty, this includes for pre-arrival risk assessment purposes, and validating that all travellers hold a prescribed travel document to enter Canada, or are exempt from that requirement.

11. The use of PNR is strictly limited in law. As set out in section 4 of the *Protection of Passenger Information Regulations* (PPIR), PNR data may be used by authorized CBSA personnel only for the following purposes:

(a) to identify persons who have or may have committed a terrorism offence or a serious transnational crime; or

(b) to conduct trend analysis or develop risk indicators for the purpose of identifying persons who have or may have committed a terrorism offence or a serious transnational crime.

12. Section 1 of the PPIR defines “terrorism offence” and “serious transnational crime” for the purpose of the permitted uses discussed above.

13. In brief, it defines “terrorism offence” as an act or omission committed "in whole or in part for a political, religious or ideological purpose, objective or cause" with the intention of intimidating the public “with regard to its

security, including its economic security", or "compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act " Activities recognized within this context include death and bodily harm with the use of violence; endangering a person's life; risking the health and safety of the public; significant property damage; and interference or disruption of essential services, facilities or systems. This includes conspiracy, attempt, or threat to commit such an act or omission, or being an accessory after the fact or counselling in relation to any such act or omission. The definition also includes knowingly participating in or contributing to a terrorist group for any of the above purposes or providing material or financial support to such a group. Readers should refer to the PPIR for a complete definition of this term.

14. The PPIR defines "serious transnational crime" as an act or omission that constitutes an offence that is punishable in Canada by a maximum term of imprisonment of at least four years and is committed:

(a) in more than one country;

(b) in only one country but a substantial part of its preparation, planning, direction or control takes place in another country;

(c) in only one country but an organized criminal group that engages in criminal activities in more than one country is implicated in the act or omission;

(d) in only one country but has substantial effects in another country; or

(e) in a country other than Canada but the offender intends to travel to or transit through Canada.

15. Examples of serious transnational crimes include, but are not limited to:

(a) narcotics smuggling;

(b) human smuggling;

(c) human trafficking; and

(d) importation or smuggling of child pornography.

16. Misuse of API or PNR data in contravention of CBSA policies, directives, or standards may be subject to security screening review for cause as well as disciplinary action, up to and including termination of employment. Additionally, a person knowingly disclosing, providing access to or using customs information in a manner not authorized by the *Customs Act* is guilty of an indictable offence or an offence punishable on summary conviction under subsection s. 160(1) of that Act.

Access to PAXIS

17. API and PNR data are stored in the Passenger Information System (PAXIS). Pursuant to Treasury Board policy and the CBSA's Directive for Access Control in Information Systems, access to PAXIS is restricted according to the "need-to-know" and "least privilege" principles. This means that users will only be granted access to PAXIS where it is required in order for the user to perform their assigned duties, and that the user will be assigned a profile with the minimum access permissions required to fulfill said duties.

18. Certain PAXIS user profiles provide access to PNR information. These profiles are assigned exclusively to targeting and intelligence personnel who require them to perform assigned duties or functions which are clearly linked to the identification of persons who have or may have committed a terrorism offence or serious transnational crime as set out in the PPIR.

19. PAXIS access requests should be submitted through the IT Self-service Portal. All access requests must be approved by the user's immediate superintendent, supervisor, chief or manager. For a list of PAXIS profiles and the associated permissions, please see the Appendix.

20. Each query and review of passenger data elements in PAXIS is recorded for audit purposes.

Timeframes for Access to Data in PAXIS

21. Per section 3 of the PPIR, API and PNR data are retained in PAXIS for 3.5 years after the CBSA receives the data, unless the data is required as part of an ongoing investigation, in which case it may be retained until the investigation is concluded, or up to a maximum of six years.

22. Additional data retained in PAXIS as part of the IAPI program, such as board/no-board messages and flight update notification messages are also retained for 3.5 years.

23. As set out in section 4 of the PPIR, access to PNR data in PAXIS changes over three distinct timeframes. During each timeframe, the treatment of PNR data becomes progressively more restrictive:

(a) All PNR data collected is available for the first 72 hours after it is received.

(b) For the period beginning 72 hours after receipt, and continuing until two years after receipt, the names of travellers in the PNR are masked. These may be unmasked only where a targeting or intelligence officer reasonably believes that the name of the person is required in order to proceed with an investigation relating to a terrorism offence or serious transnational crime.

(c) For the period beginning 2 years after receipt, and continuing until the data is deleted 3.5 years after it was received, all PNR data elements which could serve to identify the person to whom the information relates are masked and will be available for viewing only if approved by the President of the CBSA to identify persons in relation to a terrorism offence or serious transnational crime.

Requesting Access to PNR Received Two or More Years Ago

24. As required by subsection 4(3) of the PPIR, CBSA officials may have access to retained PNR elements in PAXIS that could serve to identify a person which are 2 to 3.5 years old only if the President authorizes such access as necessary to identify an individual who is reasonably suspected of having committed a terrorist offence or serious transnational crime.

25. Any request for Presidential approval to unmask this data must be made in writing. The requesting official must explain their suspicion, and set out specific and articulable facts that support the suspicion on a particularized and objective basis.

26. The President may only authorize such a request where the President has determined there are reasonable grounds to suspect that the individual in question has committed the alleged offence. This requires a finding that there is a reasonable possibility the individual has committed the offence, grounded in objective facts.

27. Presidential authorization may only be given in writing. Subsection 4(6) of the PPIR requires that a record be kept of any Presidential authorization. This record must be retained for at least two years. At a minimum, this record must contain:

(a) The name of the requesting official;

(b) The reasons for the request;

(c) The name of the subject of the request; and

(d) The date on which the request was made, the date the request was authorized, and the date the information was accessed.

Disclosure of API

28. Disclosures of API information are no longer governed by the PPIR. Instead, as API is collected under both the *Customs Act* and the IRPA, API should only be disclosed under the more restrictive disclosure regime of the two acts. As s. 107 of the *Customs Act* is a more restrictive disclosure regime than that afforded to personal information collected under IRPA by s. 8 of the *Privacy Act*, s. 107 prevails and API disclosures must only be made pursuant to its provisions.

29. For additional guidance on section 107 of the *Customs Act* and Section 8 of the *Privacy Act* contact CBSA officials at the Information Sharing and Collaborative Arrangements Unit directly.

30. Members of the public may request copies of the aforementioned policies by contacting CBSA-ASFC_ATIP-AIPRP@cbsa-asfc.gc.ca.

Disclosure of PNR

31. It is the policy of the CBSA that PNR information is only disclosed pursuant to the applicable provisions of the PPIR.

Disclosure of PNR to Domestic Authorities

32. The CBSA may disclose PNR to domestic authorities, including federal and provincial departments and authorities, such as the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, and provincial and municipal police forces. Such disclosures may be made in response to a request; pursuant to the terms of a written agreement between the CBSA and the domestic recipient; or as a proactive disclosure, that is, where a CBSA official provides information to a domestic recipient without said recipient having asked for the information. A disclosure of PNR in any of the foregoing circumstances is subject to the following conditions as laid out in section 6 of the PPIR:

(a) The disclosure must be on a case-by-case basis. PNR must never be disclosed in bulk.

(b) There are reasonable grounds to believe that the PNR would be relevant to the prevention, investigation or prosecution of a terrorism offence or serious transnational crime. Reasonable grounds exist if the CBSA official authorizing the disclosure believes the PNR would be relevant to the prevention, investigation or prosecution of a terrorism offence or serious transnational crime, and that belief is supported by compelling and credible information. In cases where a CBSA official has concerns as to whether there are reasonable grounds to disclose, the official may advise the requester that a subpoena or a judicial order may be required.

(c) The receiving department or authority exercises functions directly related to the prevention, detection, investigation or prosecution of terrorism offences or serious transnational crimes. This condition cannot be satisfied if the receiving department or authority does not have clear lawful authority to receive the PNR in question.

(d) The receiving department or authority has undertaken to apply standards to protect the PNR that are at least equivalent to those set out in the PPIR. This would include commitments to not use the PNR other than for the prevention, detection, investigation or prosecution of terrorism offences or serious transnational crimes; and to not retain the PNR longer than the retention limits discussed in paragraph 21 of this memorandum. This may be accomplished through the use of caveats included with the disclosure.

(e) The receiving department or authority has undertaken not to further disclose the PNR without the permission of the Agency, unless required by law to do so. Like the requirements in paragraph 32*(c)*, this may be accomplished through the use of caveats included with the disclosure.

(f) The CBSA must disclose only the minimum elements of PNR necessary for the purposes for which it is disclosed.

33. Deciding to disclose PNR is a discretionary decision that should be exercised with care and only after diligent consideration of the circumstances. A lawful authority to disclose must always exist and the onus is on the official approving the disclosure to ensure that there is an appropriate rationale for the disclosure and that the conditions laid out in in paragraph 32 are satisfied. Proactive disclosures, in particular, should only take place where an official is of an opinion that the receiving department or authority's interest in the disclosure clearly outweighs the person's expectation of privacy.

34. Per section 7 of the PPIR, Despite the conditions laid out in paragraph 32, nothing prevents the Agency from disclosing PNR information to comply with a subpoena, warrant or order issued by a court, person or body with jurisdiction in Canada to compel the production of information. This is the only exception to the disclosure requirements outlined in the foregoing paragraphs.

35. Whenever it becomes evident that a disclosure of PNR may lead to a series of similar disclosures to the same department or authority, it is recommended that the Agency enter into a written collaborative arrangement (WCA) with the recipient of the information. The WCA must satisfy all the requirements laid out in paragraph 32.

Disclosure of PNR to Foreign Authorities

36. The CBSA may disclose PNR to a foreign government authority only where there is an applicable international agreement or arrangement that authorizes the disclosure of PNR by the CBSA to the receiving foreign government authority. A disclosure of PNR subject to such an agreement or arrangement must meet the following conditions as laid out in section 8 of the PPIR:

(a) The disclosure must be on a case-by-case basis. PNR must never be disclosed in bulk.

(b) There are reasonable grounds to believe that the PNR would be relevant to the prevention, investigation or prosecution of a terrorism offence or serious transnational crime. Reasonable grounds exist if the CBSA official authorizing the disclosure believes the PNR would be relevant to the prevention, investigation or prosecution of a terrorism offence or serious transnational crime, and that belief is supported by compelling and credible information.

(c) The receiving foreign government authority exercises functions directly related to the prevention, detection, investigation or prosecution of terrorism offences or serious transnational crimes.

(d) The receiving foreign government authority has undertaken to apply standards to protect the PNR that at least equivalent to those set out in the PPIR. This would include commitments to not use the PNR other than for the prevention, detection, investigation or prosecution of terrorism offences or serious transnational crimes; and to not retain the PNR longer than the retention limits discussed in paragraph 21 of this memorandum. This may be accomplished through the use of caveats included with the disclosure. If the receiving foreign government authority is subject to a treaty with the European Union that sets out standards to protect PNR, those standards will be considered equivalent for the purposes of this paragraph and thus additional caveats will not be necessary. Currently, foreign government authorities in the United States and Australia are governed by applicable treaties.

(e) The CBSA must disclose only the minimum elements of PNR necessary for the purposes for which it is disclosed.

37. Deciding to disclose PNR, especially outside of Canada, is a discretionary decision that should be exercised with care and only after diligent consideration of the circumstances. A lawful authority, and an applicable agreement or arrangement, must always exist and the onus is on the official approving the disclosure to ensure that there is an appropriate rationale for the disclosure and the conditions laid out in in paragraph 36 are satisfied.

Recording Disclosures of PNR

38. Section 9 of the PPIR requires that a record be kept of any disclosure of PNR. This record must be retained for at least two years. At a minimum, this record must contain:

(a) the name of the person to whom the information was disclosed, and the government department or authority where they are employed;

(b) the reasons for the disclosure;

(c) the name of the subject of the disclosure; and

(d) the date of the disclosure.

Rights of Access, Correction, and Complaint

39. Upon request, the CBSA will provide any individual, regardless of citizenship or presence in Canada, access to their API and PNR information held by the CBSA, including board/no-board information. Individuals may make a request by completing the *Traveller's API/PNR Information Request* form.

40. The CBSA will consider any individual's request to correct any error contained in their API or PNR information. The Agency will either make the applicable correction, or attach a notation to the information indicating a request for correction was refused, and respond to the individual with an explanation of the legal or factual reasons why the request was refused.

41. Canadian citizens, permanent residents, and any individual present in Canada may make a complaint to the Office of the Privacy Commissioner (OPC) concerning a request for access, correction, or notation.

42. Foreign nationals not present in Canada may make a complaint to the Recourse Directorate of the CBSA concerning a request for access, correction, or notation.

Additional Information

43. For more information, within Canada call the Border Information Service at **1-800-461-9999**. From outside Canada call 204-983-3500 or 506-636-5064. Long distance charges will apply. Agents are available Monday to Friday (08:00 – 16:00 local time / except holidays). TTY is also available within Canada: **1-866-335-3237**.

Appendix

PAXIS Profiles	
Role (#)	**Purpose**
Project Support User (2293)	May be assigned to officers who are employed on teams working on PAXIS system development projects.
Business Support (2294)	May be assigned to officers who are employed on teams working on business system support for the PAXIS system.
Targeting Officer – People (2295)	May only be assigned to Targeting Officers employed by the people targeting section at the National Targeting Centre.
Targeting Supervisor/Manager (2296)	May only be assigned to Targeting Supervisors and Managers who work in the targeting people section at the National Targeting Centre.
Targeting Ops Support – People (2297)	May only be assigned to program officers who are employed in the NTC Targeting Ops Support Unit – People.
NTC Intelligence – People (2298)	May only be assigned to officers employed by the Targeting Operations Intelligence Unit who support NTC Targeting – People.
Traveller Targeting Programs (2299)	May be assigned to program officers within the Programs Branch who are employed on the team responsible for the targeting program.
Regional/HQ Intelligence (2300)	May be assigned to CBSA Intelligence Officers and Analysts.
HQ Program Support (2301)	May be assigned to program officers employed at HQ that support IAPI or the targeting program.
Compliance Officer (2302)	May be assigned only to program officers who are employed with the Airline Compliance Unit.

References	
Issuing Office	Program and Policy Management Division Traveller Programs Directorate Programs Branch
Headquarters File	
Legislative References	*Customs Act* *Immigration and Refugee Protection Act* *Privacy Act* *Passenger Information (Customs) Regulations* *Immigration and Refugee Protection Regulations* *Protection of Passenger Information Regulations*
Other References	
Superseded Memorandum D	D1-16-3 dated January 14, 2010