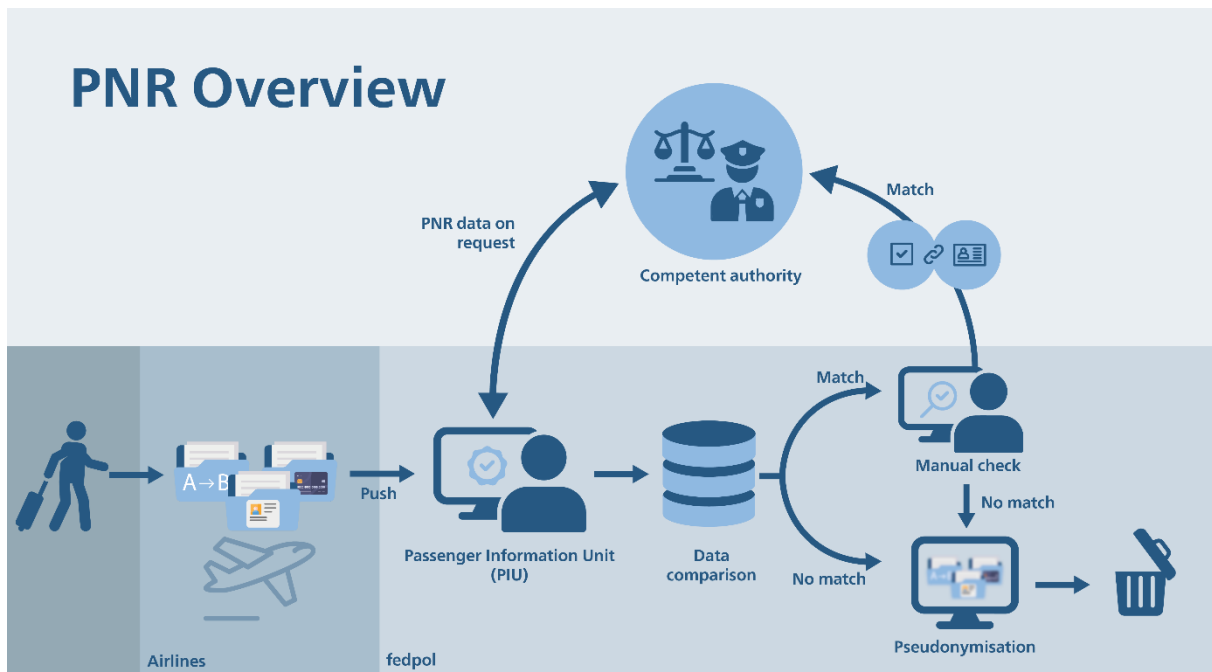




FAQ – Passenger Name Records (PNR)



- **What are passenger name records (PNR)?**

PNR are records containing personal information provided by passengers when booking a flight. They contain the following information:

1. Passenger booking code
2. Date of ticket booking/issue
3. Date of travel
4. Passenger's first names and surnames
5. Passenger's address and contact details, including telephone number and email address
6. Payment/billing details
7. Full itinerary
8. Frequent flyer programme information: name of air carrier/aviation company; programme status and number
9. Name of the travel agency and agent who made the booking
10. Passenger's travel status: details of travel confirmation; check-in status; booked flights not taken; passengers with a ticket but no reservation
11. Information on split/shared passenger data (i.e. when one PNR contains data on persons who book a flight but do not travel together; where this occurs, the PNR data is only collected once and split)
12. For unaccompanied minors (under 18 years): name; gender; age; language(s); name and contact details of person accompanying the minor to departure and relationship to the passenger; name and contact details of

person collecting the passenger on arrival and relationship to the passenger; name of airport staff accompanying the passenger on departure and arrival

13. Ticket information: ticket number; date of issue; single or return ticket; Automated Ticket Fare Quote (ATFQ)
14. Seat number and other seating information
15. Code share information (i.e. when one air carrier sells seats on another air carrier's flight)
16. Baggage information
17. Number and full names of fellow travellers
18. API data¹ if available
19. Any changes to the PNR data listed in numbers 1 to 18

- **For what flights must PNR data be collected?**

Airlines must collect PNR data for all scheduled and chartered flights to and from Switzerland.

- **Is any further information required?**

No further information is required other than that recorded when booking the flight.

- **Will PNR data processing change current airport procedures?**

No, the processing of PNR data will not change airport procedures.

- **What happens to my data?**

- Your PNR data is transmitted to the Passenger Information Unit (PIU) by the airline.
- Upon receipt, the PIU checks the PNR data against police databases, risk profiles and watch lists.
- If the check does not return a match (see graphic below) the PNR data is automatically pseudonymised after a month and deleted after six months.
- If the check returns a match, (see graphic below) the PNR data is checked manually by PIU specialists. If the check is negative, the data undergoes the same process as for a non-match.
- If the check is positive, the match and the PNR data are forwarded to the competent authority.
- A competent authority may also submit a written request to obtain certain data.
- All data disclosed to a competent authority is flagged by the PIU and retained for a period of five years. After that, it is automatically and permanently deleted.
- Data that is not disclosed to an authority remains unflagged. It is revocably pseudonymised a month after it has been sent to the PIU and permanently deleted after a further five months.

¹ See Art. 104a Foreign Nationals and Integration Act FNIA

- **Where is PNR data stored?**
 The data transmitted to the Swiss PIU is stored on a federal government server. This is in accordance with the security requirements for data requiring a very high level of protection as provided for by the federal directives on basic ICT security.
- **What is a risk profile?**
 A risk profile identifies combinations of data, for example travel route and payment method, or travel route and travel agency, which occur frequently in certain criminal offences, particularly in organised crime. It does not contain any personal data. A PIU may only create a risk profile at the request of the competent authorities. The profile is used in the automated comparison of air passenger data. If the comparison returns a match, the result is checked manually by PIU specialists. If confirmed, the data is retained for five years.
- **What is a watch list?**
 A watch list consists of data relating to a known or suspected criminal or terrorist, for example a mobile phone number, a credit card number or the name of a travel agency where a booking was made. The purpose of a watch list is to identify potential threats prior to the departure of an aircraft. A watch list may only be created by a PIU at the request of the competent authorities. If the automated comparison of passenger data with a watch list returns a match, the match is checked manually by PIU specialists.
- **What authorities can obtain PNR data?**
 Under the Intelligence Service Act, fedpol, the cantonal police forces, the Office of the Attorney General of Switzerland, the cantonal public prosecution services, the Federal Intelligence Service and the cantonal law enforcement authorities may obtain PNR data. These authorities do not have direct access to the PNR database, but may obtain PNR data from the PIU on request or in cases that are required by law and lie in their jurisdiction.
- **How can I find out whether my passenger data has been passed on to a law enforcement service?**
 You can submit a request for information to fedpol to find out whether the PIU has forwarded your data to a law enforcement service.
- **Is the PIU permitted to process PNR data, for example, on my dietary preferences, origin, skin colour, or political or other affiliations?**
 The PIU is not permitted to process this type of particularly sensitive data.
- **Will PNR data be used for creating a 'No Fly List'?**
 No, the Passenger Name Record Act does not contain any such provisions.
- **Under what conditions will Switzerland exchange PNR data with other countries?**
 Switzerland will negotiate agreements on exchanging PNR data primarily with countries that guarantee an adequate level of data protection, i.e. a level comparable to that of Switzerland. However, if data protection in the partner state is inadequate, the agreement will contain provisions that the partner state must comply with when processing PNR data from Switzerland.

- **What rules apply to the processing of children's PNR data?**

A child under the age of two may only board an aircraft if accompanied by an adult and does not, in general, occupy its own seat. The child's data is part of the accompanying adult's PNR data and is therefore subject to the same retention period. This rule applies to children up to the age of 12. If a separate flight is booked for a child aged five or over, the child has its own PNR data.

- **Why is PNR data pseudonymised after a month and not deleted immediately?**

In Switzerland, as in the EU, PNR data that does not contain any indication of terrorist or criminal activity is retained for six months. Pseudonymising the data after one month restricts its availability, but increases data protection. The six-month retention period enables law enforcement services to clarify in a PNR-related investigation, for example, whether and how or with whom a person has travelled in that period.

- **What is 'pseudonymisation'?**

Pseudonymising PNR data ensures that it can no longer be attributed to a specific person and thus complies with data protection requirements.

Pseudonymisation can only be lifted by the Federal Administrative Court on request by the competent authorities.