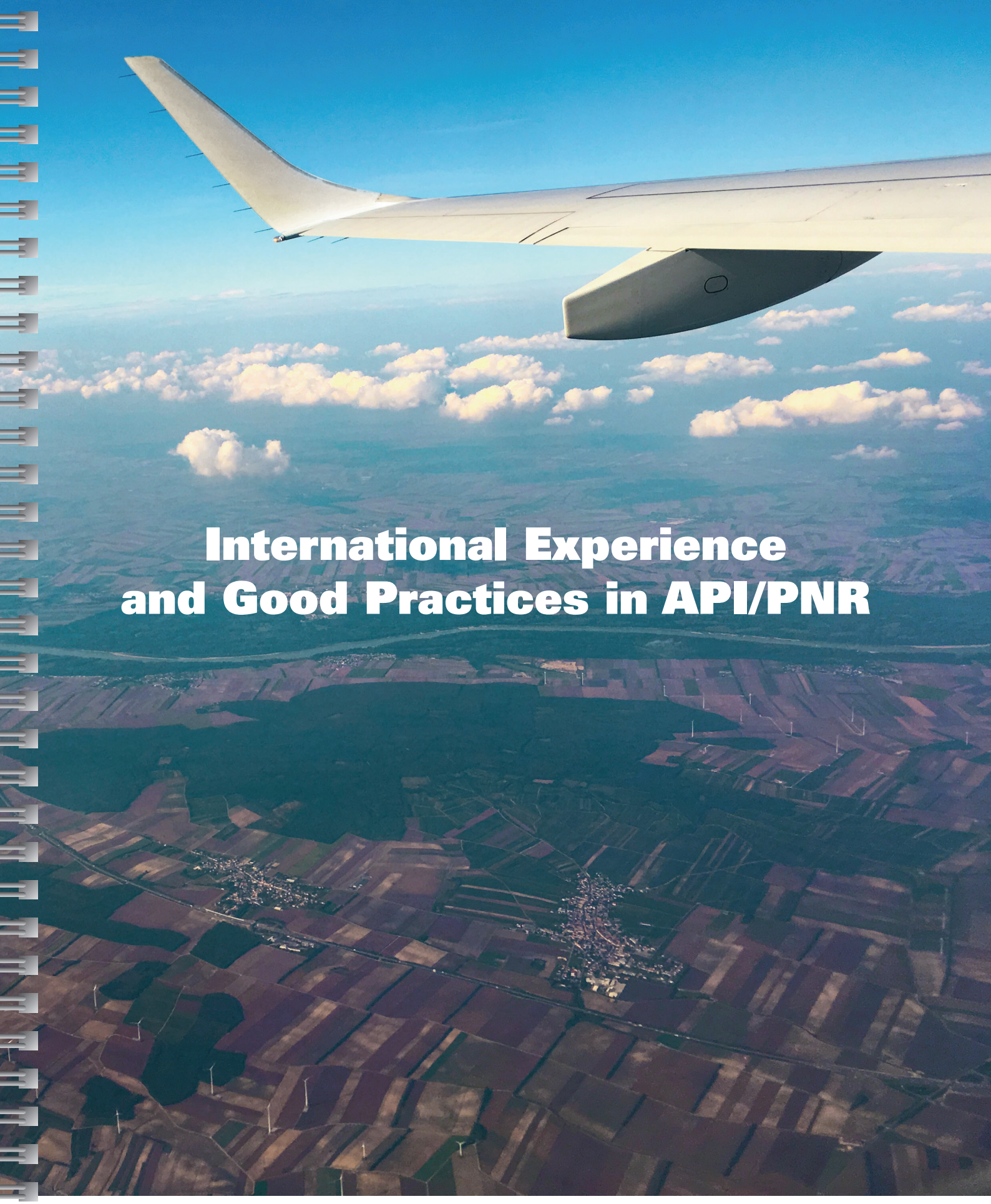


International Experience and Good Practices in API/PNR

OSCE Organization for Security and Co-operation in Europe
Project Co-ordinator in Ukraine

STATE BORDER GUARD SERVICE OF UKRAINE

These materials were developed within the framework of the international project "Assisting the State Border Guard Service of Ukraine in Detecting Terrorism Threats at the State Border", implemented by the State Border Guard Service of Ukraine and the OSCE Project Co-ordinator in Ukraine in 2021.

International Experience and Good Practices in API/PNR / Andrew Priestley, Marc Beauvais, 2021.- 44 pages.

Authors:
Andrew Priestley, International API/PNR Expert
Marc Beauvais, International API/PNR Expert

In order to assist Ukraine in developing an effective national API/PNR system, the OSCE Project Co-ordinator in Ukraine gathered, analyzed and prepared international experiences and good practices in API/PNR as well as developed a Concept Roadmap for API/PNR.

These materials were published with the support of the OSCE Project Co-ordinator in Ukraine. Its content does not necessarily reflect the policy and position of the OSCE PCU.

OSCE Organization for Security and Co-operation in Europe
Project Co-ordinator in Ukraine

STATE BORDER GUARD SERVICE OF UKRAINE

Contents

I. API/PNR basics

Advance Passenger Information (API) and Passenger Name Record (PNR) collected by the commercial air carriers, is used by registered countries to identify passengers who may pose a risk to the safety and security of their country, before they reach a Port of Entry. Furthermore, API transmitted by commercial air carriers may be used for Interactive Advance Passenger Information (iAPI) to issue board/no-board messages indicating if the passenger requires a prescribed travel document, and if so, that they possess one, or if the passenger is a prescribed person. The API (and sometimes PNR) transmitted by commercial air carriers is also used to vet against all known risk for travellers departing their country.

API consists of data that identifies a person, including:

- Surname
- First name
- Middle names
- Date of birth
- Gender
- Citizenship or nationality
- Number and country of issue of the travel document type

PNR relates to traveller reservation and itinerary data contained in a carrier's departure control and reservation systems. This includes but is not limited to:

- PNR locator code
- Date of reservation
- Dates of intended travel
- Ticketing information
- Seat information
- Check-in information

Airline Reservation System (ARS) / Global Distribution System (GDS)

When a passenger books a flight, the travel agent or travel website will create a PNR in a Global Distribution System (GDS). A GDS is a computerized reservation network that is used to store and retrieve information related to air travel. It also acts as a single point of access for travel agents and travel websites that allow commercial air carriers to share the PNR should there be changes required to the reservation. Some examples of a GDS are SABRE, Amadeus, and Travelsky.

If a passenger books directly with an airline over the telephone or an airline specific website, or if an airline does not have a GDS, then the PNR can/will be stored in that airline's Airline Reservation System (ARS).

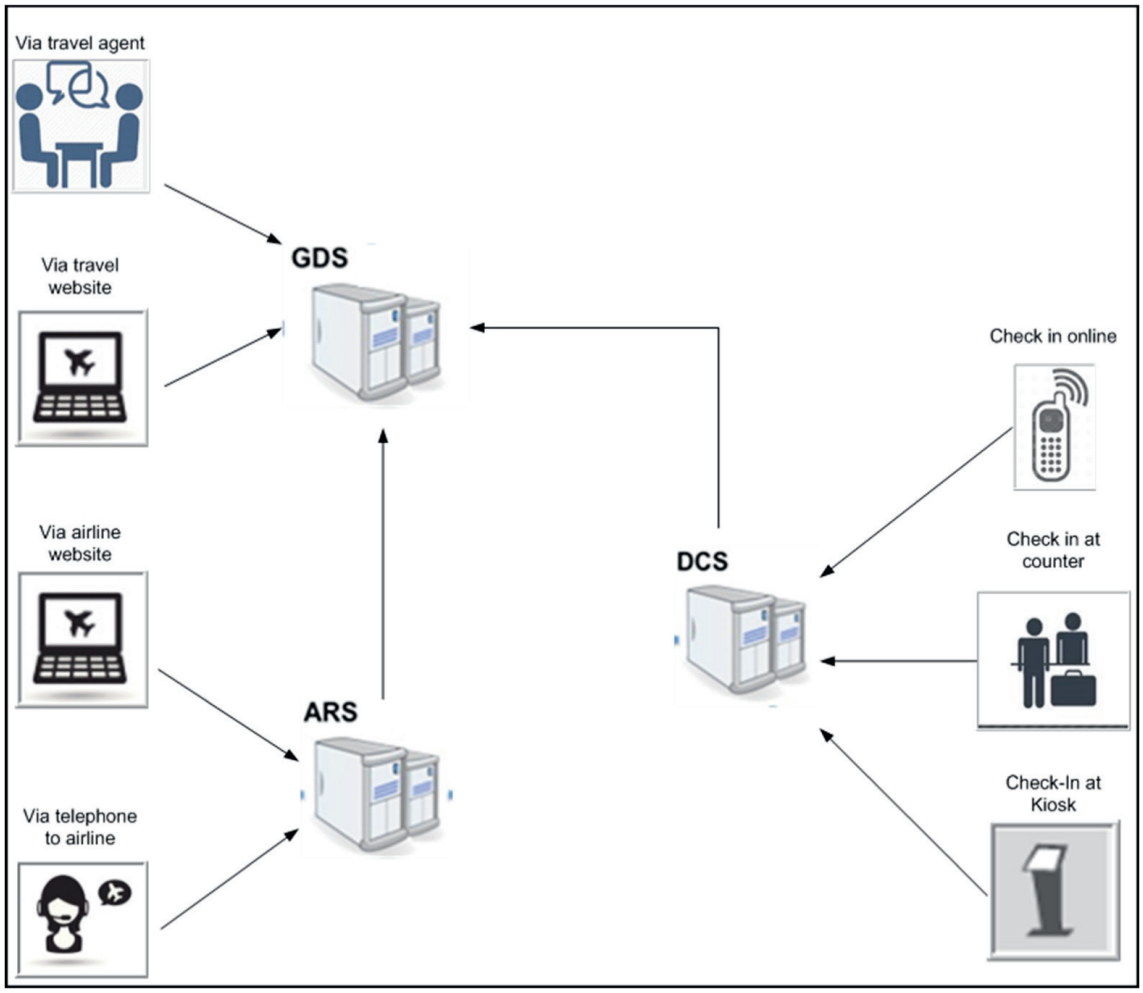
There are five parts of a PNR required before the booking can be completed in a GDS and/or ARS:

- Name of the passenger(s)
- Contact details for the travel agent or airline office
- Ticketing details (either a ticket number or a ticketing time limit)
- Itinerary of at least one segment, which must be the same for all passengers listed
- Name of the person making the booking

Once these five parts of PNR are completed, a GDS and/or ARS will issue a unique six character alphanumeric record locator (also referred to as a locator number or PNR/PNR Locator), which remains the same regardless of any further changes made to the reservation, including a cancellation.

The next step in the information chain is the Departure Control System (DCS), which is an automated computer system used by commercial air carriers for departing flights. Up to 24 hours before departure, the GDS/ARS transfers passenger data to the DCS and will continue to send updates as they occur, until the time of departure. The DCS is used for passenger check-in, boarding control, load planning and weight/balance distribution. Systems vary from one airline to another, but generally all have these same features.

When a passenger checks in, the DCS records are updated with seat, baggage and document information; this can be done at the airline check-in counter, web check-in or via self-service kiosks.



Advance Passenger Information (API)

Passenger information for a person who is expected to be on board the commercial conveyance destined for a participating country is prescribed by the country's law and must be provided to the participating country no later than the time of check-in. Passenger information for a person who is expected to be on board the commercial conveyance departing the participating country is prescribed by the country's law and must be provided to the participating country starting 72 hours prior to the scheduled time of departure, if available Crew member information for a person who is expected to be on board the commercial conveyance is prescribed by the country's law and must be provided to the country no later than one hour before the time of departure. Many countries have laws, regulations or directives in this regard.

In the EU, the transmission of advance passenger data is regulated by Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data. The main objectives of the Directive are to combat irregular immigration and to improve border control. The Directive also allows Member States to use API data for law enforcement purposes on the basis of national law. API data are a very useful tool for law enforcement authorities when used in combination with PNR data.

API is defined (as for most countries) as the following prescribed information about a person on board or expected to be on board a conveyance:

(a) their surname, first name and any middle names, their date of birth, their citizenship or nationality and their gender.

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

(c) their reservation record locator number, if any.

(d) the unique passenger reference assigned to them, if any, by the person that has been required to provide information or, in the case of a crew member who has not been assigned one, notification of their status as a crew member.

(f) the following information about their carriage on board the commercial conveyance:

(i) the following dates and times:

(A) in the case of a person who is or is expected to be transported on board a commercial conveyance by air, the date and time of take-off from the last point of embarkation of persons before the conveyance arrives in or departs from the participating country, or

(B) in the case of a person who is or is expected to be transported on board a commercial conveyance by water or land, the date and time of departure from the last point of embarkation of persons before the conveyance arrives in the participating country,

(ii) the last point of embarkation of persons before the commercial conveyance arrives in or departs from the participating country,

(iii) the date and time of arrival of the commercial conveyance at the first point of disembarkation of persons in or outside of the participating country,

(iv) the first point of disembarkation of persons in or outside of the participating country, and

(v) in the case of a commercial conveyance that transports persons or goods by air, the flight code identifying the commercial carrier and the flight number.

API information is often populated with information retrieved from the machine readablezone (MRZ) of the passport. However, the API information can also be captured from the visual inspectionzone (VIZ) of the passport.

Passenger Name Record (PNR)

PNR is an airline industry term that refers to information about a passenger held within a computer system (ARS, DCS, GDS) used by the commercial air carrier, charter operator or vendor. It contains the information that is relevant to a traveller's booking or reservation. Once created, the PNR is retained by the carrier or its 3rd party service provider until it is required to provide verification of a passenger's status during the check-in process. As noted above, API often contains information drawn from the (MRZ) of a travel document. PNR on the other hand is registered or entered by commercial air carriers or travel agents into a computer system, or by a traveller online, at the time a reservation is made. One of the main differences between API and PNR is that information that can be found in PNR mainly depends on the information that the passenger themselves provided either online or to an agent, as opposed to API which is captured from the official travel document.

The analysis of PNR data can provide the authorities with important elements from a criminal intelligence point of view, allowing them to detect suspicious travel patterns and identify associates of criminals and terrorists, in particular those previously unknown to law enforcement. Accordingly, the processing of PNR data has become a widely used essential law enforcement tool, in the EU and beyond, to prevent and fight terrorism and other forms of serious crime, such as drugs-related offences, human trafficking, and child sexual exploitation.

For the purposes of the data submission, current regulations outline what information is considered to be PNR information, if received in a PNR or DCS message. They include but not limited to the following:

- PNR locator code
- Date of reservation
- Passenger Name
- Billing Address
- Contact telephone numbers
- Travel agency information
- Travel agent
- Ticket number
- Seat number
- Bag tag numbers (baggage information)
- Seat information
- Check-in information

This list is often misinterpreted to mean that countries are limited to receive independent data elements only. In actuality, most of the PNR elements are overarching data titles for which countries receives multiple pieces of information. Countries are able to receive and process, if the commercial air carrier collects and uses that information, upwards of 400 distinct pieces of data that make up DCS and PNR messages. For example, the item listed above called "baggage information", can be made up of the following pieces of information, which countries can and does receive if it is captured and sent by the commercial air carrier or 3rd party service provider:

- Total number of pieces of checked baggage
- Total number of pieces of carry-on baggage
- Weight of checked baggage
- Kilograms or pounds
- Pooled baggage indicator

- Pooled baggage identifier
- Company identification
- Tag numbers
- Number of consecutive tags
- Place of destination
- Airline code number
- Bag tag characteristic

Commercial Air carriers are required to provide to countries only that information which they collect and retain for their own business purposes.

Flight Update Notification Messages

Commercial air carriers may or may not provide participating countries with the following Flight Update Notification (FUN) Messages:

- Close-out Message – to be provided for every flight no later than 30 minutes after departure to indicate travellers on-board the flight.
- Cancelled Reservation Message – to be provided any time a traveller (or group of travellers under the same PNR locator number) cancels their reservation.
- Reduction in Party Message – to be provided when a traveller (or several travellers but not all of the travellers under the same PNR locator number) cancels from a group reservation.
- Cancelled Flight Message – to be provided when a traveller(s) and crew member(s) flight is cancelled.

Data Acquisition System (DAS)

The technology used by participating countries to support the transmission of crew and passenger information by a commercial air carrier and/or 3rd party service provider is called the Data Acquisition Solution (DAS). The DAS will validate and process the data prior to sending the data to the participating country's targeting system. The DAS retains the raw message for 90 days, then the data is purged.

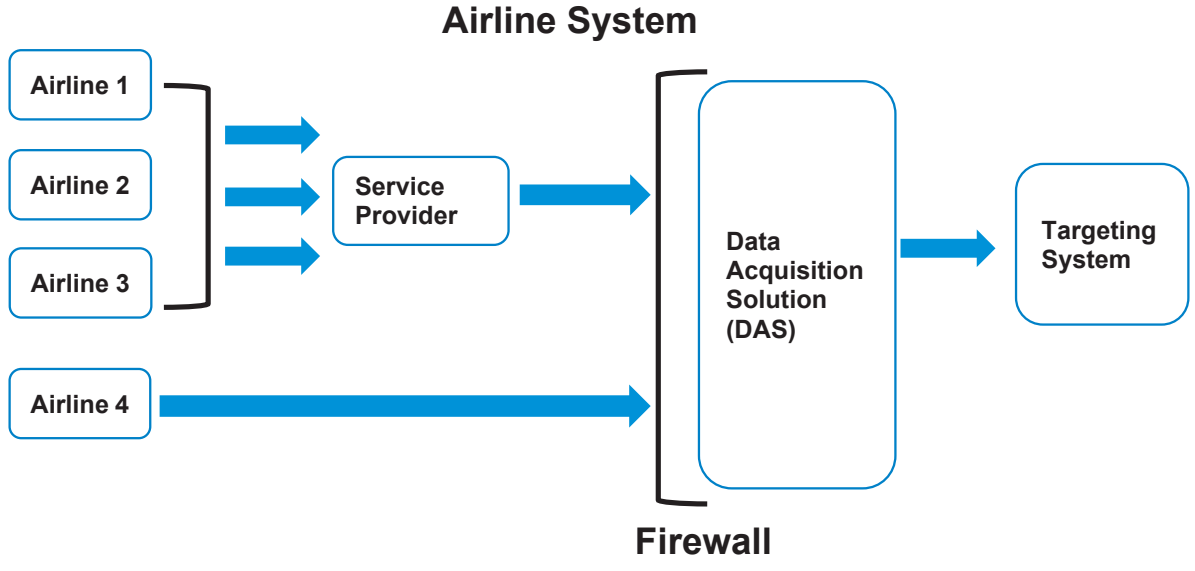
There are three methods for the airline industry to push API, FUN, PNR, and DCS data to the participating countries. It should be noted that many commercial air carriers utilize multiple methods of transmission, depending on the type of information being sent and from where. In addition, some commercial air carriers utilize multiple service providers, depending on the type of data being sent.

All new carriers and 3rd party service providers require certification prior to being able to send data to a participating country. All methods of transmission as well as the message formats chosen must be certified and tested by the participating country to ensure that the data and formatting of the messages meet their standards.

Authorized Methods of Transmission

Transmission by Direct Connection

In the diagram below there are two options for commercial air carriers to push data to participating countries using a secure channel, (message query [MQ] connection) via a 3rd party service provider and/or commercial air carrier directly to the participating country.



3rd Party Service Provider

Many commercial air carriers enter into contractual arrangements with a 3rd party service provider that will be responsible to provide information to a participating country on behalf of the carrier in accordance with applicable legislation and regulations. The 3rd party service provider will provide the required information in one of the authorized formats for transmission. In some instances, an air carrier can act as a service provider for another carrier. An example of this type of arrangement is Delta Commercial air carriers, which submits information on behalf of several smaller commercial air carriers. Commercial air carriers use service providers for a variety of reasons which can include but is not limited to, a lack of system capability or knowledge on the commercial air carriers' side or for increased efficiency. Some service providers host the data, format it and transmit it to the participating country, some acquire the data from the carrier's systems and then format and transmit it, while others are simply used as a transmission method (or pipeline) to the participating country. In the last instance, carriers will develop and certify the message format(s), but will transmit the data via their chosen service provider.

A sampling of 3rd party service providers include:

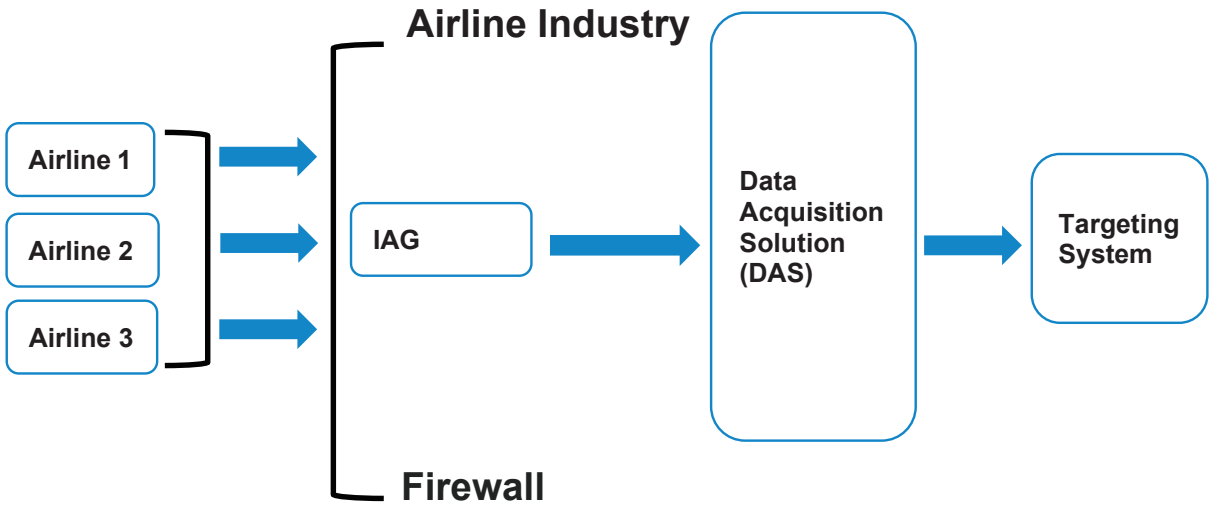
- SITA
- Amadeus
- ARINC
- Travelsky
- AvFinity
- Sabre

Commercial air carriers

Another option that DAS allows is a direct connection of any commercial air carrier system that maintains API, PNR or DCS information to the participating country through a secure channel, MQ connection. This secure channel essentially creates a one-to-one relationship between the commercial air carrier and the participating country, eliminating the need to engage with a 3rd party service provider.

Transmission by Internet API Gateway (IAG)

An IAG provides commercial air carriers and 3rd party service providers with a free option for sending their required data for processing. An IAG provides a method of uploading API, FUN, PNR and DCS data files using the message formats identified below and it also allows for manual data entry of API and FUN data files. IAG users require an individual user-id and password that are provided by the participating country. The diagram below depicts the flow of data from IAG to DAS.

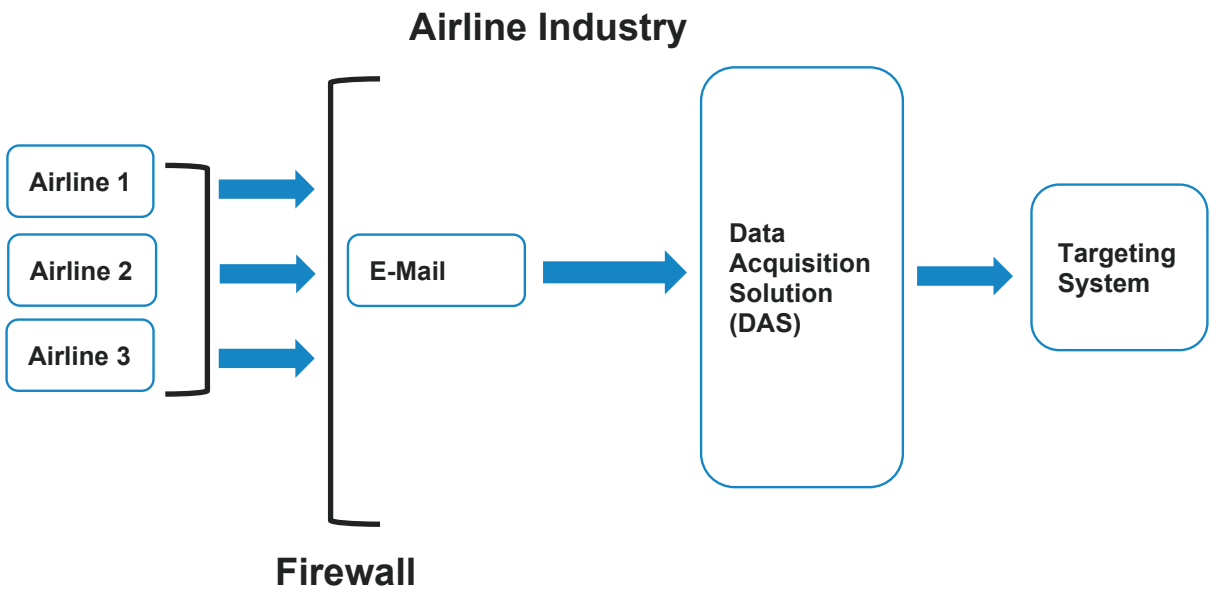


Transmission by E-Mail

Another option for commercial air carriers and 3rd party service providers transmitting API and FUN data to participating countries is e-mail. Commercial air carriers and 3rd party service providers cannot use e-mail to transmit PNR data. The API or FUN data can be sent via e-mail to participating countries using one of the API and FUN message standards that the country support. In order to submit information via email, the commercial air carriers or 3rd party service provider must be certified to use this method, and the associated sender email address must be registered with the participating country.

Transmission by E-mail is not usually recommended by airlines or receiving countries due to the fact it is a manual process however the method is useful for one-off flights (i.e. emergency flights) or in times of disrupted operations.

The diagram below depicts the flow of data using the e-mail method.



Cargo carriers that are only required to report API for crew members most commonly use this method. Although many commercial air carriers will use this particular method of sending API data for crew and passengers only as a back-up, some commercial air carriers with low volumes of flights, or who predominately depart from less or non-automated ports such as those in the Caribbean, will use this method as their primary method of sending API data.

Authorized Message Formats

In addition to establishing the preferred transmission method(s), a commercial air carrier or 3rd party service provider would also be required to develop the API, FUN, PNR, and/or DCS message format standards that are accepted by the participating country. The message standards include the following:

- Electronic Data Interchange For Administration, Commerce, and Transport (EDIFACT) for API data, PNR data, cancelled flight, reduction in party, cancelled reservation, and closeout message;
- Extensible Mark-up Language (XML) for PNR data only;
- Comma-Separated Values (CSV) for API data, cancelled flight, reduction in party, cancelled reservation, and close-out messages;
- IAG – Interactive Data Entry (IDE) for API data, cancelled flight, and close-out messages; and
- Customs Response Message (CUSRES) for commercial air carrier acknowledgement of receipt of an unsolicited board/no-board message.

Message Type received	Direct Connect / MQ	IAG – IDE	IAG – File Upload	Email
API	• UN/EDIFACT (PAXLST)	• IDE	• UN/EDIFACT (PAXLST) • CSV	• UN/EDIFACT (PAXLST) • CSV
PNR	• CBSA XML • EDIFACT (PNRGOV)	• N/A	• CBSA XML • EDIFACT (PNRGOV)	• N/A
Flight Update Notification*	• UN/EDIFACT (PAXLST)	• IDE*	• UN/EDIFACT (PAXLST) • CSV	• UN/EDIFACT (PAXLST) • CSV
Commercial Air Carrier Unsolicited Acknowledgement Message	• CUSRES	• N/A	• N/A	• CUSRES

*Only Cancelled Flight and Close-Out Messages are accepted via IAG-IDE

Role of the passenger information units (PIUs)

PIUs are in charge of:

- collecting PNR data from airlines,
- comparing PNR data against relevant law enforcement databases and processing them against pre-determined criteria, to identify persons potentially involved in a terrorist offence or serious crime,
- disseminating PNR data to national competent authorities, Europol, and PIUs of other EU countries, either spontaneously or in response to duly reasoned requests

Data protection safeguards

The EU PNR Directive provides **data protection safeguards**, such as:

- sensitive data must not be processed,
- data must be depersonalised after 6 months,
- data may be re-personalised only under strict conditions,
- data must be deleted after 5 years,
- a data protection officer is appointed in each PIU and
- an independent national supervisory authorities must oversee the processing activities.

PNR: List of Member States who have decided to apply the Directive (EU) 2016/681 to intra-EU flights

The following Member States have communicated full transposition of the EU Passenger Name Record (PNR) Directive and have notified the Commission of their decision to apply the PNR to intra-EU flights:

- Belgium,
- Bulgaria,
- Croatia,
- Cyprus,
- Czech Republic,
- Estonia,
- Finland,
- France,
- Germany,
- Greece,
- Italy,
- Latvia,
- Lithuania,
- Luxembourg,
- Hungary,
- Malta,
- Netherlands,
- Poland,
- Portugal,
- Romania,
- Slovakia,
- Spain,
- Sweden,
- United Kingdom.

II. Requirements and recommendations about API and PNR legislation by the UN, EU, OSCE, IATA and ICAO with examples of these being translated into national legislation

Advance Passenger Information (API)

European Union API Directive[1]

To combat illegal migration and to aid law enforcement, Member States must "introduce provisions laying down obligations on air carriers transporting passengers to the territory of the Member States" as follows:

- Communicate Passenger Data to authorities responsible for carrying out border checks on passengers
- Transmit the required data "by the end of check in"
- Forbid data being used for any other purpose other than migration and law enforcement
- Defines the data fields that are required as:
  - The number and type of travel document used
  - Nationality
  - Full names
  - Date of birth
  - The border crossing point of entry into the territory of the Member States
  - Code of transport (this is widely regarded as the flight number)
  - Departure and arrival time of the transportation
  - Total number of passengers carried on that transport
  - The initial point of embarkation (of each passenger)
- Sanctions (penalties/fines) will be imposed on airlines that do not send or that transmit incomplete or incorrect data
  - The minimum fine is to be more than €3,000
  - The maximum fine is to be more than €5,000
  - Higher sanctions can be made on airlines with serious infringements, including withdrawing the operating licence or confiscating or immobilising aircraft
  - Airlines have a right of appeal to these sanctions
- Data must be transmitted and collected electronically
- Data must be deleted by the authorities 24 hours after it was transmitted by the airline unless it is being actively used, for example in an investigation
- Airlines must be obliged to delete the data 24 hours after the flight arrives
- Airlines must inform passengers of the need to transmit passenger data

United Nations Security Council Resolution 2178[2]

UNSCR 2178 was passed in 2014 and describes how UN Member States should work to combat terrorism. The Resolution is far reaching, but the salient points regarding the application of API are as follows:

- UNSCR 2178 "calls upon Member States to require that airlines operating in their territories provide advance passenger information to the appropriate national authorities in order to detect the departure from their territories, or attempted entry into or transit through their territories, by means of civil aircraft, of individuals designated by the Committee" as posing a risk under this category of traveller.
- International cooperation is encouraged by UNSCR 2178 through the use of bilateral agreements that allow sharing of data "to prevent the travel of foreign terrorist fighters from or through their territories, including through increased sharing of information for the purpose of identifying foreign terrorist fighters, the sharing and adoption of best practices, and improved understanding of the patterns of travel by foreign terrorist fighters, and for Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law."

United Nations Security Council Resolution 2309[3]

UNSCR 2309 was passed in 2016 and describes how UN Member States should further work to combat terrorism particularly motivated by intolerance or violent extremism.

1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0082&from=en

2 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/547/98/PDF/N1454798.pdf?OpenElement

3 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/295/78/PDF/N1629578.pdf?OpenElement

UNSCR 2309 "calls upon all States, as part of their efforts to prevent and counter terrorist threats to civil aviation and acting consistent with relevant international legal instruments and framework documents, to:

- "Require that airlines operating in their territories provide advance passenger information to the appropriate national authorities in order to detect the departure from their territories, or attempted entry into or transit through their territories, by means of civil aircraft, of individuals designated by the Committee" as presenting a threat in accordance with the relevant definitions.
- "Urges States able to do so to assist in the delivery of effective and targeted capacity development, training and other necessary resources, technical assistance, technology transfers and programmes, where it is needed to enable all States to achieve the outcomes set out above.
- Calls upon all States to strengthen their international and regional cooperation to strengthen information-sharing, border control, law enforcement and criminal justice to better counter the threat posed by foreign terrorist fighters and returnees.
- Urges all States to ensure that all their relevant domestic departments, agencies and other entities work closely and effectively together on matters of aviation security."

OSCE Ministerial Council Decision 6/16 on Enhancing the Use of Advance Passenger Information[4]

In Hamburg, the OSCE Ministerial Council adopted Decision 6/16 on Enhancing the Use of Advance Passenger Information on 9 December 2016. The Decision supports implementation of the UN Security Council Resolutions 2170 (2014), 2178 (2014), 2309 (2016) and is aimed at prevention of movement of terrorists, terrorist groups and foreign terrorist fighters through effective border controls while fully respecting the obligations under international law, in particular international humanitarian law and international refugee law, including to ensure that refugee status is not abused by perpetrators, organizers or facilitators of terrorist acts. By the Decision, OSCE participating States committed to:

1. Establish national advance passenger information (API) systems in accordance with the provisions contained in ICAO's Annex 9 to the Convention on International Civil Aviation (the Chicago Convention) and aligned with the WCO/IATA/ICAO Guidelines on Advance Passenger Information (API), including those on privacy and data protection, in order to effectively collect passenger and/or crew data from airlines operating in their territories;
2. Consider establishing at the national level an interactive system to exchange API data (iAPI);
3. Adhere to ICAO Document 9082 "ICAO's Policies on Charges for Airports and Air Navigation Services" in the context of establishing an API system, recognizing that States are responsible for ensuring the implementation of adequate security measures at airports;
4. Collaborate with all relevant national stakeholders in the implementation of national-level API systems, and consider establishing one authority to receive, on behalf of all other authorities, all forms of passenger data through one single window data entry point;
5. Increase the added value of API data by seeking to establish automated cross-checking of this data against relevant national, regional and international watch lists, in particular INTERPOL databases and UN Sanctions Lists;
6. Provide assistance to support other requesting participating States in establishing an API system.

In order to intensify co-operation and support international efforts for enhancing aviation security and preventing the travel of foreign terrorist fighters, the OSCE Secretariat also signed the Memorandum of Understanding with IATA in Geneva on 14 October 2016.

ICAO Annex 9 to the Convention of International Civil Aviation - Facilitation (more commonly known as Chicago Convention Annex 9)

Annex 9 to the Chicago Convention deals with facilitation of passengers. Facilitation of passengers is the steps that are taken to process each passenger on their arrival at and departure from a border.

In October 2017 Annex 9 the Chicago Convention was updated to declare that:

- Each Contracting State shall establish an Advance Passenger Information (API) system.

ICAO has two levels of requirements when making statements about practices that are to be adopted:

- Recommended practice
- Standard

Recommended practices are activities that UN Member States should carry out, these are advisory recommendations, things that the UN believes are a good idea.

Standards are mandatory, UN Member States must carry out standards.

The implementation of API became a UN Standard on 23rd October 2017 and therefore UN Member States must implement API to be compliant with Annex 9 of the Chicago Convention.

4 https://www.osce.org/files/f/documents/4/f/288256.pdf

IATA/ICAO/WCO Guidelines on Advance Passenger Information (API)[5]

Joint guidelines issued by IATA/ICAO/WCO are not standards so do not have any legal standing. The following is provided for information purposes only.

The Guidelines define the requirement for API as arising from the paradox created by growing passenger numbers, stressed airport facilities, international terrorism, serious crime, and increasing pressure being put on personnel carrying out border checks. Pressure on personnel is increased due to many agencies working at the border without inter-agency cooperation, meaning the time taken to carry out passenger processing can be prolonged.

The API Guidelines describe the following:

- There are two versions of API
- Batch – airlines send API and get no response from the authorities
- Interactive – airlines send API and get a near real-time response from the authorities with an authority to carry each passenger, passengers that are ineligible to enter the destination country are denied boarding
- Batch API uses UN/EDIFACT PAXLST format and is usually sent via Type B Messaging over legacy airline service provider networks
- Interactive API (iAPI) can result in more benefits to airlines and governments by stopping ineligible passengers from travelling
- iAPI systems are usually more complex and expensive than Batch API
- Costs are borne by governments and airlines when implementing Batch API and iAPI
- ICAO has a target that all passengers should be processed through final clearance within 45 of disembarkation, API and iAPI may help achieve this target by pre-clearing passengers that present a low risk

Data Capture and Transmission:

- Data collected should be limited and uniform between countries to enable airlines to comply
- Governments should require the minimum data necessary and this should fall into two categories:
- Data relating to the flight header:
- Flight number
- Date and time of scheduled departure
- Date and time of scheduled arrival
- Last port of call
- Port of initial arrival
- Subsequent port of arrival
- Number of passengers on board
- Data relating to each passenger found in Machine Readable Zone (MRZ) of travel document:
- Travel document type and number
- Issuing state or organisation of travel document
- Travel document expiry number
- Family name and given name(s) of traveller
- Nationality of traveller
- Date of birth
- Gender
- Other data may be requested and the airline **might be able** to provide it if the information is available:
- Seat number
- Baggage information (tag number, number of pieces, weight)
- Traveller's status (passenger, crew, in-transit)
- Passenger Name Record Locator (also known as booking reference)
- Other data fields can be requested but are not recommended as these would have to be input manually by the airline check in staff.
- The data fields of Machine-Readable Travel Documents are defined by ICAO Standard 9303.
- If data is required other than that which is contained in the MRZ consideration should be given to collecting this in another way. Countries such as the USA and Canada do this by means of an Electronic Travel Authorisation.

IATA/ICAO/WCO summarise the legal aspects of API as follows:

There is a large degree of commonality within the provisions of [different countries'] legislation. Privacy and data protection legislation typically requires that personal data undergoing automated (computer) processing:

- should be obtained and processed fairly and lawfully
- should be stored for legitimate purposes and not used in any way incompatible with those purposes
- should be adequate, relevant and not excessive in relation to the purposes for which they are stored
- should be accurate and, where necessary, kept up to date
- should be preserved in a form which permits identification of the data subjects for no longer than is required for the purposes for which that data is stored

5 https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/api-guidelines-main-text_2014.pdf

Advance Passenger Information – Suggested points to Include in Ukrainian Legislation

Suggest key point to include	Mandated by	Examples in Other Legislation
Mandate collection and use of API	EU API Directive UNSCRs 2178, 2309 ICAO Annex 9	Canada: Subsection 107.1(1) of the Customs Act empowers the Minister to compel prescribed information about any person on board a conveyance in advance of their arrival in Canada. United Kingdom: Chapter 27B, Schedule 2, of the Immigration Act 1971: Passenger information must be provided by the carrier if an immigration officer asks the owner or agent. France: Code de la sécurité intérieure,. Partie législative (Articles L111-1 à L898-1) the Minister of the Interior is authorised to proceed with the implementation of automated processing of personal data, collected during international trips in from or to States not belonging to the European Union. Lithuania: Law on the Fundamentals of Transport Activities of the Republic of Lithuania and other relevant legislation: Air carriers must communicate passenger data (API and PNR), in line with the one-stop-shop principle, to the authorised Passenger Information Unit of Lithuania
Define purpose for requesting API	EU API Directive UNSCRs 2178, 2309	Canada: Passenger Information (Customs) Regulations: to identify individuals who may [have] involvement in, or connection to terrorism or terrorism-related crimes or other serious crimes, including organized crime that are trans-national in nature. Lithuania: Law on the Principles of Transport Activities: The data ….. shall be managed for the purposes of prevention, detection, investigation and criminal prosecution for terrorist offences and criminal activities associated with terrorism.
Name the competent authorities that will use the data	EU API Directive	United Kingdom: Immigration Act 1971, Schedule 2, 27B "The Secretary of State may by order require, or enable an immigration officer to require……." (This implies the Home Office and Immigration Officials from UK Border Force) France: Complete list of all agencies and the roles they play: Section 4 : Le traitement de données à caractère personnel «système API-PNR France» (Articles R232-12 à R232-22)[6]
Define how and when data must be sent	EU API Directive IATA API Toolkit	France: Code de la sécurité intérieure. Section 1: Transmission des données (Articles R232-1 à R232-1-1): "The personal data mentioned in article L. 232-4 of this code are transmitted by the air carriers, as soon as the flight is closed, by secure electronic transmission to the Ministry of the Interior, in UN/EDIFACT PAXLST message formats as defined in section 3.47.1 of Annex 9 of the Chicago Convention." Canada: Passenger Information (Customs) Regulations SOR/2003-219. Customs Act. Section 6. "The information referred to in section 5 must be provided by electronic means in accordance with the technical requirements, specifications and procedures for electronic data interchange set out in the document entitled CBSA Carrier Messaging Requirements established by the Agency, as amended from time to time." **and** Guidelines for Commercial Air Carriers for the Processing of Prescribed Traveller Information. Section 30 "For inbound flights, pursuant to paragraph 269(3)(a)-(b) of the IRPR, commercial air carriers are required to provide the prescribed API information to the CBSA at the following intervals: (a) For passengers: not later than the time of check-in; and (b) For crew members: no later than one hour before the time of departure to Canada.

6 https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042961132/

Define which data fields are required	EU API Directive[7] IATA API Toolkit	France: All API fields are listed. Code de la sécurité intériere, Section 4 : Le traitement de données à caractère personnel «système API-PNR France» (Articles R232-12 à R232-22), Part B[8] (Part A contains details of PNR) Canada: Passenger Information (Customs) Regulations SOR/2003-219, Customs Act, Part 5 – Prescribed Information lists all data fields required[9]
Define penalties for late, missing, or incorrect data	EU API Directive	Canada: Guidelines for Commercial Air Carriers for the Processing of Prescribed Traveller Information[10]. Section 63 to 68 France: Chapitre II : Traitements automatisés de données recueillies à l'occasion de déplacements internationaux (Articles L232-1 à L232-8)[11] "A fine of a maximum amount of 50,000 euros for each trip is punishable by an airline, sea or rail transport company disregarding the obligations set out in article L. 232-4."

Passenger Name Record (PNR)

European Union PNR Directive[12]

General Overview

The full title of the EU PNR Directive is "Directive (EU) 2016/681 of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime" and it was adopted on 27 April 2016. "The objectives of [the PNR] Directive are, inter alia, to ensure security, to protect life and safety of persons, and to create a legal framework for the protection of PNR data with regard to their processing by competent authorities."

In simplistic terms, the PNR Directive is concerned not only with the use of PNR to fight serious crime and terrorist offences, but also the protection of the data contained with PNR while it is being used by the relevant authorities.

The PNR Directive explains that through the use of PNR it may be possible to identify persons of interest that were previously unknown to law enforcement agencies, although the Directive also states that the use of PNR in this way should be limited to the prescribed reasons detailed within the Directive.

PNR is already collected and used by airlines as part of their day-to day operations. Airlines should not be requested to capture or process any data that is not already collected under normal operating circumstances. API may be collected as part of the PNR collection process and may be available with as a part of the PNR dataset.

API collected within the scope of the PNR Directive is protected under the rules of the PNR Directive. If governments require API for use outside the terms of the PNR Directive they should collect and use it within the scope of the API Directive.

Airlines that cannot send PNR due to technical or legal reasons may still be able to send API under the API Directive.

Processing of PNR data is to be "proportionate to the specific security goals" pursued by the Directive.

Annex 2 of the PNR Directive describes PNR may be used to tackle the following serious crimes:

1. participation in a criminal organisation,
2. trafficking in human beings,
3. sexual exploitation of children and child pornography,
4. illicit trafficking in narcotic drugs and psychotropic substances,
5. illicit trafficking in weapons, munitions and explosives,
6. corruption,
7. fraud, including that against the financial interests of the Union,

7 EU API Directive is being refreshed at present and the list of data fields in the Directive is incomplete, suggest not basing legislation for data fields on API Directive but to use examples from other laws or IATA API Toolkit

8 https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037305903

9 https://laws-lois.justice.gc.ca/eng/regulations/sor-2003-219/FullText.html

10 https://www.cbsa-asfc.gc.ca/publications/dm-md/d2/d2-5-11-eng.html

11 https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000025505275/

12 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0681&from=EN

8. laundering of the proceeds of crime and counterfeiting of currency, including the euro,
9. computer-related crime/cybercrime,
10. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
11. facilitation of unauthorised entry and residence,
12. murder, grievous bodily injury,
13. illicit trade in human organs and tissue,
14. kidnapping, illegal restraint and hostage-taking,
15. organised and armed robbery,
16. illicit trafficking in cultural goods, including antiques and works of art,
17. counterfeiting and piracy of products,
18. forgery of administrative documents and trafficking therein,
19. illicit trafficking in hormonal substances and other growth promoters,
20. illicit trafficking in nuclear or radioactive materials,
21. rape,
22. crimes within the jurisdiction of the International Criminal Court,
23. unlawful seizure of aircraft/ships,
24. sabotage,
25. trafficking in stolen vehicles,
26. industrial espionage.

PNR data should be sent by airlines to a "single designated passenger information unit (PIU) in the relevant Member State, so as to ensure clarity and reduce costs for air carriers. The PIU may have different branches in one Member State and Member States may also establish one PIU jointly." This means that a country may have more than one PIU, but governments should only ask for the PNR to be delivered once and to one location. Data may then be shared between different operational units or used in one multi-agency PIU. Airlines should not be asked to provide data to more than one location or agency.

EU Member States should bear the costs of using, retaining and exchanging PNR data.

The data that may be asked for is listed in Annex 1 to the PNR Directive and is as follows:

1. PNR record locator (Booking reference number)
2. Date of reservation/issue of ticket
3. Date(s) of intended travel
4. Name(s)
5. Address and contact information (telephone number, e-mail address)
6. All forms of payment information, including billing address
7. Complete travel itinerary for specific PNR
8. Frequent flyer information
9. Travel agency/travel agent
10. Travel status of passenger, including confirmations, check-in status, no-show or go-show information
11. Split/divided PNR information
12. General remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)
13. Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields
14. Seat number and other seat information
15. Code share information
16. All baggage information
17. Number and other names of travellers on the PNR
18. Any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time)
19. All historical changes to the PNR listed in numbers 1 to 18.

It should be noted that unlike API, PNR may contain blank fields. For example, if a passenger travels with hand luggage only there will be no information about baggage in the PNR. If an airline does not have a frequent flyer programme there will be no information about frequent flyer status.

Terrorist offences are defined as the offences under national law referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA[13] (Council Framework Decision of 13 June 2002 on combating terrorism).

Governments should use push rather than pull methods to obtain PNR data where possible. In other words,

13 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002F0475&from=EN

airlines should proactively send the data to governments (push), governments should not access airline systems to collect the data themselves (pull).

PNR should not be used in a way that discriminates against a person's "sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation." and "The PNR data should only contain details of passengers' reservations and travel itineraries that enable competent authorities to identify air passengers representing a threat to internal security."

The EU Commission supports ICAO's guidelines on PNR and these guidelines should be the basis for adopting supported data formats for the transfer of PNR from airlines.

Each country is responsible for identifying relevant threats related to serious crime and terrorism. This is not carried out at a central EU level.

PNR should not be used to deny refugees their right to claim asylum.

To prevent disproportionate of PNR, there is a need for country specific laws relating to the retention, depersonalisation, and deletion of PNR data. Depersonalised PNR can only be restored with permission from the highest level under very strict and controlled circumstances.

Depersonalisation of data means "to render those data elements which could serve to identify directly the data subject invisible to a user."

Processing of PNR must be carried out in accordance with Council Framework Decision 2008/977/JHA (The protection of personal data processed in the framework of police and judicial cooperation in criminal matters[14]) and also in accordance with any legislation that may replace this Framework Decision.

PNR data may be transferred outside the EU to third countries in accordance with the above Framework Decision, subject to the principles of necessity and proportionality and to the high level of protection provided by the Charter of Fundamental Rights of the European Union[15] and the European Convention on Human Rights[16]

PNR must be depersonalised after six months.

PNR must be deleted after a period of five years.

A data protection officer must be appointed to oversee the data protection requirements laid down in the Directive.

Passengers must be informed about the collection of their PNR and their rights relating to data protection and redress.

The EU PNR Directive permits Member States to collect, use, and store PNR from flights arriving from outside the Schengen Area, or if they desire, from flights operating within the Schengen Area too.

A Passenger Information Unit must be established: "Each Member State shall establish or designate an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime".

The PIU's functions include:

1. collecting PNR data from air carriers, storing and processing those data and transferring those data or the result of processing them to the competent authorities,
2. exchanging both PNR data and the result of processing those data with the PIUs of other Member States and with Europol

The PIU will be run by one or more "Competent Authority". The government should define and list the competent authorities that are entitled to request or receive PNR data, or to carry out the processing of the PNR data sent to the PIU so they may take action for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.

The PIU may only process the defined PNR data fields transferred by airlines, if any other data is received the PIU must delete it immediately.

The PIU may only process PNR for the following purposes:

a) "carrying out an assessment of passengers prior to their scheduled arrival in or departure from the Member State to identify persons who require further examination by the competent authorities referred to in Article 7, and, where relevant, by Europol in accordance with Article 10, in view of the fact that such persons may be involved in a terrorist offence or serious crime;
b) responding, on a case-by-case basis, to a duly reasoned request based on sufficient grounds from the competent authorities to provide and process PNR data in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime, and to provide the competent authorities or, where appropriate, Europol with the results of such processing; and
c) analysing PNR data for the purpose of updating or creating new criteria to be used in the assessments carried out under point (b) of paragraph 3 in order to identify any persons who may be involved in a terrorist offence or serious crime."

14 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008F0977&from=EN

15 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

16 https://www.echr.coe.int/Documents/Convention_ENG.pdf

Processing of PNR must be carried out in a non-discriminatory manner. Any pre-determined criteria must be targeted, proportionate and specific. States shall ensure that those criteria are set and regularly reviewed by the PIU in cooperation with the competent authorities. The criteria shall in no circumstances be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

Any matches or indication that a person is of interest to authorities must be verified by 'non- automated" means. In other words, a human must check the alert to verify if intervention is required. Once non-automated verification is complete, the relevant authority should be notified of the alert so they may take appropriate action.

The data protection officer must have access to all data processed by the PIU, if they are not satisfied that the data is being handled appropriately, lawfully, or with the correct degree of protection, they may refer this matter to the nation supervisory authority.

All data processing must be carried out within the territory EU Member States.

Obligations for Air Carriers

Governments shall require that airlines send the PNR data listed earlier in this document via a "push method". Airlines are obliged to send only the data that they already collect as part of their day-to-day business operations. Airlines are obliged to send the PNR to the departing and arriving territories if both of these are in the EU. For flights arriving into the EU, PNR for the arriving country is sufficient. For flights departing the EU, PNR for the country of departure is sufficient. Airlines may have other obligations to send PNR to countries outside the EU, depending on the rules in place at the time they operate the flight.

If API is sent as part of the PNR message, the rules detailed in the PNR Directive regarding data protection apply and not the rules described in the API Directive.

In times of technical failure or other unforeseen circumstances, PNR may be sent by an alternative means to the method usually used, proving an adequate level of data protection and security are used.

Data Retention

PNR should be sent by the airline to the PIU:

1. 24 to 48 hours before the scheduled flight departure time; and
2. Immediately after the flight is closed for boarding, meaning it is not possible for passengers to board or leave the aircraft before departure.

Governments may request additional transmissions of PNR if there is a specific threat relating to terrorism or serious crime on a case-by-case basis, should national law permit this.

EU Member states may transfer relevant PNR or the results of processing PNR to other PIUs in Member States. Similarly, Member States may request specific PNR from other Member States if it is relevant to investigations. Data that has been depersonalised may only be restored once the relevant authorization has been obtained.

Europol may also request PNR from Member States within the limitations of their competences and for the performance of their tasks.

Member States may transfer PNR to third countries on a case-by-case basis and only if the PNR is to be used for the same purposes as allowed in the PNR Directive and if the data will be protected to the same level as it would be within the EU.

All PNR shall be depersonalised six months after it is received. The depersonalisation of data means the following fields will be removed or masked so they cannot be read without decryption:

a) name(s), including the names of other passengers on the PNR and number of travellers on the PNR travelling together;

b) address and contact information;

c) all forms of payment information, including billing address, to the extent that it contains any information which could serve to identify directly the passenger to whom the PNR relate or any other persons;

d) frequent flyer information;

e) general remarks to the extent that they contain any information which could serve to identify directly the passenger to whom the PNR relate; and

f) any API data that have been collected.

Disclosure of the full PNR can only be authorised if it is believed it is strictly necessary for the purposes of preventing solving very serious crime including terrorism and it must be approved by:

a) judicial authority; or

b) another national authority competent under national law to verify whether the conditions for disclosure are met, subject to informing the data protection officer of the PIU and to an ex-post review by that data protection

officer.

All PNR must be permanently deleted after a period of five years unless the data is relevant to ongoing specific investigations or is being used in some other way that is compatible with the Directive.

All positive matches must be deleted as soon as the relevant authorities, other Member States, or third countries have been informed.

Matches that prove to be negative after non automated review may be kept to avoid future incidences of a "false positive" match being made.

Protection of Personal Data

Every passenger's data must be equally protected; they will have the right to access this data, and to seek correction, compensation, and rights of redress where appropriate in accordance with national law and Articles 17, 18, 19 and 20 of Framework Decision 2008/977/JHA[17].

Member States must prohibit the processing of PNR data revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. In the event that PNR data revealing such information are received by the PIU, they must be deleted immediately.

PIUs must maintain documents explaining their processing systems and procedures covering at least:

a) the name and contact details of the organisation and personnel in the PIU entrusted with the processing of the PNR data and the different levels of access authorisation;

b) the requests made by competent authorities and PIUs of other Member States;

c) all requests for and transfers of PNR data to a third country.

This information must be made available to the national data protection supervisory authority should they request it.

The PIU must keep records of collection, consultation, disclosure and erasure of data. The records of consultation and disclosure must show, in particular, the purpose, date and time of such operations and, as far as possible, the identity of the person who consulted or disclosed the PNR data and the identity of recipients of the data. These records will be used solely for the purposes of verification, of self-monitoring, of ensuring data integrity and data security or of auditing. The PIU shall make the records available, upon request, to the national supervisory authority. The records must be kept for five years.

In case of potential data security breach, the PIU must contact the subject whose data has been breached to inform them of the incident without delay.

Penalties

Penalties for airlines who do not send data at all, or who send it late, or not in the required format, must be able to be penalised. The penalties are not defined in the Directive, but it is stated that "penalties provided for shall be effective, proportionate and dissuasive"

National Supervisory Authority

Each Member State must provide a national supervisory body in accordance with Article 25 of Framework Decision 2008/977/JHA[18].

The supervisory body ensures fundamental rights are protected in relation to the processing of personal data as well as dealing with complaints logged by data subjects and verifies the lawfulness of the ongoing data processing.

Airlines must send PNR data to PIUs for the relevant purposes by electronic means that are sufficiently secure. In case of technical failure or difficulties, another appropriately secure means of transmission may be agreed providing data security and protection laws are obeyed.

The data protocols that governments may offer to airlines to send PNR are[19]:

- IBM MQ Series,
- IATA Type B,
- AS4

United Nations Security Council Resolution 2396[20]

17 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008F0977&from=EN

18 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008F0977&from=EN

19 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1309-Passenger-name-record-PNR-data-formats-and-transmission-protocols_en Annex (2nd Document)

20 https://undocs.org/S/RES/2396(2017)

United Nations Security Council Resolution 2396 was adopted on 21st December 2017 and has the primary objective of preventing the spread of terrorism, including radicalisation of individuals, and the movement of foreign terrorist fighters.

The stated main objectives of the Resolution are:

- to prevent the movement of terrorists by effective national border controls and controls on issuance and identification of forged identity papers and travel documents;
- to notify relevant countries, in a timely manner, upon travel, arrival, or deportation of captured or detained individuals whom they have reasonable grounds to believe are terrorists, including suspected foreign terrorist fighters, including any additional relevant information about the individuals, to act quickly and to share such information with INTERPOL;
- to assess and investigate individuals whom they have reasonable grounds to believe are terrorists, and distinguish them from other individuals, by employing evidence-based risk assessments, screening procedures, and the collection and analysis of travel data, in accordance with domestic and international law, including international human rights and humanitarian law, as applicable, without resorting to profiling based on any discriminatory ground prohibited by international law;
- to share appropriate information quickly and securely in line with international agreements, respecting all human rights and data security aspects;
- to create and use watchlists containing details of suspected terrorists;
- biometrics should be deployed to verify identity of travellers and to screen against the known biometric features of suspected terrorists

There are several strong references to the collection of PNR in line with human rights and data protection requirements, for example "with full respect for human rights and fundamental freedoms for the purpose of preventing, detecting and investigating terrorist offenses [sic] and related travel."

The Resolution states that the concerns that lead to the UN taking the steps regarding PNR are "that Foreign Terrorist Fighters may use civil aviation both as a means of transportation and as a target, and may use cargo both to target civil aviation and as a means of shipment of materiel".

The Resolution states that Member States should cooperate with the agencies that would benefit most from the use of PNR, calling upon Member States "to improve timely information sharing, through appropriate channels and arrangements, and consistent with international and domestic law, on foreign terrorist fighters, especially among law enforcement, intelligence, counterterrorism, and special services agencies, to aid in determining the risk foreign terrorist fighters pose, and preventing them from planning, directing, conducting, or recruiting for or inspiring others to commit terrorist attacks."

United Nations Security Council Resolution 2482[21]

United Nations Security Council Resolution 2482 was adopted on 19th July 2019 and is focused on the prevention of international organised serious crime, including violent extremism, terrorism, trafficking of drugs and persons, and money laundering.

PNR is mentioned in only one section of the Resolution; however, it is noticeable that the aims of the resolution are often the primary drivers for other countries introducing API and PNR systems. Topics such as counter terrorism and fighting international organised crime are high priorities for almost every country.

PNR is mentioned in only one section of the Resolution, adherence to the ICAO standards and recommended practices is encouraged, along with the sharing of relevant information in accordance with human rights and data protection laws.

The Resolution calls upon Member States to: "implement obligations to collect and analyse Advance Passenger Information (API) and develop the ability to collect, process and analyse, in furtherance of International Civil Aviation Organization (ICAO) standards recommended practices, Passenger Name Record (PNR) data and to ensure PNR data is used by and shared with competent national authorities, with full respect for human rights and fundamental freedoms, which will help security officials make connections between individuals associated to organized crime, whether domestic or transnational, and terrorists, to stop terrorist travel and prosecute terrorism and organized crime, whether domestic or transnational, including by making use of capacity building programmes."

The Resolution also calls for Member States to make "best use of" INTERPOL policing capabilities, including analytical databases. Countries that have access to INTERPOL data sources always use these when processing PNR to check for a number of risks, including lost or stolen documents, wanted persons, and travel documents with notices or alerts.

21 http://unscr.com/en/resolutions/doc/2482

Summary list of requirements and obligations as per EU PNR Directive

The European Union Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime[22], commonly referred to as the "EU PNR Directive", contains mandatory requirements with which EU Member States implementing the Directive must comply. These requirements are listed below to aid understanding of these obligations.

Appoint a "competent authority". This means that there must be a named agency responsible for overseeing the implementation of PNR. For PNR this can be customs, but it may also be the border agency, the security service, or any other relevant agency. In many cases the agency that will make most use of the information gained from analysing the PNR will be appointed the lead agency.

Create a PIU (Passenger Information Unit) led by the competent authority to oversee and manage the collection, analysis, storage, sharing, and deletion of PNR.

Create a means whereby airlines can send PNR to the PIU using a "Push" method and common standards and protocols. The protocols are detailed in a very comprehensive document written and maintained by IATA's PADIS working group (the International Air Transport Association Passenger and Airport Data Interchange Standards working group), This document is titled PNR EDIFACT/XML Implementation Guide and there are a number of versions of the document available[23]. Governments will have to decide which version of PNR they will require from airlines and follow the instructions in the appropriate version of the guide. When choosing which version of PNR to implement, a number of factors will need to be taken into account, including determining which version of PNR is appropriate for the government's needs as well as considering the capabilities of the airlines at the time of implementation. OSCE can provide relevant guidance at the appropriate time on request.

A list of permitted data fields within PNR is included in an Appendix to the Directive. It is worth noting that API received within PNR can be treated under the data retention rules of the PNR Directive rather than those of the API Directive. API received as part of PNR must be kept for 5 years and depersonalised after 6 months. There are 19 data elements listed in the Annex. The 19th data element can cause confusion as it any updates to fields that have been changed, rather than a data field in its own right.

The permitted data elements within PNR are:

1. PNR record locator, sometimes referred to as the "booking reference number"
2. Date of reservation/issue of ticket
3. Date(s) of intended travel
4. Name(s)
5. Address and contact information (telephone number, e-mail address)
6. All forms of payment information, including billing address
7. Complete travel itinerary for specific PNR
8. Frequent flyer information
9. Travel agency/travel agent
10. Travel status of passenger, including confirmations, check-in status, no-show or go-show information
11. Split/divided PNR information
12. General remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)
13. Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields
14. Seat number and other seat information
15. Code share information
16. All baggage information
17. Number and other names of travellers on the PNR
18. Any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time)
19. All historical changes to the PNR listed in numbers 1 to 18.

Airlines can only send the PNR data that they collect in the normal course of their business. It is worth remembering that PNR is different to API in that there may be empty fields. Airlines can only provide information that is collected in the course of their usual business activities, if the airline does not collect a particular element, it cannot be provided. Additionally, if a passenger travels with hand luggage only the baggage element of the PNR will be empty.

Collect PNR for arriving and departing international flights.

Appoint a data protection officer. The appointment of an independent data protection officer is a key part of the

22 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0681&from=EN

23 https://www.iata.org/en/publications/api-pnr-toolkit/#tab-3

Directive. This ensures that the PIU adheres to local and EU regulations about the protection of all data, with a particular importance placed on data security, protection, deletion, depersonalisation, and ensures the PNR data is only used for the permitted reasons defined in Annex 2 of the Directive (detailed later in this document).

Keep PNR data for five years after which it must be deleted so that it is not possible for it to be recovered. Data that is being used for permitted purposes may be kept as long as it is being actively used, for example, in the course of an investigation.

PNR must be depersonalised six months after receipt and can only be restored with authority of a judge or similar person in authority.

PNR may only be used to detect or prevent the actions of those involved in terrorism or very serious crimes. The 26 very serious crimes relating to the PNR Directive are listed in Appendix 2 to the PNR Directive and are as follows:

1. participation in a criminal organisation,
2. trafficking in human beings,
3. sexual exploitation of children and child pornography,
4. illicit trafficking in narcotic drugs and psychotropic substances,
5. illicit trafficking in weapons, munitions and explosives,
6. corruption,
7. fraud, including that against the financial interests of the Union,
8. laundering of the proceeds of crime and counterfeiting of currency, including the euro,
9. computer-related crime/cybercrime,
10. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
11. facilitation of unauthorised entry and residence,
12. murder, grievous bodily injury,
13. illicit trade in human organs and tissue,
14. kidnapping, illegal restraint and hostage-taking,
15. organised and armed robbery,
16. illicit trafficking in cultural goods, including antiques and works of art,
17. counterfeiting and piracy of products,
18. forgery of administrative documents and trafficking therein,
19. illicit trafficking in hormonal substances and other growth promoters,
20. illicit trafficking in nuclear or radioactive materials,
21. rape,
22. crimes within the jurisdiction of the International Criminal Court,
23. unlawful seizure of aircraft/ships,
24. sabotage,
25. trafficking in stolen vehicles,
26. industrial espionage.

This summary list of requirements is not intended to replace the EU PNR Directive and is provided as an aid to assist with understanding and appreciating the key specific activities and actions that are detailed within the Directive. It is provided for information purposes only.

Examples of PNR legislation in other countries

The PNR Directive is much more prescriptive than the API Directive (as at 31/10/2021) and offers less scope for individual states to have different interpretations of the requirements. EU Member States have mostly transcribed the EU PNR Directive in its entirety into their own national legislation. Due to this simplicity, finding examples of and undertaking analysis of PNR legislation is simpler than that of API.

Netherlands

The legislation in the Netherlands[24] is very clear and simple to follow. All the points in the Directive are contained in the Dutch legislation, albeit in a slightly different order and some topics have been joined together. The Dutch legislation is only available in Dutch so caution should be used when considering the following information as it was translated by means of an online tool. The Dutch legislation covers the following topics:

- Airline obligations
- Passenger Information Unit (PIU)
- Processing of data at the PIU
- Competent authorities
- Exchanging data with other states, Europol, and third countries

24 https://wetten.overheid.nl/BWBR0042301/2019-06-18/

- Requests to other states
- Data protection
- Enforcement and sanctions
- The list of both the Directives annexes detailing the data fields and the permitted uses of PNR

Germany

The legislation relating to the collection and use of PNR in Germany is the Act on the Processing of Passenger Name Record (PNR) Data to Implement Directive (EU) 2016/681 (Passenger Name Record Act, FlugDaG)[25]. The opening lines of this legislation state that its objective is to "transpose into national law Directive (EU) 2016/681 of the European Parliament", the legislation appears very close in spirit and in meaning to the EU PNR Directive and includes the following headings:

- Passenger Information Unit and the purpose of the PNR database
- Data transfer by air carriers (includes a list of all required data fields)
- Conditions of processing
- Depersonalization of data
- Transfer of data to other competent authorities
- Exchange of data between EU Member States
- Joint procedures for cooperation
- Transfer of data to Europol
- Data protection officer
- Deletion of data

Lithuania

The legislation relating to the collection and use of PNR in Lithuania is the Lithuanian Police Commissioner General's Order on the Approval of the Description of the Procedure for Ticket Booking and Departure Control, Provision of Passenger Flight Data and Air Carrier Information to Passenger Information Unit of 23rd December 2016 No. 5-V-1091[26]. The Lithuanian legislation differs from the examples already given in terms of some additional information provided, but the core information from the EU PNR Directive is still reflected in the content of the law.

Like Germany, Lithuania's objective in their PNR legislation was, among others, to "implement the provisions of the Directive (EU) 2016/681 of the European Parliament" and the content of their legislation follows a similar pattern to the legislation already described, although the language and format used are slightly different.

The initial section of the legislation is titled "General Provisions" and the following concepts or practices are outlined:

- Air Carriers
- Passenger Information Unit
- Passenger Name Records
- Passenger Name Record Information System
- Extra-EU flight
- Intra-EU flight
- Passenger
- Reservation System

The next section describes procedures, manners, formats and terms for provision of passenger data and describes how and when airlines must send data to the PIU including transmission protocols and data formats. Details are also given about transmission of data in times of technical difficulties and the practices to be undertaken if a flight is operated under a code share agreement.

The third section of the law describes the practical details for sending the information to the Lithuanian PIU including commencement of data transfer, what data will actually be sent by the carrier, the airline's chosen transmission formats and protocols, details of designated contacts at the airline to deal with queries, and details of who may be contacted during the testing period after and airline commences sending PNR.

The forth section of the legislation contains more information about the provision of passenger data to the PIU and the procedures airlines must follow when setting up the data transfer of PNR. Details of flight schedules must be provided by the airport to the Police.

The final section of the legislation is a table for the airline to complete with many fields to fill in. There is a request for information about all practical details of an airline beginning to send PNR as well as a list of all the data fields the Lithuanian authorities are asking the airlines to send to the PIU. Some of the data fields have been broken out into more than one box in the table in the legislation, so there is the potential for some confusion about exactly how much information is being requested and whether or not more information is being requested than is required in the

25 https://www.gesetze-im-internet.de/englisch_flugdag/englisch_flugdag.html

26 https://www.ltou.lt/uploads/documents/files/corporate/aircraft-services/airport-charges/Description%20EN.pdf

EU PNR Directive. Also included in the form is a statement about the fact that the airline has briefed their staff on the importance of sending data and that the data collected and sent must be treated in a proper manner according to the appropriate legislation.

The Lithuanian legislation is very different to those of the Netherlands and Germany and stands as an example of how EU Member States have the flexibility they need when transposing EU Legislation into their own laws. Each country's legal system is different and will require a different approach based on their unique circumstances.

Conclusion

Although the API and PNR Directives and the United Nations Security Council Resolutions are issued and apply equally to the countries having an obligation to implement them, it is clear each country has taken their own approach to transposing the Directives into their own legislation.

Each country has their own legal system, some are based on precedent and case law and require less detail while other nations' legal systems are fully codified meaning laws passed need to be detailed and contain instructions about every element relating to API and PNR.

It is also important to recognise that while any legislation passed in Ukraine would have to be appropriate to Ukraine's own legal system, deviation from the EU Directives may make it impossible for airlines based in other countries to send passenger data to Ukraine as foreign airlines must comply with the regulations in place where they are based.

Legislation in countries with a fully codified legal system may need to be updated should API and/or PNR evolve and change over time. If new data fields are introduced or other changes are made, countries with prescriptive and detailed laws may find they need to make amendments to their passenger data legislation.

It is common practice for governments to keep API and PNR legislation separate, addressing each EU Directive and dataset individually as the requirements of each are quite different in terms of data protection and data fields. This gives airlines that cannot send PNR due to the lack of a legal agreement with the EU for example, the opportunity to send API as the rules around sending API outside the EU are much more relaxed than sending PNR outside the EU. There is a risk that laws that combine API and PNR may prohibit airlines that cannot send PNR from sending any information at all.

The EU Directives on API and PNR do not conflict with the various UN Security Council Resolutions. The Resolutions compel governments to implement API and PNR for a range of reasons, most are related to preventing terrorism and other serious cross border crime. This is aligned with the EU Directives.

Any legal discussion in this document is based on experience of common international practice and is not intended as legal advice. OSCE can provide specialist legal advice relating to any new or changed API/PNR legislation to Ukraine should this be of interest.

III. National Legislation in API/PNR

United Kingdom

Overview

The United Kingdom started their API project in 2003[27]. The project has evolved over time, as a few different systems and service providers, and includes a requirement for passenger information to be sent by airlines, shipping companies and trains using the Eurotunnel, connecting the UK and mainland Europe.

In the United Kingdom, the requirement for airlines and shipping companies to send passenger information is found in Chapter 27B, Schedule 2, of the Immigration Act 1971. The Immigration Act has been updated over several years to reflect the changing landscape as regards the requirement for airlines and ships. Information is required for journeys that both arrive in and depart from the United Kingdom. Updates to the Immigration Act were made to take into account new requirements and changes being made in other UK laws, including the Immigration, Asylum, and Nationality Act 2006, the UK Borders Act 2007, and the Counter-Terrorism and Security Act 2015.

Passenger information must be provided by the carrier "if an immigration officer asks the owner or agent". Similar requirements can be found in many API and/or PNR laws as it offers a degree of flexibility between the time the law is passed and when it is enforced. There is usually a period of several months between the law being passed and the airlines or shipping companies starting to send the required information. There can also be a period of several months between a law being passed and the government being able to process any information that may be sent. Clauses asking for information on request help ensure a government is not in breach of its own law requiring carriers to send passenger information during the implementation of API and PNR projects.

Comparisons of UK law to that of other countries

The legislation in force in the UK differs from many countries' legislation in that it is generic, rather than specific in nature. Some countries list all the data fields that are required in API and PNR, the UK Immigration Act does not. There are requirements to send information about the persons on board, and information about the voyage or flight. The reason for the lack of detail around data fields may be that the UK requires passenger information from both airlines and shipping companies, API and PNR are datasets that are specific to aviation. If the Immigration Act specified API and PNR data fields it may have made collecting the required information from ships as well as international trains more challenging from a legal perspective.

The UK Immigration Act is also unusual in that it does not specify how or when the information should be sent to the authorities. Carriers wishing to start service to the UK are directed to email the relevant authority in the UK and seek instructions as to how to proceed[28]. It is possible that, as there is a requirement for airlines, maritime carriers, and international trains to send information, it may be the intention of the UK authorities to avoid confusion and to instruct each carrier according to their specific situation.

Many countries' legislation details the penalties that are in place for non-compliance with a request to send passenger information, the UK Immigration Act does not. The law does explain that penalties can be enforced against carriers that do not submit the required passenger information, but there are no details about how much a potential fine may be. Further research found that in October 2020, the fine in place for carriers failing to provide complete or accurate API was up to £10,000 per incident[29] (approximately 372,300 UAH at the time of writing this report).

The method and times of transmission of passenger data are not described in the UK legislation. Part 8 of Chapter 27B, Schedule 2 of the UK Immigration Act states that "The information must be provided a) in such form and manner as the Secretary of State may direct; and b) at such time as may be stated in the request." Many countries detail the transmission means and may include text such as "transmission via direct MQ connection or aviation industry standard messaging", as well as detailing when passenger data should be sent.

Data protection is not mentioned in the UK Immigration Act, although all data processed in the UK will fall under the Data Protection Act 2018, which is broadly aligned with the EU GDPR and offers high levels of protection for all data that is transmitted, received, or stored in the United Kingdom.

27 National Audit Office. E-Borders and successor programmes. https://www.nao.org.uk/report/home-office-e-borders-and-successor-programmes/

28 Border Force API (advance passenger information) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/300741/CarrierInformation.pdf

29 Independent Chief Inspector of Borders and Immigration, An inspection of the Home Office's use of sanctions and penalties (November 2019 – October 2020) Figure 2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/951438/An_inspection_of_the_Home_Office_s_use_of_sanctions_and_penalties__November_2019___October_2020_.pdf

When requesting API and PNR from airlines, the UK Home Office provides carriers with details of the passenger information that is required, there is one document for API, and another for PNR.

The documents detailing the information and when it must be sent by carriers brings the UK's practices in line with those of most other countries, even though the level of detail in the law itself is less detailed than is often found in other countries. As the documents refer to the UK Immigration Act, there is sufficient legal basis for airlines flying to the UK from all over the world to send passenger information to the UK authorities when requested.

Compatibility with UNSC Resolutions, OSCE Ministerial Council Decision 6/16, and IATA/ICAO/ WCO API-PNR Toolkit

In implementing API and PNR, the United Kingdom's practices around passenger data are aligned with the UN Security Council Resolutions. The UK is using API and PNR for all flights originating overseas to reduce very serious crime, illegal activity, and activities relating to terrorism.

The United Kingdom's decision to implement API and PNR is compatible with the OSCE Ministerial Council Decision 6/16 to require participating states to implement API systems in accordance with international best practices and guidelines laid down by ICAO and others.

When read with the specific instructions issued to carriers at the time that API and PNR is requested, the UK legislation is in accordance with the IATA/ICAO/WCO API – PNR Toolkit in that all the data fields, timings of data transmission, methods of connection, and other technical details adhere to the guidelines issued.

The UK left the European Union at the beginning of 2021; however, the laws and practices in the UK remain aligned with those of the EU. In June 2021, the relevant body in the EU stated that data transfers within the scope of EU GDPR had no implications for the transfer of PNR data or API to the UK. This means that the UK continues to be able to require PNR data from all airlines based within the EU without further legislation[30].

Gender issues are not apparent in the legislation relating to the collection and transmission of passenger data to the United Kingdom.

Netherlands

Overview

The Netherlands began working with API in 2009[31] when a pilot programme to receive and process API from a limited number of airlines was launched. In 2012, a full API programme was launched and the number of airlines connected and sending API increased. The Dutch authorities may request any airline operating flights from outside the European Union to send API to the Netherlands[32]. The agency responsible for collecting and analysing API in the Netherlands is the Royal Netherlands Marechaussee, part of the Ministry of Defence. The Royal Netherlands Marechaussee is responsible for securing the borders of the Netherlands and may be considered as the border guard, although they have other duties too. The use of API is controlled by the Aliens Act (2000), Chapter 2, Part 4[33] which states "The carrier … may be obliged to collect passenger data or data about the crew for the purpose of border control and the prevention of illegal immigration and to provide it to the officials charged with border control." The Dutch began collecting and using PNR in June 2019[34], requiring information to be sent to the Passenger Information Unit for all flights arriving in and departing from the Netherlands[35]. Customs only receives information about PNR for arriving flights.

PNR is collected and used by Customs and the Passenger Information Unit, it is mandated and authorised by the Use of Passenger Information (Terrorist Offences and Other Serious Crimes) Act, the Union Customs Code, and the General Customs Act. There are links to each of these acts provided in a table later in this section.

The Dutch government has provided the following table on their website to help travellers understand which agency uses API and PNR, for what purposes, how long it is kept for, and which legislation is applicable.[36] This table is useful in helping to understand who uses the data, how long it is kept for, for which purposes, and which legislation applies.

30 Data protection: Commission adopts adequacy decisions for the UK https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183

31 https://www.airport-technology.com/contractors/consult/arinc-airports/pressreleases/pressarinc-delivers-advance-passenger-information-service/

32 https://english.defensie.nl/topics/border-controls/passenger-data-and-border-controls

33 https://wetten.overheid.nl/BWBR0011823/2019-02-27

34 https://www.privacy-ticker.com/the-netherlands-passed-new-law-on-the-use-of-passenger-data/

35 https://www.government.nl/topics/aviation/air-passenger-travel-information

36 https://www.government.nl/topics/aviation/air-passenger-travel-information

Organisation	Pi-NL	Customs	Royal Military and Border Police (KMar)
Passenger information	PNR	PNR	API
Tasks	Combating terrorism and other serious crimes	Checks on passengers' baggage	Combating illegal migration Border checks on of individuals
Flights	All flights arriving in or departing from the Netherlands (from and to countries both within and outside the European Union)	All flights arriving in the Netherlands from a location outside the EU All flights departing from the Netherlands to a destination outside the EU	All flights arriving in the Netherlands from a location outside the EU All flights arriving in the Netherlands from a location in Europe outside the Schengen area
Retention period for information	5 years	48 hours	24 hours, or longer if further investigation is required; in that case, the period laid down by the Police Data Act (WPG) (in Dutch)
Legislation	Use of Passenger Information (Terrorist Offences and Other Serious Crimes) Act (in Dutch)	• Union Customs Code (UCC) and the General Customs Act (in Dutch)	Aliens Act 2000 (in Dutch)

Comparisons of Dutch law to that of other countries

All the legislation relating to the collection and use of API and PNR in the Netherlands is provided in Dutch. Translations of the relevant legislation was undertaken using automated tools, including Google Translate, and this should be remembered when making use of the information provided. When viewing sources of information, the use of a browser with inbuilt translation tools, such as Google Chrome, may be helpful.

The law relating to API, the Aliens Act (2000), does not refer to the specific data fields that are required, but these are listed elsewhere on the Royal Marechaussee's website[37]. The list is compliant with the guidelines contained in the IATA API Toolkit. The Aliens Act is also clear that information may be required for both passengers and crew.

A challenge for some countries that have used their own Aliens Act or equivalent, such as the Law on Foreigners, is that they have not been able to request or use API and/or PNR from the own citizens. This is something Ukraine may wish to bear in mind when deciding where to place their own laws relating to passenger data.

The Use of Passenger Information to Combat Serious Crimes Act details how PNR may be collected and used. As expected for a law passed by a European Union Member State, the act is completely aligned with the EU PNR Directive in that it lists the 19 data fields, describes the criminal activity that will be targeted by the use of PNR, and prescribes the strict rules around data privacy and protection.

The Use of Passenger Information to Combat Serious Crimes Act also details how airlines must send PNR once (or more if directed by a Minister) between 48 and 24 hours before departure, and again after the flight has closed, boarded and ready for departure.

The competent authorities that may process and use PNR are described as: the public prosecutor's office, the police, the special investigative services, the Royal Netherlands Marechaussee, and the National Criminal Investigation Department.

The API and PNR laws in place in the Netherlands are aligned with the relevant EU Directives and mirror the majority of other European Union Member States.

Compatibility with UNSC Resolutions, OSCE Ministerial Council Decision 6/16, and IATA/ICAO/ WCO API-PNR Toolkit

In implementing API and PNR, the Netherland's practices around passenger data are aligned with the UN Security Council Resolutions. The Netherlands is using API and PNR for all flights originating outside the European Union and Schengen Zone, and PNR only for flights within the EU/Schengen Zone to reduce very serious crime, illegal activity and activities relating to terrorism.

The Netherland's decision to implement API and PNR is compatible with the OSCE Ministerial Council Decision 6/16 to require participating states to implement API systems in accordance with international best practices and guidelines laid down by ICAO and others.

37 https://www.defensie.nl/onderwerpen/taken-in-nederland/grenstoezicht/passagiersgegevens-en-privacy

When read with the specific instructions issued to carriers at the time that API and PNR is requested, the Dutch legislation is in accordance with the IATA/ICAO/WCO API – PNR Toolkit in that all the data fields, timings of data transmission, methods of connection, and other technical details adhere to the guidelines issued.

Gender issues are not apparent in the legislation relating to the collection and transmission of passenger data to the Netherlands.

Canada

Overview

The Advance Passenger Information/Passenger Name Record (API/PNR) program is designed to protect Canadians by enabling the Canada Border Services Agency (CBSA) to perform a risk assessment of travellers prior to their arrival in Canada and to identify those who require further examination upon arrival.

API/PNR may be used for the purpose of identifying persons who are or may be involved with or connected to terrorism or terrorism-related crimes or other serious crimes, including organized crime, that are transnational in nature.

The CBSA operates within the "Guidelines on API" put forward by World Customs Organization (WCO)/International Civil Aviation Organization (ICAO)/International Air Transport Association (IATA). API is defined in the *Immigration and Refugee Protection Regulations (IRPR)* and the *Passenger Information (Customs) Regulations (PICR)* as the following information, to be transmitted before arrival in Canada:

a) their surname, first name and initial or initials of any middle names;

b) their date of birth;

c) the country that issued them a passport or travel document or, if they do not have a passport or travel document, their citizenship or nationality;

d) their gender;

e) their passport number or, if they do not have a passport, the number on the travel document that identifies them; and

f) their reservation record locator or file number.

The CBSA collects up to 25 PNR data elements under the API/PNR program.

The CBSA took a phased-in implementation approach to the API/PNR program:

- Implementation of the API component of the program commenced on October 7, 2002
- Implementation of the PNR component of the program commenced on July 8, 2003

The program has grown steadily since 2003, when only 23 carriers provided API and 6 carriers provided PNR. Today, 263 carries provide API and 98 carriers provide PNR representing over 90% of all international air passengers to Canada (the majority of carriers not providing PNR are smaller airlines or discount airlines).

The receipt, use, retention, disclosure and disposal of API/PNR information is governed by numerous pieces of legislation and regulations. The following information outlines the existing legislation and regulations:

- Subsection 107.1(1) of the *Customs Act* empowers the Minister to compel prescribed information about any person on board a conveyance in advance of their arrival in Canada. https://laws-lois.justice.gc.ca/eng/acts/c-52.6/index.html
- The *Passenger Information (Customs) Regulations* under this Act set out specifics related to the collection of this information. https://laws-lois.justice.gc.ca/eng/regulations/sor-2003-219/index.html
  1. Required from commercial carriers, charterers, travel agents, and owners/operators of a reservation system
  2. Prescribed information to be transmitted (API/PNR)
  3. Prescribed conditions for data transmission
- Paragraph 148.(1)(d) and 149 (a) of the *Immigration and Refugee Protection Act* (*IRPA)* requires transportation companies to provide prescribed information on all persons being transported to Canada. https://laws-lois.justice.gc.ca/eng/acts/i-2.5/
  1. Regulation 269 under this Act defines the specific information to be provided (i.e., API/PNR).
  2. The *Protection of Passenger Information Regulations* under this Act restrict the CBSA's actions related to collection, retention, use, access and disclosure of API/PNR information.
- Section 269 of the Immigration and Refugee Protection Regulations details who is required to provide API/PNR information. It outlines the specific information required and indicates how access to that information is to be provided. https://laws-lois.justice.gc.ca/eng/regulations/sor-2002-227/
- *The Protection of Passenger Information Regulations (PPIR)* is made under section 150.1 of the Immigration and Refugee Protection Act. It governs the CBSA's actions related to the collection, retention, use, access and disclosure of PNR information. https://laws.justice.gc.ca/eng/regulations/SOR-2005-346/index.html
- *CBSA's Departmental Memorandum D1-16-3*: Guidelines for the Access to and Disclosure of Advance Passenger

Information (API) and Passenger Name Record (PNR) Data. http://www.cbsa-asfc.gc.ca/publications/dm-md/d1/d1-16-3-eng.html

API/PNR data is defined as "personal information" under Canadian law and is protected by:

1. *Privacy Act*
2. *Canadian Charter of Rights and Freedoms*
3. *Personal Information Protection and Electronic Documents Act (PIPEDA)*
4. *Protection of Passenger Information Regulations*

To ensure compliance with domestic and international privacy requirements:

1. The PNR data elements collected are limited.
2. API/PNR data is retained for 3.5 years but becomes increasingly depersonalized with time. Access and disclosure are severely restricted throughout the retention period.
3. The number of CBSA officials with access to API/PNR is limited.
4. API/PNR is purged from the CBSA system when the retention period has expired.
5. Any traveller can request a copy of their API/PNR data from CBSA.

Any traveller can request that corrections be made to their API/PNR data.

All commercial air carriers must transmit the API of every person (including passengers and crew) on board of an aircraft destined to Canada; however, PNR is available for passengers only. The CBSA does not require carriers to provide any PNR information that they do not collect for their own purposes.

A dedicated CBSA client service team works with air carriers during implementation and to ensure continued compliance. The CBSA client service team works with all airlines that provide API/PNR and follow-up with air carriers when there are issues with not receiving data. They meet with carriers to explain Canada's legislative requirements and the carrier's responsibility to submit API/PNR. Carriers need to ensure that their systems are functioning properly for the processing of API and PNR data and that appropriate standard operating procedures are put in place.

API must be transmitted in a prescribed format (passenger manifest) in accordance with CBSA technical requirements. A penalty regime exists for failure to provide API/PNR ($3000 CAD per flight).

Gender issues are not apparent in the legislation relating to the collection and transmission of passenger data to Canada.

France

Overview

European Union (EU) Directive 2016/681 on the use of Passenger Name Record (PNR) data was adopted on 27 April 2016. It requires EU Member States to collect and use both PNR data and Advanced Passenger Information (API) "for the prevention, detection, investigation and prosecution of terrorist offences and serious crime." The Member States have two years to transpose the Directive into their national law, by which time it must be ready for implementation.

The Directive stipulates that a Passenger Information Unit (PIU) responsible for collecting, storing and processing data should be set up in each Member State. According to the text, any hits or positive results must be sent by the PIU to the operational units referred to as "competent authorities." In addition, the Directive also covers data exchange between PIUs and with Europol, as well as with third countries on a case by case basis.

Moreover, the Directive also stipulates that implementing acts should be drafted and adopted in order to ensure that the International Civil Aviation Organization (ICAO) Guidelines are followed when it comes to the format of the data and the protocols applicable to the transfer of data from the aviation sector.

Without waiting for the Directive to be adopted, France established a set of national legal measures, authorizing the collection, storage and processing of API-PNR data on air passengers and crew. The system was established by the law of 18 December 2013, which created Article L232-7 of the '*Code de la Sécurité Intérieur*' (internal security code).

Two implementing decrees were adopted in order to get the API-PNR France system up and running: the decree of 26 September 2014, which provides for data processing; and the decree of 22 December 2014, which establishes a PIU. Article L232-7 was then amended, by the law of 28 July 2015, to broaden the scope of data collection to include 'non-carrier economic operators' (travel agencies, tour operators) that charter all or part of an aircraft, and by the law of 20 June 2016, to include shipping lines.

France transposed the Directive into national legislation and ensured that its national provisions on PNR are fully in line with EU legislation: for example, a data protection officer (DPO) was appointed at the PIU; and the amount of time that data can be stored before personal information is masked out was reduced from two years to six months.

The 26 September 2014 decree provides for the collection of data on air passengers and crew on all flights into and out of France, except domestic flights, as of 1 January 2015. The data collection process has been introduced gradually, starting with the four airlines (Air France, Delta Airlines, Ethiad Airways and ASL Airlines France) that helped develop the API-PNR France programme, and later expanding to include other airlines from 1 January 2016.

To begin with, only flights to and from countries outside of the EU were covered, which were around 55 million passengers per year out of a total of 110 million. In 2017, just over 40 airlines were connected to the system, covering around 70% of all non-EU passengers. Nowadays, about 250 airlines operating international flights into or out of France (including intra-EU and French overseas territories) send data on the passengers they are carrying.

The API-PNR system has a number of search, targeting and sorting functionalities designed to:

- obtain information from the passenger database;
- identify persons representing a risk from pre-tested standard profiles;
- compare passenger data collected with data from national, EU or international data bases concerning people who are known or wanted, and stolen or lost documents;
- put one or more people or targets under surveillance for a given period.

With respect to French Customs, the analysis of the data enables it to identify, on a large-scale basis and very rapidly, sensitive or illogical routes, return flights at unduly close intervals in light of the weight of a passenger's luggage, unusual forms of payment, suspect travel agencies, etc., or a combination of these different criteria.

The API-PNR France project entered a test phase in June 2016: the list of operational units designated as 'competent authorities' was established; and a plan was devised for phasing in the new information technology (IT) system within these units. This is currently being rolled-out across all Customs units based at main international airports in France. The system was also becoming increasingly powerful as more and more airlines connected to it.

The main purposes of processing data are for the prevention and detection of acts of terrorism, the offences referred to in Article 695-23 of the Code of Criminal Procedure – participation in a criminal organization, trafficking in human beings, illicit trafficking in arms or drugs, etc. – and acts which violate the fundamental interests of the Nation.

Thanks to the new data collection and analysis system, Customs has brought to light a number of matters linked to attacks on EU financial interests and money laundering, and has also made a number of seizures of cigarettes and tobacco. For the police, positive screening results have led to cases being handed over to the criminal prosecution authorities as well as to the detention of a number of 'flagged' individuals. Intelligence services too reported having identified individuals whose movements were being monitored.

Over and above the results already mentioned, the system has proven its worth to intelligence services in detecting 'weak signals' (the term used in the prevention of terrorism to refer to the faint/limited signals given out by an individual that presents a risk), has been of use in investigations and handling evidence, and simplifies investigative procedures (PNR data can be attached to reports and it is no longer necessary to issue a warrant in order to gain access to airline data).

Given that, by its very nature, such a system involves giving access to huge amounts of personal data, any PNR system must be used on the basis of a principle of proportionality, meaning that any use of personal data must be commensurate with the specific security objectives set out by law in accordance with personal freedom requirements and personal data protection guarantees.

The French Administration presented its guarantees before the national data protection authority, and was met with approval. The French Administration has undertaken to:

- secure data collection;
- limit its collection of PNR data to the 19 authorized categories;
- limit the storage of data to five years, and to mask out data revealing an individual's identity after two years (reduced to six months after the Directive was transposed);
- set up an automatic data filter to remove and destroy any sensitive data;
- give the 'competent authorities' access to the data once it has been checked, and set up a system to track any communication;
- stick to the list of authorized units (and related functions) set down in the December 2014 decree;
- guarantee passengers' rights to information;
- undergo audits and receive visits from the national data protection authority.

Furthermore, once the EU Directive was transposed into national law, a data protection officer (DPO) was appointed at the French PIU. The DPO has access to all the data processed by the PIU, and if the officer feels that this is not being done in line with the law, then he/she is responsible for reporting non-compliance to the national data protection authority. Passengers can also contact the DPO, who acts as a single contact point within the PIU for any data protection issues. The DPO is also informed of any PNR data shared with a third country.

From the very beginning of the project, the choice was made to use the complementarity of API and PNR data (i.e. to marry the API data, which is limited in quality, with the PNR data, which is declarative and not verified, but potentially richer in information), and to respect international standards and examples of best practice.

For data produced by departure control systems (API data), a standard computer message (called the PAXLST) was developed to transmit information related to the identity of passengers, usually during the scanning of the machine readablezone (MRZ) of travel documents. The message, which has been used in the airline industry for many years, is quite short and can be sent easily via the carriers' traditional communication networks.

As for the collection and processing of booking information (PNR data), an internationally standardized message format (called the PNRGOV) allows this data to be sent to governments. Since 2013, France has been participating in the work

to develop the PNRGOV standard, led by the WCO, ICAO and IATA.

While the PNRGOV message structure is now well-established, the standard leaves some room for manoeuvre for those in the aviation sector: the private sector and governments are still in the learning stages. The French API-PNR system, therefore, had to be made more flexible in order to make it possible to accept certain messages.

It should also be noted that PNR data is commercial data which is collected primarily by the industry for the industry. Consequently, only data collected for commercial purposes will be transmitted as stipulated in ICAO document 9944. This explains why the quantity, type and quality of PNR data varies considerably from one airline to the next, and from one passenger to the next.

Yet, ensuring the quality of the data is, of course, essential: the IT data processing system must include all data received in order to (a) filter out any sensitive data, and (b) ensure that risk analysis results are as reliable as possible, thereby enabling unnecessary inspections to be avoided.

This issue was raised by France before the spring 2016 meeting of the PNRGOV Working Group, which brought together government and private sector representatives. The governments represented at the meeting identified the priority issues as being the lack of compliance with industry documentation, and the poor quality of third-party data (from traders, other airlines operating the same flight, etc.). A working group facilitated by the United Kingdom was set up in order to address these issues and come up with medium-term solutions.

France advises States that are looking to set up their own API-PNR programme to take part in the discussions of the PNRGOV Working Group, which are held twice a year in spring and autumn, as well as in those held at the WCO during the API-PNR Contact Committee, which meets in autumn.

Two WCO-supported initiatives that came out of the meeting are worth noting: the creation of Guidelines on how to use API-PNR data; and, more recently, the draft Guidance on how to build API-PNR systems.

Gender issues are not apparent in the legislation relating to the collection and transmission of passenger data to France.

Lithuania

Overview

Carriers engaged in the carriage of passengers by air are subject to the procedures for communicating passenger data

According to:

- Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (API),
- Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime,
- Law on the Fundamentals of Transport Activities of the Republic of Lithuania and other relevant legislation.

Natural or legal persons who are engaged in the carriage of passengers by air to and from the Republic of Lithuania and meet the conditions and requirements for carriers established in the laws of the Republic of Lithuania (hereinafter – air carriers) must communicate passenger data (API and PNR), in line with the one-stop-shop principle, to the authorized Passenger Information Unit of Lithuania - the Force Management Board of the Police Department under the Ministry of the Interior of the Republic of Lithuania. Air carriers are required to communicate this data free of charge by electronic means of communication in a pre-agreed manner and format.

Basic legal acts governing communication of passenger data by air carriers

Law on the Fundamentals of Transport Activities of the Republic of Lithuania

https://www.ltou.lt/uploads/documents/files/corporate/aircraft-services/airport-charges/TVPI%20EN.pdf

The Description of the Procedure for ticket booking and departure control, provision of passenger flight data and air carrier information to Passenger Information Unit approved by the Order No 5-V-1091 of the Lithuanian Police Commissioner General of 23 December 2016 on the Approval of the Description of the Procedure for Ticket Booking and Departure Control, Provision of Passenger Flight Data and Air Carrier Information to Passenger Information Unit

https://www.ltou.lt/uploads/documents/files/corporate/aircraft-services/airport-charges/Description%20EN.pdf

Main requirements on Passenger Data Provision for Air Carriers operating flights to and from Lithuania

https://www.ltou.lt/uploads/documents/files/corporate/aircraft-services/airport-charges/FACTSHEET%20EN.pdf

Hungary

Overview

The subsection 4/I (1) of Act. LXXV. of 1999 on the Rules of Action against Organised Crime and certain Related Phenomena and on the required amendments of the law, allows the Coordination Centre against Organised Crime

(TIBEK) to request access to PNR data, in a particular manner and form, from all international passenger air service operators flying to and from a country outside Schengen area to or from Hungary.

Under subsection 27/C (5) of the Act XCVII of 1995 on Air Traffic, airlines must forward the PNR data to the TIBEK, or a data processing organization assigned by TIBEK after the checking in process occurred, immediately after take-off ("wheels up"). According to the technical solution, repeated push of the data is also needed.

Currently the airline's responsibility escalates only to the forwarding of Advance Passenger Information (API data) according to the Council directive 2004/82/EC on the obligation of carriers to communicate passenger data and according to the section 27/B of Act XCVII of 1995 on Air Traffic. In Hungary, the API data are collected and fixed according to the Passport data, about which the passenger can be identified. The aim of the collection of API data is to combat illegal immigration effectively and to improve border control. In Hungary, the collecting and forwarding of API data occurs according to the section 27/B of Act XCVII of 1995 on Air Traffic.

The "Passenger Information Unit" (PIU) is a service of the Member State administration that brings together the various authorities responsible for the prevention of and fight against terrorism and serious crime. It is the single entry point for interactions with the airlines or data providers. The PIU is responsible for the collection, storage and processing of PNR data transmitted by the aviation stakeholders. The PIU is also responsible for managing the relationship with the airlines and their service providers as well as their monitoring and certification. In Hungary, the TIBEK is responsible for the tasks of the PIU.

Airlines are responsible for the transmission of reservation data (PNR). PNR data are uncontrolled reservation information stemming from passengers and are transmitted by means of an automated process enabling "machine to machine" interface. The information may be transmitted in whole or in part by the carrier or a service provider authorized by the carrier.

Under subsection 27/C (5) of Act 1995 on Air Traffic, airlines must forward the PNR data to the Hungarian PIU, or a data processing organization assigned by TIBEK after the checking in process occurred, immediately after take-off ("wheels up"). Under subsection 27/C (6) of Act 1995 on Air Traffic, airlines must inform the passenger about the transmission of data (to which organization could the data be forwarded), the manager of data, the data-processer, and about the right of data correction immediately.

The airline must forward the PNR data to the Hungarian PIU after the checking in process occurred, immediately after take-off ("wheels up"). The Hungarian PIU requires the specified PNR data elements to be transmitted a total of two times, once 12 hours before the scheduled flight and again after flight closure as shown below:

- 12 hours (Push 1)
- After the checking in process occurred, immediately after take-off ("wheels up") (Push 2)

Airlines must provide a 'push' electronic transfer of passenger information from their Reservations system and from Departure Control System to Hungarian PIU as defined in subsection 27/C (5) of the Act XCVII of 1995 on Air Traffic. PNR data must be provided to the Hungarian PIU for passengers whose itineraries include a flight to, from or through Hungary, to or from a country outside Schengen area by the operating airline.

The Hungarian PIU prefers when airlines transfer PNR data in PNRGOV format according to the International Air Transport Association (IATA) / International Civil Aviation Organisation (ICAO) / World Customs Organisation (WCO) common Guidelines. The preferred PNRGOV message have to be developed under the auspices of the IATA PADIS Board. The message structure and the contents of the message need to provide a consistent approach for all airlines required to provide PNR information to Governments.

The PIU in Hungary manages a data transmission register on passenger data and it is bound to preserve it for ten years. The passenger data can be managed from the date of data transmission till 5 years. After 30 days, the passenger data transmitted to the PIU must be depersonalised. The data could be depersonalised only if the head of the PIU disposes it in the cases of:

- an affair which threatens the national security or the independence of the country, or
- the suspicion of a preparation of a felony punished with imprisonment of five years or more severe punishment.

Under subsection 66/A (1) f) of Act 1995 on Air Traffic the Air Traffic Authority can impose a penalty up to 100 000 000 Ft, if an Airline violates the commitments on data supplying, information or notification stated in the regulations of an act, regulation based on an act, or EU regulation. In regard to the transmission of PNR, data is a statutory commitment (stated in an act), so the subsection 66/A (1) f) of Act 1995 on Air Traffic can be applied in case of the violation of the regulations.

Recommendation

Based on review of a number of countries and their stages of implementing an API/PNR program, it is recommended that Ukraine begins a similar process to EU countries sharing borders with Ukraine and begins focus on the transmission of PNR data. As legislation is developed and negotiations with airlines begin to mature and a PIU/NTC is created, then Ukraine should proceed to a more robust targeting process similar to more distant EU countries and those of Northern America which includes the use of API.

IV. Passenger Information Unit (PIU) / National Targeting Center (NTC)

National Risk Assessment Centre (NRAC) - Canada

Prior to 2012, the Canada Border Services Agency (CBSA) approached targeting in a multi tiered approach. The National Risk Assessment Centre (NRAC) located in Ottawa had a primary focus on national security, while regional operations focused on contraband and illicit migration targeting. The National Targeting Centre (NTC) was created in April 2012 operating 24 hours a day, 7 days a week with a goal of establishing a centralized, fully integrated, nationally consistent program that is an integral part of the CBSA's border risk management. The NTC identifies suspected high-risk people, goods and conveyances through an integrated, comprehensive targeting program that effectively uses intelligence products and technology to support the CBSA's mandate. Other major partner countries have, or are in the process of, centralizing targeting functions and Canada is viewed as a model to follow.

The NTC utilizes CBSA and partner information to conduct integrated risk assessments. The targeting centre is continually enhancing targeting systems to provide NTC Targeting Officers with high-quality pre-arrival data and risk identification capacity. As well, the NTC continues to increase collaboration with international partners by harmonizing targeting methodologies, information exchange, and coordination in areas of common threats. Operationally, the NTC's collective capacity to track, trace, and monitor threats will be continually enhanced.

The NTC is comprised of 245 staff performing targeting support and functions, 6 units including passenger and commercial targeting units as well as supporting passenger and commercial intelligence units. Specifically, the passenger targeting unit is responsible for the following activities:

- Risk Assessment and targeting is undertaken of high risk travellers in the air passenger mode for national security, contraband, immigration and health & safety concerns by utilising the API/PNR data provided by airlines at wheels up. Data elements include – name, DOB, Gender; PNR data includes travel agency the passenger booked with, billing address; contact phone numbers. Both sets of data go hand in hand in our ability to risk assess.
- All selected travellers are run through the various enforcement databases and systems as part of the risk assessment process.
- Passengers selected for a comprehensive review are run through additional systems such as:
    - In-depth open source – Facebook, Twitter, etc.
    - Any other relevant enforcement databases
    - Partner Request for Information (Canada Revenue Agency, Immigration, Refugees and Citizenship Canada - Passport Program, United States – National Targeting Centre, Canadian Security Intelligence Service, Royal Canadian Mounted Police)

There are two different types of targeting methods:

- Scenario Based Targeting (SBT) is an enhanced technological tool designed to support the targeting program by pre-screening all Canada bound travellers through pre-established scenarios. Scenarios are intelligence based products which are primarily built on API/PNR data elements that are reflective of an identified or anticipated trend or pattern of risk associated with national security, public safety, and other border risks/threats.
- Flight list targeting (FLT) incorporates the same ideology of SBT where targeting officers are using API/PNR elements to risk assess passengers but in contrast to the SBT model, they are responsible for sorting and assessing the different data elements while looking at a complete flight manifest. The targeting officer will apply their experience and knowledge to sort and assess a flight manifest in accordance to the perceived risk (illicit migration, contraband or national security). The primary focus of FLT is to identify new trends and patterns not already captured by SBT.

The risk assessment process involves a review of the travellers API/ PNR, database checks, requests for information with partner agencies and an open-source analysis while also taking into account current intelligence trends.

An RFI is requested during the comprehensive review of a passenger, meaning an initial analysis of their API/PNR and database checks have been performed and the risk could not be negated. The NTC has established a number of partnerships which contribute to the ability to obtain information in support of the risk assessment process. Partnerships include the following:

On-site:

- Canadian Security Intelligence Service (CSIS)
- Canada Revenue Agency (CRA)
- United States Custom and Border Protection (US CBP)

Off-site:

- Passport Canada
- Royal Canadian Mounted Police (RCMP)
- CBSA Liaison Officer on site at US NTC-P
- Canadian Food Inspection Agency (CFIA)
- Communications Security Establishment (CSE)
- Health Canada
- Transport Canada
- Department of Foreign Affairs and International Trade
- Australian Customs and Border Protection Services
- United Kingdom Border Force

The CBSA regularly compares targeting information with International partners including; the United States, United Kingdom, Australia and New Zealand.

The NTC participates in joint B5/Heads of Intelligence (HIINT/Targeting Working Group (TWG) projects in coordination with partner international agencies and conducts analysis of best practices and targeting methodologies of international partners.

As a results of targeting efforts, the NTC continuously learn from their targets and their results: Border Services Officers provide exam results which allows for the closing of the loop whereby results are analyzed to assist Targeting Officers in the creation of future targets.

With the implementation of the Interactive Advanced Passenger Information (iAPI) initiative, the passenger targeting unit communicates with commercial air carriers to prevent prescribed persons subject to an enforced removal order or a Negative Discretion Authority (NDA) from boarding a commercial aircraft bound for Canada.

On an average day, Targeting Officers within the passenger targeting unit will:

- Perform 620 passenger risk assessments
- Issue 41 Targets- (2.5 National Security/21 Contraband/17.5 Illicit Migration)
- Issue 132 Requests for Information (RFIs) with partner agencies

The passenger intelligence unit which support the passenger targeting unit provided the following support activities:

- Supports national targeting operations by providing actionable products developed from regional, national and international intelligence information
- Analyzes intelligence-generated targeting, and resultant examinations, to identify unknown threat and risk trends, patterns and indicators
- Produces and disseminates actionable intelligence- Bulletins, Scenarios and Trends analysis, Alerts, Projects, Shift briefings
- Conducts information gathering and trend analysis; Identification of suspected high risk people or shipments
- Review of post-seizure/enforcement action

In implementing API and PNR, Canada practices around passenger data are aligned with the UN Security Council Resolutions. The API/PNR program enables the CBSA to conduct a risk assessment for customs and immigration purposes to identify high risk travellers prior to their arrival in Canada. The legislative authority for the program is provided under the *Customs Act* and the *Immigration and Refugee Protection Act* (*IRPA*). In addition, to satisfy the requirements imposed by the European Union (EU), the CBSA made a series of commitments in terms of data use, retention, access and disclosure in conjunction with *the Agreement between the Government of Canada and the European Community*. Canada was also required to enact these commitments into the *Protection of Passenger Information Regulations* pursuant to *IRPA*.

Although the CBSA has legislative authority under *IRPA* to use API for issues such as illegal migration, inadmissible persons or subjects of warrants, the current CBSA commitments made to the EU, the *Protection of Passenger Information Regulations* and related CBSA policies (Memorandum D1-16-3 and Enforcement Manual Part 3 Chapter 5) limit the use of API/PNR information to the identification of persons who are at risk to import goods related to, or those who are inadmissible to Canada, because of their potential relationship to terrorism or terrorism-related crimes or other serious crimes, including organized crime, that are transnational in nature.

The CBSA operates within the "Guidelines on API" put forward by World Customs Organization (WCO)/ International Civil Aviation Organization (ICAO)/International Air Transport Association (IATA).

API is defined in the *Immigration and Refugee Protection Regulations (IRPR)* and the *Passenger Information (Customs) Regulations (PICR)* as the following information, to be transmitted before arrival in Canada:

- their surname, first name and initial or initials of any middle names;

- their date of birth;
- the country that issued them a passport or travel document or, if they do not have a passport or travel document, their citizenship or nationality;
- their gender;
- their passport number or, if they do not have a passport, the number on the travel document that identifies them; and
- their reservation record locator or file number.

The CBSA collects up to 25 PNR data elements under the API/PNR program. For the purposes of the data submission, current regulations outline what information is considered to be PNR information, if received in a PNR or DCS message. They include:

- PNR locator code
- Date of reservation
- Dates of intended travel
- Passenger Name
- Other names on PNR
- All forms of payment information
- Billing Address
- Contact telephone numbers
- All travel itinerary information for specific PNR
- Frequent flyer information
- Travel agency information
- Travel agent
- Split/divided PNR information
- Ticketing information
- Ticket number
- Seat number
- Date of ticket issuance
- No show information
- Go show information
- Bag tag numbers (baggage information)
- Seat information
- One-way tickets
- Any collected API information
- Standby
- Check-in information

This list is often misinterpreted to mean that countries are limited to receive 25 independent data elements only. In actuality, most of the 25 items listed above are overarching data titles for which countries receive multiple pieces of information. Countries are able to receive and process, if the commercial air carrier collects and uses that information, upwards of 400 distinct pieces of data that make up DCS and PNR messages. For example, the item listed above called "baggage information", can be made up of the following pieces of information, which countries can and does receive if it is captured and sent by the commercial air carrier or 3rd party service provider:

- Total number of pieces of checked baggage
- Total number of pieces of carry-on baggage
- Weight of checked baggage
- Kilograms or pounds
- Pooled baggage indicator
- Pooled baggage identifier
- Company identification
- Tag numbers
- Number of consecutive tags
- Place of destination
- Airline code number
- Bag tag characteristic

All commercial air carriers must transmit the API of every person (including passengers and crew) on board an aircraft destined to Canada; however, PNR is available for passengers only. The CBSA does not require carriers to provide any PNR information that they do not collect for their own purposes.

A dedicated CBSA client service team works with air carriers during implementation and to ensure continued compliance. The CBSA client service team works with all airlines that provide API/PNR and follow-up with air carriers when there are issues with not receiving data. They meet with carriers to explain Canada's legislative requirements and the carrier's responsibility to submit API/PNR. Carriers need to ensure that their systems are functioning properly for the processing of API and PNR data and that appropriate standard operating procedures are put in place.

The CBSA, in cooperation with the Airline Industry, has formed the Advance Passenger Information/Passenger Name Record (API/PNR) Coordination and Compliance Working Group (CCWG). This working group provides a forum to allow for the exchange of information between stakeholders and promotes the discussion of issues relating to current and proposed changes to policies and administrative procedures involving the API/PNR Compliance framework. The CCWG is represented by the following associations: Airlines for America; National Airlines Council of Canada (NACC); Regional Airline Association; International Air Transport Association (IATA); Air Transport Association of Canada (ATAC).

In order to transmit API/PNR data to the CBSA, operating commercial air carriers can opt to send the data themselves, employ a service provider(s) or a combination of the two, select a message format and a transmission method.

There are 3 available transmission options:

- Message Queue (MQ) Network- Direct Connect (API and PNR).
- Internet API Gateway (IAG), which includes API and/or PNR file upload and API interactive data entry (IDE).
- E-mail (API only).

API must be transmitted in a prescribed format (passenger manifest) in accordance with CBSA technical requirements. A penalty regime exists for failure to provide API/PNR ($3000 CAD per flight).

The CBSA requires both data sets (API/PNR) in order to properly risk assess high risk travellers. While both are important, PNR is critical to the risk assessment process.

PAXIS is the primary application utilized by CBSA performing pre-departure board/no-board processing (automated and manual board/no-board decisions), pre-arrival intelligence and targeting activities for travellers in the air mode. PAXIS also performs the pre-departure vetting against known risk for all traveller departing Canada in the air mode. While discussions have occurred regarding the expansion of PAXIS for other modes of transport, including Cruise Ships and Rail, no decisions have been made. Advance Passenger Information and Passenger Name Record information (API/PNR) is provided to the CBSA by commercial air carriers and/or 3rd party service providers which is then used by PAXIS and its authorized users as part of these activities. SEE SECTION B4 for more details on the transmission of data to the CBSA.

PAXIS processes and displays API/PNR information it receives for crew and passengers inbound to Canada as well as API data information it receives for crew and passengers outbound from Canada. Various workflows within PAXIS allow for viewing and manipulating these sets of data by users working within the National Targeting Centre (NTC).

In 2014/2015, the PAXIS system was redesigned which included the centralization of targeting to a National Targeting Centre located in Ottawa, Ontario. Between 2015 and 2018, PAXIS was further updated to support the Interactive Advance Passenger Information (iAPI) Initiative to allowing the CBSA to receive advance information earlier in the travel continuum and respond back to commercial air carriers with board or no-board messages. In 2019, PAXIS was updated to include vetting activities against known risk for all outbound travellers in the air mode. The CBSA started collecting and vetting outbound travellers in the air mode as of Summer 2020, with Air Exit regulations are in place. For all outbound vetting activities only API data will be used. PNR data is not collected or used for Air Exit.

In summer 2015, the second main phase of the implementation of the SBT methodology was implemented. The release saw SBT introduced as the primary workflow for targeting officers. It was crucial that PAXIS processing speed was sufficient to allow SBT threat identification and Targeting Officer risk assessment.

The NTC has implemented a robust scenario development, maintenance, monitoring and governance framework. The cyclical process includes:

- scenario identification, analysis, evaluation and creation
- scenario review and finalization
- scenario activation
- scenario performance monitoring and reporting
- scenario management committee discussions and
- scenario evaluation and determination of status (modification, deactivation etc).

As new threats emerge and the NTC's internal and external engagement with partner agencies continue to progress, the development and activation of scenarios will be ongoing.

Items to consider for a passenger targeting centre:

People

- Commitment to dedicated passenger targeting resources. Passenger targeting unit will require dedicated staff working 24/7, Sunday to Saturday to ensure full coverage. Staffing will include a formal shift schedule.
- Once committed to staffing resources the passenger targeting unit will have to be committed to training the resources based on a structured training plan.
- The passenger targeting unit will need to commit to a staffing action plan to determine their staffing levels and the recruitment process.

- Once a staffing action plan is determined, there will be a need for Performance Management expectations.
- The passenger targeting unit will need a clear sense of roles and responsibilities between Targeting Officers, Targeting Experts and Targeting Supervisors, etc.

Technology

- Once a system is designed and implemented, a continual review of Risk Rules/scenarios will ensure most accurate indicators, which impact Ukraine and surrounding countries. Need constant communication with partner agencies to determine the highest risk and modify the risk rules to address those risks.
- Requirement to work with our stakeholders and obtain importation history from a Border standpoint to support the risk assessment process. Minimum of 2 years history however 6 years would be ideal. The data should be ingested into the passenger targeting system and should be available automatically for Targeting Officer review.
- Requirement to gain access to partner agency information. As there are a multitude of law enforcement agencies within Ukraine and neighboring country, contact with these agencies and obtaining their enforcement information is essential to the risk assessment process. Separate Customs and Police makes it difficult however consultations must take place to promote interoperability opportunities. Ideally the information would be ingested within passenger targeting system, however if this is not available, automated requests for information must be made available.

Collaboration

- As per the technology enhancements identified above, MOU's must be put into place with stakeholders and partner agencies to obtain relevant information. The MOU's must also outline how the passenger targeting unit and partner agencies can work together for the whole of Ukraine. The sharing of information is not a one-way delivery of information, rather it will be a two-way process where passenger targeting unit shares information equally with partner agencies.
- Outreach should be performed with partner agencies outlining the passenger targeting unit's capacities and how agencies can work together to address high risk passengers entering into Ukraine.

Processes

- Standard Operating Procedures must be drafted and agreed upon moving forward. Once the final products have been finalized, then they must be adopted in support of the risk assessment process.
- Standard reporting process to be implemented to ensure management is aware of the day-to-day activities.

Passenger Information Unit (PIU) - France

Decree No.2014-1095 of September 26, 2014 (modified by decree No. 2018-714 of August 03, 2018) created the API-PNR France device, requires airlines to transmit reservation data (PNR) and registration (API) of their passengers and crews for trips to and from the national territory, with the exception of trips connecting two points in mainland France.

This same text authorizes the automated processing of this data for the purposes of meeting the needs of government services, for the prevention and detection of acts of terrorism, serious offenses and crimes and attacks on the fundamental interests of the Nation.

Decree number 2014-1566 of 22 December 2014 (amended by decree number 2018-722 of 03 August 2018) creates the Passenger Information Unit (PIU), an interministerial service with national competence, which provides the interface between the data relating to air passengers and operational services.

The French PIU is based near Roissy Charles de Gaulle airport, and is made up of staff from four partner administrations (Interior, Defence, Transport and Customs). It is open from 07.00 until 19.30, from Monday to Friday. The PIU is staffed by more than 70 people, ensuring a 24/7 service.

Access to personal data contained in the system is therefore not direct for end users, but indirect: the requests submitted and their results are validated or refused by the PIU, which contributes, in this sense, to the protection of personal data.

A training plan for staff from the PIU and 'competent authorities' has been put in place, and over 100 people have already received training. The training strategy focuses on training trainers so as to increase each unit's training capacities. The PIU has equally been supporting users throughout the current test phase.

The main purposes of processing data are for the prevention and detection of acts of terrorism, the offences referred to in Article 695-23 of the Code of Criminal Procedure – participation in a criminal organization, trafficking in human beings, illicit trafficking in arms or drugs, etc. – and acts which violate the fundamental interests of the Nation.

Over and above the results already mentioned, the system has proven its worth to intelligence services in detecting 'weak signals' (the term used in the prevention of terrorism to refer to the faint/limited signals given out by an individual that presents a risk), has been of use in investigations and handling evidence, and simplifies investigative procedures (PNR data can be attached to reports and it is no longer necessary to issue a warrant in order to gain access to airline data).

Given that, by its very nature, such a system involves giving access to huge amounts of personal data, any PNR system must be used on the basis of a principle of proportionality, meaning that any use of personal data must be commensurate with the specific security objectives set out by law in accordance with personal freedom requirements and personal data protection guarantees.

The French Administration presented its guarantees before the national data protection authority, and was met with approval. The French Administration has undertaken to:

- secure data collection;
- limit its collection of PNR data to the 19 authorized categories;
- limit the storage of data to five years, and to mask out data revealing an individual's identity after two years (reduced to six months after the Directive was transposed);
- set up an automatic data filter to remove and destroy any sensitive data;
- give the 'competent authorities' access to the data once it has been checked, and set up a system to track any communication;
- stick to the list of authorized units (and related functions) set down in the December 2014 decree;
- guarantee passengers' rights to information;
- undergo audits and receive visits from the national data protection authority.

From the very beginning, the choice was made to use the complementarity of API and PNR data (i.e. to marry the API data, which is limited in quality, with the PNR data, which is declarative and not verified, but potentially richer in information), and to respect international standards and examples of best practice.

For data produced by departure control systems (API data), a standard computer message (called the PAXLST) was developed to transmit information related to the identity of passengers, usually during the scanning of the machine readablezone (MRZ) of travel documents. The message, which has been used in the airline industry for many years, is quite short and can be sent easily via the carriers' traditional communication networks.

As for the collection and processing of booking information (PNR data), an internationally standardized message format (called the PNRGOV) allows this data to be sent to governments. Since 2013, France has been participating in the work to develop the PNRGOV standard, led by the WCO, ICAO and IATA.

While the PNRGOV message structure is now well-established, the standard leaves some room for manoeuvre for those in the aviation sector: the private sector and governments are still in the learning stages. The French API-PNR system, therefore, had to be made more flexible in order to make it possible to accept certain messages.

It should also be noted that PNR data is commercial data which is collected primarily by the industry for the industry. Consequently, only data collected for commercial purposes will be transmitted as stipulated in ICAO document 9944. This explains why the quantity, type and quality of PNR data varies considerably from one airline to the next, and from one passenger to the next.

Yet, ensuring the quality of the data is, of course, essential: the IT data processing system must include all data received in order to (a) filter out any sensitive data, and (b) ensure that risk analysis results are as reliable as possible, thereby enabling unnecessary inspections to be avoided.

European Union (EU) Directive 2016/681 on the use of Passenger Name Record (PNR) data was adopted on 27 April 2016. It requires EU Member States to collect and use both PNR data and Advanced Passenger Information (API) "for the prevention, detection, investigation and prosecution of terrorist offences and serious crime." The Member States had two years to transpose the Directive into their national law, by which time it was to be ready for implementation.

The Directive stipulates that a Passenger Information Unit (PIU) responsible for collecting, storing and processing data should be set up in each Member State. According to the text, any hits or positive results must be sent by the PIU to the operational units referred to as "competent authorities." In addition, the Directive also covers data exchange between PIUs and with Europol, as well as with third countries on a case by case basis.

France transposed the Directive into national legislation in 2017 in order to ensure that its national provisions on PNR were fully in line with EU legislation: for example, a data protection officer (DPO) was appointed at the PIU; and the amount of time that data can be stored before personal information is masked out was be reduced from two years to six months.

V. Concept Roadmap for API/PNR

Specific Outcome	Activity	Sub-Activity and Requirement
I. Legislation	1. Develop and adopt national legislation for Advanced Passenger Information (API)	• Conduct a legislative assessment in API • Develop a draft legislation or amendments to the current legislation in API • Adopt a draft legislation or amendments to the current legislation in API
	2. Develop and adopt national legislation for Passenger Name Record (PNR)	• Conduct a legislative assessment in PNR • Develop a draft legislation or amendments to the current legislation in PNR • Adopt a draft legislation or amendments to the current legislation in PNR
	3. Ensure compliance of the developed national legislation in API/PNR with international regulations and directives	• Ensure all pieces of legislation adhere to UNSC Resolutions 2178, 2309, 2396, 2482, the EU API and PNR Directives, OSCE Ministerial Council Decision 6/16, ICAO Guidelines for API/PNR, WCO Guidelines for API/PNR and the IATA API-PNR Toolkit
	4. Appoint a competent authority that will implement and oversee the implementation of API/PNR *(EU PNR Directive)*	• Identify the competent authority for implementation and overseeing of the implementation of API/PNR
	5. Develop a full implementation programme including a project plan, technical guide for the airlines, notification plan for the airlines. The plan will depend on the final design on the solution and the number and type of service providers and donors involved.	• Develop the implementation program including a project plan, technical guide for the airlines, notification plan for the airlines
II. API/PNR data	6. Identify competent authority that will use the data *(EU API Directive)*	• Identify the competent authority that will ingest the data • Identify other agencies who will use the data and how it will be shared
	7. Mandate collection and use of API *(EU API Directive, UNSC Resolutions 2178, 2309, ICAO Annex 9)*	• Identify the specific legislation in which the collection and use of API will be collected Examples include the following: • Customs • Immigration • Privacy • Access to Information
	8. Define purpose for requesting API *(EU API Directive, UNSC Resolutions 2178, 2309)*	• Utilize API to perform a risk assessment of travellers prior to their arrival in a country and to identify those who require further examination upon arrival
	9. Define how and when data is transmitted *(EU API Directive, IATI API Toolkit)*	• Ensure that transmission of API of every person (including passengers and crew) on board an aircraft destined to a country is provided from all carriers • Ensure API is collected upon booking/reservation and confirmed upon check-in/boarding. API is comprised of seven biographical data elements (tombstone data) and is to be legislated by law for the airlines to provide to a country at "wheels up". Although API is comprised of seven biographical data elements, many countries use more (many 16). The competent authority should indicate the data elements they require considering the Directive and IATA/ICAO Guidelines. PNR should be sent by the airline to the PIU: a) 24 to 48 hours before the scheduled flight departure time; and b) Immediately after the flight is closed for boarding, meaning it is not possible for passengers to board or leave the aircraft before departure

	10. Define penalties for late, missing or incorrect data *(EU API Directive)*	• Draft regulations that include "Failing to provide, or provide access to, prescribed information about any person on board a conveyance in advance of, or within a reasonable time after, the arrival of the conveyance in a country" is an offence.
		• Ensure these penalties are stated in national legislation and that "penalties provided for shall be effective, proportionate and dissuasive":
		  • The minimum fine is to be more than €3,000
		  • The maximum fine is to be more than €5,000
		  • Higher sanctions can be made on airlines with serious infringements, including withdrawing the operating licence or confiscating or immobilising aircraft
		  • Airlines have a right of appeal to these sanctions

	11. Create a means whereby airlines can send PNR to the PIU using a "Push" method and common standards and protocols *(EU PNR Directive)*	• Create a means through the Departure Control System (DCS), which is an automated computer system used by commercial air carriers for departing flights. Up to 24 hours before departure, the Global Distribution System and Airline Reservation System will transfer passenger data to the DCS and will continue to send updates as they occur, until the time of departure. A country will only be concerned with the check-in and boarding control information, as they provide the API. When a passenger checks in, the DCS records are updated with seat, baggage and document information.
	12. Determine which PNR data elements are to be included within the transmission (19 elements are listed within the Directive) *(EU PNR Directive)*	• Identify which of the 19 PNR data elements are required (as defined in the EU Directive) for the use intended within the PIU. Sensitive data is not to be collected. Sensitive data is defined as "information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or information about a person's health or sex life." This data is rarely present in PNR, but may be included in special food or service requests (e.g. kosher meal, insulin pump, oxygen tank). Requested passenger data should be limited and uniform. 19 data fields mentioned in the EU PNR Directive Data elements received that are outside the prescribed 19 elements listed in the EU Directive are to be deleted on receipt and not processed further Passenger data to be in accordance with human rights and data protection laws • Ensure respect of the obligations under international law, in particular international humanitarian law and international refugee law • Review international legislation and international good practices.
	13. Collect PNR for arriving and departing international flights *(EU PNR Directive)*	• Determine a PIU processes and displays API/ PNR information and data it receives for crew and passengers inbound to and outbound from a country
	14. Specify data retention- maintain PNR for 5 years *(EU PNR Directive)*	• Include the following requirements in the legislation: All PNR data collected is readily available for the first 6 months then depersonalised and only re-populated by order of a judge (or similar) then permanently deleted at 5 years unless actively used. 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 competent authority to identify persons in relation to a terrorism offence or serious transnational crime

	15. Specify PNR data depersonalized 6 months after receipt *(EU PNR Directive)*	• Include the following requirements in the legislation: All PNR data collected is readily available for the first 6 months then depersonalised and only re-populated by order of a judge (or similar) then permanently deleted at 5 years unless actively used. 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 competent authority to identify persons in relation to a terrorism offence or serious transnational crime
	16. Ensure PNR data only to be used to detect or prevent the actions of those involved in terrorism or very serious crimes *(EU PNR Directive)*	• Introduce the concept of a PNR database. The concept would be to expand the storage and use of API and PNR in a "data warehouse" outside of the API/PNR system. • Include a unit responsible for the data warehouse, i.e. Data Analytics. Use of PNR to perform intelligence analysis on historical PNR which is crucial information for intelligence and investigative analysis. If an enforcement action occurs on an individual (or an individual is under investigation for transnational organised crime or terrorism) historical. API/PNR is valuable information as it pertains to identifying trends or patterns. PNR may only be used to detect or prevent the actions of those involved in terrorism or very serious crimes. The 26 very serious crimes relating to the PNR Directive are listed in Appendix 2.
	17. Specify disclosure of Information *(EU PNR Directive)*	• Specify that disclosure is handled on a case-by-case basis and is linked with a significant enforcement action, transnational organised crime groups, and terrorism provided the disclosure meet the regulatory and legislative requirements.

III. Passenger Information Unit	18. Establish a Passenger Information Unit (PIU) as a single window	• Define competent authorities that will be represented at the PIU.
		• Develop an operating concept based on international experiences.
		• Ensure that the development of a Passenger Information Unit model includes the following:
		  • Development, maintenance and communication of the targeting mandate, strategies, and overall targeting process
		  • Development and maintenance of targeting policies
		  • Development and maintenance of the Targeting Community which includes the HR strategy for recruitment and retention of Targeting Officers
		  • Development and maintenance of training of the PIU's staff
		Single window will receive the API/PNR which will then be shared with each interested organisation to perform their own analysis. Owner is to be decided. As part of the single window development, Ensure the passenger data is checked against databases of INTERPOL and Europol. More databases will be defined as user requirements are defined.
		• Create a webpage within the competent authority's main website referencing the PIU.

	19. Allow for the ability to target for multiple categories of risk	• Design and develop an own targeting system or use the one already developed by another country to include data collection, risk rules (scenarios), partner interface and analysis tools. • Ensure access to national, regional and international databases and watch lists.

	20. Appoint a Data Protection Officer *(EU PNR Directive)*	• Include a position of a data protection officer and ensure its independence at a PIU. • Provide a national supervisory authority that will ensure protection of passenger data. National supervisory authority, which is able to ensure fundamental rights are protected in relation to the processing of personal data as well as dealing with complaints and verifies the lawfulness of the ongoing data processing
IV. Strategic Collaboration	21. Develop a Stakeholder Engagement Strategy	• Develop a Stakeholder Management Plan to include airlines, airports, service providers and other impacted partners

	22. Develop (and implement) MOU's with strategic partners on security-related manners	• Ensure all relevant domestic departments, agencies and other entities work closely and effectively together on matters of aviation security.
		Include the following:
		  • Define the competent authorities that are involved in establishing API/PNR.
		  • Define the competent authorities that will use the passenger data.
		  • Define the competent authorities that will be represented at the PIU/NTC, if the case.
		  • Launch and maintain regular cooperation with all the parties involved in this field.
		• Sign intra-agency agreements/memorandums with competent state authorities.
		• Ensure PIU cooperates and exchanges information with PIU/NTC's of other countries.
		• Strengthen international and regional cooperation to facilitate information-sharing, border control, law enforcement and criminal justice to better counter the threat posed by foreign terrorist fighters and returnees

	23. Cooperation with the airline industry	• Ensure commercial airlines carry out all registration, testing and certification procedures before operating flights to a country. Transmission can be done by direct connection or service provider or both. • Define contact points at air carriers. • Define the form (data fields) and format of requested passenger data to be transmitted to a PIU. All API/PNR data must be transmitted to the PIU in an electronic format. To ensure sustained compliance, all air carriers will be requested to establish a secondary transmission method in the event their primary transmission method is unavailable. • Include a client service team and/or airline account manager/liaison manager to work with the air carriers (similar to international practices)

The Concept Roadmap for API/PNR, which is based on international and European legislation, experience and best practices, is aimed to provide guidance that outlines the minimum list of activities and requirements to be addressed in order to establish an API/PNR system and a PIU in a country that plans to join the EU or is bordering the EU and has many flights to and from the EU countries. The document is not all-inclusive as there will be other additional activities and sub-activities required to be addressed in order to establish an API/PNR system in a particular country. Therefore, it is recommended to draft a national tailor-made roadmap for establishing an API/PNR system in a particular country that will take into consideration national characteristics and already developed elements of the system in that country. This Concept Roadmap is and will always be a living document that develops over the course of maturity based on the international legislation and international experience.