Act on the Processing of Passenger Name Record (PNR) Data to Implement Directive (EU) 2016/681 (Passenger Name Record Act, FlugDaG)

Passenger Name Record Act of 6 June 2017 (Federal Law Gazette [BGBl.] Part I p. 1484), amended by Article 2 of the Act of 6 June 2017 (BGBl. Part I p. 1484)

This Act is intended to transpose into national law 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 (OJ L 119 of 4 May 2016, p. 132).

Part 1
Passenger information unit and purpose of the passenger name record database

Section 1
Passenger information unit and purpose of the passenger name record database

(1) The Federal Criminal Police Office (Bundeskriminalamt) shall be the national unit for processing passenger name record data (passenger information unit, PIU). The PIU shall maintain a passenger name record database (PNR database) in accordance with this Act.
(2) The PNR database shall serve to prevent and prosecute terrorist offences and serious crime.
(3) The Federal Office of Administration (Bundesverwaltungsamt) shall process PNR data on behalf of and at the instruction of the PIU.

Part 2
Transfer of PNR data to the PIU

Section 2
Data transfer by air carriers

(1) In accordance with subsection 3, air carriers shall transfer to the PIU PNR data of their passengers, including transfer and transit passengers, collected in the course of their business
(2) PNR data are

1. the passenger's family name, name at birth, given names and any doctoral degree;
2. PNR record locator;
3. date of reservation and issue of ticket;

4. date(s) of intended travel;

5. address and contact information, including telephone number and e-mail address;

6. ticketing field information, including ticket number, date of ticket issuance, one-way tickets and automated ticket fare quote fields;

7. all baggage information;

8. 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(s), gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time;

9. other name information;

10. all forms of payment information, including billing address;

11. complete travel itinerary for specific PNR data;

12. frequent flyer information;

13. travel agency and travel agent;

14. travel status of passenger, including confirmations, check-in status, no-show information, ticket without reservation;

15. split and divided PNR data;

16. 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;

17. seat number and other seat information;

18. code share information;

19. number and other names of travellers on the PNR; and

20. all historical changes to the PNR listed in numbers 1 to 19.

(3) PNR data shall be transferred for all scheduled, charter and taxi flights for non-military purposes which

1. depart from the Federal Republic of Germany and arrive in another country, or

2. depart from another country and land in the Federal Republic of Germany as a stopover or final destination.

(4) Where the flight is code-shared between one or more air carriers, the air carrier that operates the flight shall be obligated to transfer to the PIU the PNR data of all passengers on the flight.

(5) Air carriers shall transfer the PNR data to the PIU pursuant to subsection 7, first sentence, at the following times:

1. 48 to 24 hours before the scheduled flight departure time and

2. immediately after flight closure, that is, once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for passengers to board or leave.

If no PNR data are available for a passenger at the time of data transfer pursuant to the first sentence, no. 1, the air carrier shall report the PNR data of this passenger to the PIU no later than two hours prior to the scheduled departure time, as far as the air carrier has these data at that time; the first sentence, no. 2 shall remain unaffected. Data transfer pursuant to the first sentence, no. 2 may be limited to an update of data transferred pursuant to the first sentence, no. 1.

(6) In addition to the times given in subsection 5, in individual cases the PNR data shall be transferred to the PIU immediately upon request, if there is reason to believe that a crime listed in Section 4 (1) is about to be committed in the immediate future, and the data transfer is necessary to carry out the tasks listed in Section 6 (1), first sentence, and (2) first sentence. The first sentence shall apply accordingly to requests pursuant to Section 7 (3), first sentence, no. 3.

(7) Air carriers shall transfer PNR data by electronic means. They shall use the common protocols and supported data formats defined in implementing acts of the European Commission pursuant to Article 16 (3) of 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 (OJ L 119 of 4 May 2016, p. 132). Air carriers shall inform the PIU which protocol and data format they use for transferring PNR data. In the event of technical failure, PNR data shall be transferred in agreement with the PIU using any other appropriate means ensuring an appropriate level of data security.

Section 3
Transfer of PNR data collected by other enterprises

Where other enterprises which are involved in reserving or booking flights or issuing tickets transfer PNR data to air carriers in the course of their business, the following shall apply:

1. the air carriers shall transfer these data to the PIU without prejudice to Section 2 (1) at the times given in Section 2 (5), first and second sentences;

2. the other enterprises shall transfer the PNR data to the relevant air carrier enough in advance so that the air carrier can transfer the data to the PIU at the times given in Section 2 (5), first and second sentences.

Part 3
Processing of PNR data by the PIU

Section 4
Conditions of processing

(1) The PIU shall process the PNR data transferred by the air carriers and check them against databases and patterns in accordance with subsections 2 and 5 in order to identify persons for whom there is reason to believe that they have committed or will commit in the foreseeable future one of the following offences:

1. an offence pursuant to Section 129a, also in conjunction with Section 129b, of the Criminal Code;

2. an offence identified in Section 129a (1) nos. 1 and 2, (2) nos. 1 to 5 of the Criminal Code which are intended to seriously intimidate the population, to unlawfully coerce an authority or an international organization by the use or the threat of force or to abolish or significantly impair the fundamental political, constitutional, economic or social structures of a state or an international organization, and which may, by their modus operandi or their consequences, seriously harm a state or an international organization;

3. an offence intended to threaten one of the offences referred to in no. 2;

4. an offence pursuant to Sections 89a to 89c and 91 of the Criminal Code;

5. an offence directly connected to terrorist activities pursuant to Article 3 (2) of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164 of 22 June 2002, p. 3), last amended by Article 1 no. 1 of Council Framework Decision 2008/919/JHA (OJ L 330 of 9 December 2008, p. 21); or

6. an offence corresponding to an offence listed in Annex II of Directive (EU) 2016/681 and punishable by a custodial sentence of at least three years.

(2) The PIU shall be permitted to conduct an automated check of PNR data before an aircraft lands at or takes off from an airport in the Federal Republic of Germany

1. against databases on persons or objects sought or under alert, and

2. against certain patterns (advance check).

The PIU shall individually examine any matches resulting from an advance check.
(3) The PIU shall draw up the patterns for checks pursuant to subsection 2, first sentence, no. 2 in consultation with the PIU's data protection officer and shall be reviewed regularly, at least every six months, in cooperation with the authorities listed in Section 6 (1), first sentence and (2), first sentence, and with the PIU's data protection officer. The patterns shall contain incriminating or exonerating criteria. Incriminating criteria shall be based on the facts which the authorities referred to in Section 6 (1), first sentence or (2) first sentence have concerning certain offences. They must be suitable for identifying persons who meet meaningful criteria for preventing and prosecuting the offences listed in subsection 1. Exonerating criteria shall serve to rule out as suspects persons who fall under incriminating criteria. In the patterns, incriminating criteria shall be combined with exonerating criteria such that the number of persons matching the pattern is as small as possible. 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. The Federal Commissioner for Data Protection and Freedom of Information shall review the production and use of the patterns at least every two years. He or she shall report to the Federal Government every two years.
(4) The PIU may analyse PNR data to produce or update patterns for the advance check.
(5) In the individual case and following a justified request by the competent authorities listed in Section 6 (1), first sentence, the PIU may in special cases check data transferred from the requesting authority against data stored in the PNR database for the purposes listed in Section 1 (2). The first sentence shall apply to the authorities listed in Section 6 (2), first sentence accordingly on the condition that the data may be checked for the purpose of carrying out their tasks related to offences pursuant to subsection 1.

Section 5
Depersonalization of data

(1) Upon expiry of a period of six months after the transfer of the PNR data to the PIU, the PIU shall depersonalize all PNR data by masking out the following data elements which could serve to identify a person referred to in Section 2 (1):

1. name information as referred to in Section 2 (2) nos. 1 and 9 as well as the names and number of other passengers on the PNR travelling together as referred to in Section 2 (2) no. 19;

2. address and contact information as referred to in Section 2 (2) no. 5;

3. all forms of payment information, including billing address, as referred to in Section 2 (2) no. 10, which could serve to identify the passenger or any other persons;

4. frequent flyer information as referred to in Section 2 (2) no. 12;

5. general remarks as referred to in Section 2 (2) no. 16 which could serve to identify the passenger; and

6. data as referred to in Section 2 (2) no. 8.

(2) The PIU shall be permitted to reverse the depersonalization of PNR data only if doing so

1. is necessary to prevent or prosecute offences pursuant to Section 4 (1) in case of a data check pursuant to Section 4 (5), first sentence; and

2. has been approved by a court at the request of the head of the PIU or his or her deputy.

In case of imminent danger, the president of the Bundeskriminalamt or his or her deputy may issue the approval. The court's approval shall be obtained subsequently and without delay. With regard to the authorities listed in Section 6 (2), first sentence, the first to third sentences shall apply accordingly on the condition that the reversal of depersonalization is necessary in the case of a check pursuant to Section 4 (5), second sentence, for the purpose of carrying out their tasks related to offences pursuant to Section 4 (1).

Part 4
Transfer of PNR data by the PIU

Section 6
Transfer of data to the competent authorities in Germany

(1) Where necessary to carry out its tasks of preventing or prosecuting criminal offences pursuant to Section 4 (1), the PIU may transfer the PNR data resulting from a check pursuant to Section 4 (2) or (5) and the results of processing these data to the following authorities for further examination or to take suitable measures:

1. the Federal Criminal Police Office (Bundeskriminalamt),

2. the criminal police offices of the federal states (Landeskriminalämter),

3. the Customs administration (Zollverwaltung), and

4. the Federal Police (Bundespolizei).

The transfer of data resulting from a check pursuant to Section 4 (5) to any authority other than the requesting authority shall be permitted only in agreement with the requesting authority.

(2) Where necessary to carry out its tasks related to criminal offences pursuant to Section 4 (1), the PIU may also transfer the PNR data resulting from a check pursuant to Section 4 (2) or (5) and the results of processing these data to the following authorities:

1. the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz), and its counterparts in the federal states;

2. the Military Counterintelligence Service (Militärischer Abschirmdienst); and

3. the Federal Intelligence Service (Bundesnachrichtendienst).

Subsection 1, second sentence, shall apply accordingly.

(3) The authorities listed in subsection 1, first sentence, and subsection 2, first sentence, shall be permitted to process the transferred data only for the purposes for which they were transferred.

(4) The authorities listed in subsection 1, first sentence, may, in carrying out law enforcement tasks, process the transferred data for other purposes, if intelligence, including additional information, provides reason to suspect another specific offence.

Section 7
Exchange of data between European Union Member States

(1) The PIU shall be responsible for sharing PNR data and the results of processing the data with the PIUs of other Member States of the European Union.
(2) In response to a justified request by one of the authorities referred to in Section 6 (1), first sentence, the PIU may ask the PIU of another Member State

1. to transfer PNR data and results of processing these data, where necessary to prevent or prosecute offences pursuant to Section 4 (1); or

2. to obtain PNR data from air carriers and transfer these data, where necessary to prevent or prosecute an offence pursuant to Section 4 (1) which is about to be committed in the immediate future.

In case of imminent danger, a justified request pursuant to the first sentence, no. 1, may also be submitted by an authority as referred to in Section 6 (1), first sentence. A copy of the request shall be sent to the PIU of the requesting Member State. With regard to the authorities listed in Section 6 (2), first sentence, the first to third sentences shall apply accordingly on the condition that

1. the transfer is necessary to carry out their tasks related to offences pursuant to Section 4 (1); and

2. in the case of the first sentence, no. 2, an offence pursuant to Section 4 (1) is about to be committed in the immediate future.

(3) The PIU may transfer PNR data and the results of processing these data to the PIUs of other Member States if

1. a check pursuant to Section 4 (2) or (5) or an analysis of PNR data pursuant to Section 4 (4) reveals that the data are necessary for authorities of other Member States to carry out tasks to prevent or prosecute terrorist offences or serious crime;

2. the PIU of another Member State has submitted a request indicating that there is reason to believe that the data transfer is necessary to prevent or prosecute terrorist offences or serious crime; or

3. the PIU of another Member State has submitted a request to obtain PNR data from air carriers and transfer this data, and the request indicates that there is reason to believe that the data transfer is necessary to prevent a terrorist offence or a serious crime about to be committed in the immediate future.

Data resulting from a check pursuant to Section 4 (5) shall be transferred pursuant to the first sentence, no. 1 only in agreement with the authority requesting the check. In the cases of the first sentence, no. 2, a competent authority of another Member State may submit the request in case of imminent danger, if the Member State has included it in the notification to the European Commission pursuant to Article 7 (3) of Directive (EU) 2016/681 and the European Commission has published this notification in the Official Journal of the European Union. Section 5 (2) shall apply accordingly to data transferred on the basis of a request pursuant to the first sentence, no. 2.
(4) The PIU may process PNR data and the results of processing these data transferred from the PIUs of other Member States and may transfer them to the authorities listed in Section 6 (1), first sentence if

1. an individual examination reveals that the data are necessary for these authorities to carry out their tasks of preventing or prosecuting offences pursuant to Section 4 (1); or

2. the data were requested using a justified request pursuant to subsection 2, first or second sentence, and are necessary for these authorities to carry out their tasks.

The transfer of data pursuant to the first sentence, no. 2 to any authority other than the requesting authority shall be permitted only in agreement with the requesting authority. With regard to the authorities listed in Section 6 (2), first sentence, the first and second sentences shall apply accordingly on the condition that the data transfer is necessary for the purpose of carrying out their tasks related to offences pursuant to Section 4 (1).
(5) The provisions concerning international mutual assistance in criminal matters shall remain unaffected.

Section 8
Participation in joint procedures for cooperation

The PIU may participate in joint procedures for systematic cooperation with PIUs of other Member States to prevent and prosecute terrorist offences and serious crime in accordance with this Act. Section 7 shall remain unaffected.

Section 9
Transfer of data to Europol

The PIU may transfer to Europol PNR data and results of processing these data if Europol submits a request indicating that there is reason to believe that the data transfer is necessary for Europol to prevent or prosecute terrorist offences or serious crime. Section 5 (2) shall apply accordingly.

Section 10
Transfer of data to third countries

(1) While abiding by Sections 78 to 80 of the Federal Data Protection Act, in individual cases the PIU may transfer PNR data and the results of processing these data on request to authorities of countries which are not Member States of the European Union (third countries) if

1. these authorities are responsible for preventing or prosecuting terrorist offences or serious crime, and the data transfer is necessary for this purpose; and

2. these authorities agree to transfer the data to the authorities of another third country only if doing so is necessary to prevent or prosecute terrorist offences or serious crime, and only with the prior consent of the PIU.

Section 5 (2) shall apply accordingly. The provisions concerning international mutual assistance in criminal matters shall remain unaffected.
(2) The PIU may transfer the PNR data of another Member State under the conditions of subsection 1 to authorities of third countries only with the consent of the PIU of that Member State. If consent has not been obtained, transfer shall be permitted only if

1. the transfer is essential to prevent imminent danger from terrorist offences or serious crime in a Member State or a third country, and

2. prior consent cannot be obtained in time.

The PIU responsible for giving consent pursuant to the second sentence shall be informed without delay.
(3) The PIU shall inform the data protection officer of the PIU each time PNR data are transferred pursuant to subsections 1 and 2. The data protection officer of the PIU shall subsequently review data transfers pursuant to subsection 2, second sentence.

Part 5
Data protection provisions

Section 11
National supervisory authority

The Federal Commissioner for Data Protection and Freedom of Information shall perform the tasks of the national supervisory authority for data protection.

Section 12
Data protection officer of the PIU

(1) The data protection officer of the Bundeskriminalamt (Federal Criminal Police Office) shall perform the tasks of the data protection officer of the PIU.
(2) The data protection officer of the PIU may refer a matter to the national supervisory authority if he or she believes that an instance of processing PNR data violates the law.

Section 13
Deletion of data

(1) The PIU shall delete PNR data from the PNR database after a period of five years has elapsed from the time of their transfer to the PIU. PNR data transferred to the authorities listed in Section 6 (1), first sentence or (2), first sentence shall be deleted in accordance with the provisions which apply to these authorities.
(2) If the PIU receives data transferred from air carriers to the PIU which are not PNR data as defined in Section 2 (2) it shall delete them immediately.
(3) If the PIU receives PNR data as defined in Section 2 (2) which contain information on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation it shall delete them immediately.
(4) The PIU shall delete the results of processing PNR data as soon as they are no longer necessary to inform the authorities listed in Section 6 (1), first sentence or (2), first sentence, the PIUs of other Member States, Europol or authorities of third countries. Results of processing from analyses of PNR data shall be deleted by the PIU as soon as they are no longer needed to create or update patterns for the advance check or for the information of other Member States' PIUs. The results of processing PNR data which were transferred to the authorities listed in Section 6 (1), first sentence or (2), first sentence shall be deleted in accordance with the provisions which apply to these authorities.
(5) If the individual examination pursuant to Section 4 (2), second sentence following an advance check results in no matches, this result shall be deleted no later than the related data pursuant to subsection 1, first sentence.

Section 14
Logging

(1) The PIU shall keep records of at least the following processing operations:

1. collection,
2. alteration,
3. consultation,
4. transfer and
5. deletion.

(2) The records of consultation and transfer must make it possible to ascertain the justification, date and time of these operations and, as far as possible, the identity of the person who consulted or transferred personal data, and the identity of the data recipients.
(3) The records may be used only by the data protection officer of the PIU or the national supervisory authority to verify the lawfulness of the processing; and for self-monitoring, ensuring the integrity and security of the personal data, and for audits.
(4) These records shall be retained for five years and then destroyed.
(5) The PIU shall make these records available to the national supervisory authority on request.
(6) The information shall be recorded such that the records are available to the data protection officer of the PIU or the national supervisory authority in electronic form to verify the lawfulness of the processing.

Section 15
Documentation obligation

(1) The PIU shall maintain documentation relating to all processing systems and procedures under their responsibility.
(2) This documentation shall contain at least the following information:

1. the name and contact details of the PIU and personnel in the PIU entrusted with the processing of the PNR data, and the different levels of access authorization;

2. the requests made by

   a) authorities referred to in Section 6 (1), first sentence, and (2), first sentence;

   b) authorities of other Member States listed in Article 7 (3) of Directive (EU) 2016/681;

   c) PIUs of other Member States; and

   d) Europol; as well as

3. the requests made by authorities of third countries and every transfer of PNR data to authorities of third countries.

(3) The PIU shall make all available documentation available to the national supervisory authority upon request.

Part 6
Applicability of the Act on the Bundeskriminalamt

Section 16
Applicability of the Act on the Bundeskriminalamt

The Act on the Bundeskriminalamt shall apply accordingly unless this Act contains more specific provisions.

Part 7
Final provisions

Section 17
Jurisdiction, procedures

The local court in the jurisdiction where the Bundeskriminalamt has its headquarters shall be responsible for judicial decisions pursuant to this Act. The provisions of the Act on Procedure in Family Matters and Non-Contentious Matters shall apply accordingly to the procedure.

Section 18
Provisions on administrative fines

(1) An administrative offence shall be deemed to have been committed by any person who, intentionally or negligently,

1. in violation of Section 2 (5), first sentence, in conjunction with (2) nos. 1 to 8 fails to transfer the PNR data listed there on time, in the proper form or at all; or

2. in violation of Section 2 (5), second sentence, first half-sentence in conjunction with (2) nos. 1 to 8 fails to report the PNR data listed there on time, in the proper form or at all.

(2) This administrative offence may be punished by a fine of up to fifty thousand euros.
(3) The administrative authority within the meaning of Section 36 (1) no. 1 of the Act on Administrative Offences shall be the Federal Office of Administration.