Polizia di Stato

Frequently Asked Questions (FAQ)

Frequently Asked Questions on the System for the Processing of PNR data

1.What are PNR data (Passenger Name Record)

PNR data means a record of each passenger's travel requirements which contains information relating to the booking of a flight by one or more passengers; such information, provided by passengers themselves, is collected and retained by air carriers and/or by travel operators. Several carriers / operators in the sector may request either a minimum amount of information from passengers (for example name, travel itinerary booked, travel operator where transport was reserved, etc.) or additional information (for example, e-mail address, phone number, etc.). Annex 1 of EU Directive 2016/681 details the set of possible information included in PNR data.

Directive 2016/681, implemented in the national law by Legislative Decree no. 53 of 21 May 2018, provides that national authorities collect and process PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes (for a definition of serious crime, please refer to Annex II to Directive 2016/681).

In the context of processing PNR data, the Italian authorities cannot collect or process sensitive information such as that concerning passengers' state of health, racial or ethnic origin, political, religious and philosophical opinions, trade union membership or sexual orientation.

2.What are API data (Advanced Passenger Information) –

API data consist of all information gathered during check-in or embarkation by air carriers or other transport companies; these data are normally collected in order to properly identify passengers and are taken from valid and authentic documents. API data include:

- Serial number and type of travel document used;
- Nationality;
- Full name;
- Date of birth;
- Border crossing point of entry into the territory of Member States;
- number of transport;
- departure and arrival time of the means of transport;
- total number of passengers carried on that means of transport;
- the initial point of embarkation.

API data are processed, in compliance with the principles of necessity and proportionality, by the offices in charge of border police controls for the purpose of improving border checks and combating illegal immigration.

3.Why does Italy collect and process passengers' PNR data?

Like every EU Member State Italy is required to establish a Passenger Information Unit (PIU) tasked with collecting and analyzing PNR data as well sharing them, including the results of analysis with other Member States or with Third Countries. Data processed concern all passengers travelling from, to and in transit through Italy. This measure applies to the fight against terrorism and serious and organized crime, based on the European Directive on the use of Passenger Name Record data (EU Directive 2016/681)

Persons suspected of terrorism or other serious crimes often have specific travel behaviors and

characteristics. The analysis of PNR data plays an important role in identifying those characteristics in order to direct crime prevention and repression activities, to collect evidence and dismantle criminal networks. PNR data are analyzed, in compliance with the rules protecting the privacy of citizens and the personal data concerning them, using pre-defined and regularly updated criteria, also through a comparison with other national police databases. The effective use of these data provides a considerable added value for internal security.

Under no circumstances may PNR and API data be processed for any purpose other than those provided for by law.

4.For what purposes can authorities use PNR and API data?

The collection of PNR data is aimed at preventing and suppressing terrorist offences and serious crimes (for a definition of “serious crime”, please refer to Annex II to EU Directive 2016/681). API data are processed to improve border controls and prevent illegal immigration.

5.What is the Passenger Information Unit (PIU)?

The PIU is the competent Office, as provided for by Law, in charge of receiving, processing and sharing PNR data with the competent national authorities, Member States, third countries and Europol. The PIU is an inter-force Unit – *i.e.* it is staffed with representatives from the four police forces, pursuant to Article 16 of Law 121 on 1 April 1981 – and it is set up within the Central Criminal Police Directorate of Public Security of the Ministry of the Interior.

6.What is the legal basis for the processing of PNR data?

PNR data processing is governed by Legislative Decree no. 53 of 21 May 2018, implementing EU Directive 2016/681 in national legislation. The legislation applies to air transport both for extra-EU routes (flights departing from Italy and bound for a third country - e.g. the United States, China, etc… - or flights departing from a third country and planned to land in Italy) – and intra-EU routes (flights departing from Italy and bound for a EU Member State – e.g. France, Germany, etc … – or flying from a EU Member State and planned to land in Italy). The legislation applies to both scheduled and non-scheduled flights.

7.When are PNR and API data collected?

Air carriers are required by law to transfer PNR data to the PIU Information System:

a) over a period between 24 and 48 hours before the scheduled flight departure time;

b) immediately after flight closure, when it is no longer possible for passengers to board or leave.

Where there is a specific and actual threat related to terrorist offences or serious crime, the PIU may request air carriers to share PNR data at a point in time even before than those mentioned in letters a) and b).

API data are made available immediately after the flight closure, when it is no longer possible for a passenger to board or leave the aircraft.

8.What are the safeguards protecting the privacy of passengers?

PNR data are processed in compliance with the national and European legislation on the protection of personal data (Directive EU 680/2016, Legislative Decree 196/2003, Legislative Decree 51/2018). Furthermore, the legislation on PNR data processing contains specific measures and procedures to protect the privacy of citizens, including:

a) PNR data cannot be directly consulted by the national police forces: accessing and consulting these data is only possible through the national Passenger Information Unit (PIU) which is the inter-force office also responsible for sharing PNR data with national authorities in the event of a reasoned necessity where it is reasonably believed that it is necessary. In addition, access to data by the PIU personnel is limited on the basis of various authorization profiles in compliance with the principles of proportionality and necessity;

b) The criteria against which PNR data are analyzed are periodically evaluated and updated;

c) Any positive match resulting from the automated processing is individually reviewed in a non-automated manner, to better protect data subjects.

d) Upon expiry of a period of six months after their receipt, PNR data shall be pseudonymized (namely, they are subject to an anonymization process which is reversible, provided additional information is known which is retained separately from PNR data). Following this process, the full data can still be accessed and shared but only where there is a justified need and subject to prior authorization by the Judicial Authority or the Deputy Chief of Police – Director General of Criminal Police; in such cases the Data Protection Officer is notified in order to carry out the relevant checks.

e) 5 years after their receipt, PNR data are permanently deleted, except for those transferred to the competent national authorities and used in a specific case of prevention and suppression of terrorist offences or serious crimes;

f) API data, due to the purpose of their processing, are made available only to the offices in charge of border police controls. Within 24 hours of their transfer, or after the entry of passengers in the Italian territory, the API data that are not necessary in terms of preventing irregular immigration, are rendered invisible to the offices themselves; *vice versa*, the API data used for the prevention of irregular immigration are made invisible to the offices in charge of border police controls after 6 months from their receipt and deleted 5 years after receipt;

g) PNR data are shared with foreign authorities (except in cases of justified emergency, this happens through the PIUs of Member States) only in the event of a positive match or a reasoned request;

h) PNR data may be shared with third countries only upon a duly reasoned request, and provided that the requesting third country fulfills any obligations regarding data processing purposes and commits to process data with all safeguards in compliance with the Italian and European applicable regulations.

i) At the Central Directorate of Criminal Police, a Data Protection Officer (DPO) has been appointed responsible for monitoring the processing of PNR data and ensuring the implementation of all necessary technical security measures.

9.Rights of access for passengers

Citizens whose PNR/API data are being processed pursuant to Legislative Decree No.53 of 21 May 2018 enjoy special rights of access to their retained information. In particular:

a) The right to obtain confirmation as to whether or not their own personal data are retained, the communication of such data in an intelligibile form and the right to request the erasure of any data which is unlawfully processed or their transformation into anonymous form;

b) The right for anyone who becomes aware of the existence of his/her own personal data, processed in a non-automated way in violation of the provisions of law or regulations, to request the competent court in the place of residence of the data controller to carry out the necessary checks and order the rectification, integration, erasure or transformation of the data into anonymous form.

To exercise these rights, you can send the appropriate form. For more details on the rights of data

subjects, on how to exercise these rights, as well as on the response procedures, please refer to the dedicated information web page.

10.What should I do as a passenger?

To avoid problems at the airport, you should carefully check that the information provided during the booking process is correct.

You should always carry with you an identity document valid for expatriation.

11.How can I get other information not available on this web page?

Should you require further information not available on **the dedicated information web page or in these** FAQs, please contact the Data Protection Officer (DPO) at the following certified e-mail address: dpo.pnr@pecps.interno.it.

03/12/2019