Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP
Federal Office of Police fedpol

Passenger name records (PNR)
Data protection impact assessment (DPIA)

Last updated July 2024

Background

At its meeting on 15 May 2024, the Federal Council adopted the dispatch on the Passenger Name Records Act (PNRA) and submitted it to Parliament. Thanks to this new legislation, Switzerland will be able to set up a national PNR (Passenger Name Record) system. PNR will help to combat terrorism and other serious crime and to protect Switzerland as a business location.

Data protection and safeguarding privacy

The PNRA guarantees that air passengers' data and privacy will be protected. Access to and the use of PNR data are strictly regulated.

In response to feedback from the consultations, the Federal Council has increased the level of data protection. The data retention period has been shortened. For example, data that are not required as evidence of terrorism or other serious criminal offences may not be stored for longer than six months. These data will also be pseudonymised after just one month. This means that information that can identify specific people, such as names, contact details and dates of birth are no longer directly visible in the system. However, if the data contain evidence related to terrorism or other serious criminal offences, the data may be stored for up to five years.

All the main processing steps are logged electronically. The logs will be used by the Federal Data Protection Commissioner (FDPIC) to monitor compliance with data protection requirements.

While drafting the new legislation, a data protection impact assessment (DPIA) in accordance with the new Data Protection Ac was first carried out. The concerns of the FDPIC were taken into account when drawing up the legislation.

Summary of the data protection impact assessment (DPIA) for the Swiss PNR project

The subject of the Swiss PNR project is the collection and processing of passenger name records by the Federal Office of Police (fedpol) in order to combat terrorism and serious crime. The data protection impact assessment (DPIA) allows potential data protection risks to be identified and evaluated at an early stage. The purpose of the DPIA is not limited to identifying and assessing 'high' risks. Rather, the practical benefit of this instrument lies in comprehensibly documenting the causes and analysis of systemic and security-related risks and

thereby enabling suitable measures to be taken to reduce those risks to a level that is acceptable under data protection law. The main content of the DPIA is summarised below.

Description of the data processing

Passenger name records collected by airlines during the booking process include passengers' names, contact information and travel details. These data are passed on by the airlines to the Passenger Information Unit (PIU) and comprise 19 items of data in accordance with Annex 1 of the PNRA.

Identification of particularly vulnerable persons who are affected

This section of the DPIA identifies individuals who are considered particularly vulnerable due to their specific situation. These are:

- **Children:** Children travelling alone or accompanied by a person who is not their parent are particularly vulnerable. These include unaccompanied minors (under the age of 18), for whom detailed information such as name, age, language and contact details of accompanying persons are recorded at the departure and destination airports.
- **Persons with disabilities:** Although the fact that a person has a disability is not normally directly apparent from the PNR data, information that a wheelchair is being transported, for example, could indicate this. However, this information is not conclusive and is not systematically recorded.

Processing personal data

The main benefit of state data processing is that it allows measures to be taken at an early stage to prevent terrorism and serious offences and to bring the (potential) perpetrators to justice.

As soon as the PIU receives the data, it checks them against police information systems, watch lists and risk profiles. This not only allows potential threats of terrorism and serious crime to be identified, but also people on national and international wanted lists who are suspected of or who have been convicted of and sentenced to lengthy prison terms for such offences. Data that do not lead to a hit are pseudonymised after one month and deleted automatically after a further five months. Data that do bring a hit are marked and passed on to the responsible authorities (the police, prosecution authorities or the intelligence services at federal or cantonal levels). Marked data may be stored for up to five years.

After the automatic comparison has been made, PNR data may undergo further processing in specific cases if a competent authority requests their disclosure.

The processing is carried out by employees of the PIU and the responsible federal and cantonal authorities. As the data of millions of passengers are processed every year, the number of processing operations is very high. Advanced technologies are used for data processing, based on a tried and tested UN PNR system. It is not planned to use artificial intelligence in connection with PNR, and all measures are carried out in strict compliance with the legal requirements and data protection standards.

In a separate procedure, the PIU provides the Federal Intelligence Service with PNR data relating to routes that the Federal Council has designated as bearing a particular risk; these data are processed separately.

Identified risks

The DPIA identifies a total of 14 systemic risks to the fundamental rights of data subjects. These include in particular

- unauthorised access to PNR data;
- the misclassification of persons and incorrect labelling of their data due to inadequate information or poor data quality;
- processing of sensitive personal data that should not have been collected in the first

place.

Risk minimisation measures

The DPIA identifies a total of 22 measures that may be used to minimise the identified risks effectively to an acceptable residual risk.

The measures are of a legal, organisational and technical nature and are aimed at reducing the probability of a data breach and the extent of the damage caused.

Here are some examples of how the measures influence the residual risk:

- **Stricter access controls and technical security measures** such as improved verification procedures and logging help to prevent unauthorised access to PNR data and thus reduce the risk of data breaches.
- **Regular employee training to increase awareness and competence in handling sensitive data**, which helps to minimise human error that could lead to data breaches.
- **Technological improvements and regular system checks**, including penetration tests and data integrity checks, which ensure that systems are secure and function correctly, reducing the risk of technical breakdowns.
- **Clear legal and organisational guidelines**, which ensure better compliance and greater accountability within the organisation. This helps to reduce legal and operational risks.
- **Data minimisation and improved data protection practices**, such as the automated deletion or pseudonymisation of data after specified periods, which help to reduce the risk of misuse of old or no longer required data.

Implementation of these measures is crucial in order to ensure the security and protection of the personal data processed.

Assessment of the FDPIC

The FDPIC has examined the present DPIA and states in his Opinion of April 2024 that:

- the DPIA has been properly carried out;
- the information required for the assessment is available;
- the risks to the privacy or fundamental rights of the data subjects inherent in the entire data processing process provided for in the PNRA have been identified;
- appropriate, risk-minimising measures are planned in the case of several high risks that have been identified.

Further information

The complete document ‘Data Protection Impact Assessment PNR Switzerland’ may be requested using the following e-mail address: pnr@fedpol.admin.ch