Privacy statement; Passenger name records

1 Controller

National Police Board
Postal address: P.O. Box 1000, 02151 Espoo
Street address: Vuorimiehentie 3, Espoo
Telephone: 0295 480 181 (exchange)
E-mail: kirjaamo.poliisihallitus@poliisi.fi

2 Data Protection Officer for PNR

National Police Board
Jaana Riikonen, Senior Adviser
For contact details, see section 1 above.

3 National Police Board's Data Protection Officer

National Police Board
Harri Kukkola, Senior Adviser
For contact details, see section 1 above.

4 The legal basis for the processing of personal data

The Passenger Information Unit (PIU) is authorised to process personal data in order to prevent, detect, investigate and prosecute terrorist offences and serious crime.

The processing of personal data by the PIU and the legal basis for such processing are provided for in, among others, the following laws:

- the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018)
- the Police Act (872/2011)
- the Police Decree (1080/2013)
- the Act on the Use of Airline Passenger Name Record (PNR) Data to Combat Terrorist Offences and Serious Crime (657/2019)
- 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.

5 The purposes of processing personal data, the categories of data subjects and the categories of personal data processed

The PIU has the authority to process personal data within the meaning of the Act on the Use of Airline Passenger Name Record (PNR) Data to Combat Terrorist Offences and Serious Crime in order to identify individuals who may have links to terrorist offences or serious crime.

The PIU operates in conjunction with a collaborative criminal intelligence unit consisting of representatives of the Police, Customs and the Border Guard.

The PIU processes PNR data for the following purposes:

1) to carry out an assessment of passengers prior to their scheduled arrival or departure
2) to respond to a duly reasoned request based on sufficient grounds from a competent authority, a PIU of another Member State or Europol to provide and process PNR data and
3) to analyse PNR data for the purpose of updating or creating new criteria to be used in the assessments.

The PIU may compare PNR data by automated means against the following kinds of data and the following information systems and registers:

1) personal data within the meaning of the Act on the Processing of Personal Data by the Police that are processed for investigative or surveillance-related purposes, personal data that are processed for the purpose of preventing or detecting crime and personal data that are processed in order to ensure the performance of other statutory duties of the Police
2) personal data processed by the Finnish Security Intelligence Service in order to protect national security, to prevent, detect and investigate actions or campaigns that threaten public or social order or national security and to prevent and detect crime that threatens public or social order or national security
3) the Schengen Information System
4) personal data processed by the Border Guard for border-control purposes and in order to maintain border security and order, to investigate crime and to maintain public order and safety, as well as to prevent and detect crime

5) data required to ensure the performance of the statutory surveillance and crime-prevention duties of Customs and to prevent, detect, investigate and prosecute customs offences
6) the Register of Aliens
7) the Transport Register and more specifically data concerning registered vehicles, watercraft and operator's licences
8) the Population Information System
9) databases of the International Criminal Police Organisation (INTERPOL) and
10) data within the meaning of section 3, subsection 2 of the Act on the European Union Agency for Law Enforcement Cooperation (Europol) (214/2017).

Any positive matches resulting from the automated processing of PNR data are reviewed individually.

The PIU may not process any 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.

Notwithstanding secrecy provisions, data in the filing system of the police may also be processed in oversight of legality, analysis, planning and development activities. Such data may also be used in training activities if the data are essential for carrying out the training.

6 Disclosure of data subjects' personal data

The PIU has the right to disclose PNR data concerning any individuals identified in the course of the processing of PNR data or the result of processing such data to a competent authority in order for the latter to be able to investigate such individuals' links to terrorist offences or serious crime.

PNR data or the result of processing such data may also be disclosed to a competent authority in response to the latter's duly reasoned request based on sufficient grounds to process PNR data for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.

The aforementioned kinds of data may only be disclosed for a specific purpose.

A competent authority may also use information provided by the PIU to investigate, prevent and detect offences, or indications thereof, that come to light

in the course of the processing of the data as well as to refocus their efforts and support the presumption of innocence.

The PIU has a duty to transmit the details of any individuals identified on the basis of the legitimate processing of PNR data to the corresponding PIUs of other Member States. The PIU may also disclose PNR data or the result of processing such data to a PIU of another Member State at the latter's duly reasoned request.

The PIU may disclose PNR data or the result of any further examination of such data to Europol at the latter's duly reasoned request to process data for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime within the meaning of Chapter IV of the Regulation of the European Parliament and of the Council referred to in section 3, subsection 1, paragraph 10 of the Act on the Use of Airline Passenger Name Record (PNR) Data to Combat Terrorist Offences and Serious Crime where such a disclosure is necessary to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime within the meaning of Article 3 of the Regulation.

The PIU may only transfer PNR data and the result of processing such data to a third country on a case-by-case basis and only if

1) the conditions laid down in sections 41 to 43 of the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security are met and
2) the transfer is necessary in order to prevent, detect, investigate and prosecute terrorist offences or serious crime.

The PIU may only authorise the transfer of any PNR data and the result of processing such data from a third country to another third country where the same is strictly necessary in order to combat terrorist offences or serious crime.

The PIU may only transfer PNR data obtained from the PIU of another Member State to a third country without the prior consent of the Member State in question if such a transfer is essential to respond to a specific and actual threat related to terrorist offences or serious crime in a Member State or a third country, and prior consent cannot be obtained in good time. Such transfers must be communicated to the PIU of the Member State concerned as well as duly recorded and subjected to an *ex-post* verification.

The PIU may only transfer PNR data to the competent authorities of third countries after ascertaining that the use that the recipients intend to make of the PNR data is consistent with the aforementioned conditions and safeguards. The PIU's Data Protection Officer must be notified of all such transfers.

7 Erasure, depersonalisation and archiving of personal data

The PIU may only keep PNR data for a period of five years from the transfer of the same to the PIU. Upon the expiry of a period of six months after the transfer of PNR data, the PIU must depersonalise all PNR data through masking out the following data elements:

1) name(s), including the names of other passengers on the PNR and the number of travellers on the PNR travelling together
2) address and contact information
3) all forms of payment information, including the billing address, to the extent that it contains any information that could serve to directly identify the passenger to whom the PNR data relate or any other persons
4) frequent flyer information
5) general remarks and
6) any advance passenger information that has been collected.

To depersonalise through masking out of data elements' means to render those data elements that could serve to directly identify the passenger to whom the PNR data relate invisible to a user.

The PIU may only keep the result of the processing referred to in section 7 of the Act on the Use of Airline Passenger Name Record (PNR) Data to Combat Terrorist Offences and Serious Crime for as long as the same is necessary to inform the competent authorities or the PIUs of other Member States of a positive match. Where a result proves negative after further examination, it may, however, be stored so as to avoid future false positive matches for as long as the underlying data are not deleted under the first subsection. Such false results must be communicated to the competent authority or the PIU of the other Member State to which the result of the processing was disclosed.

In the event that PNR data received by the PIU are found to contain any information not listed in section 4, subsection 2 of the Act on the Use of Airline Passenger Name Record (PNR) Data to Combat Terrorist Offences and Serious Crime or any information revealing a person's race or ethnic origin, political

opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation, such data are deleted immediately.

8 Rights of data subjects

To ensure transparent and open provision of information and to promote the exercising of data subjects' rights, the police have made extensive information available to all on the www.poliisi.fi/en website. The site offers detailed information on matters such as how a data subject can check his/her personal data; when the right to check the information can be restricted; how and on what grounds the information can be rectified or deleted; how the police process log data; how the police, in its role as data controller, protects the rights of the data subjects; and how internal control is exercised in connection to the processing of personal data.

To ensure that the above-mentioned information is available to all in another manner, as well, a Police Data Files folder can be found at all customer service points of the police. It contains similar information aimed at data subjects in paper format.

8.1 Right of data subjects to check their records / right of access by the data subject

The starting point is that everyone has the right to obtain information from the controller as to whether his/her personal data is processed. If the data is processed, the data subject has the right to obtain from the controller, upon request, the information specified in section 23 of the Act on Data Protection in Criminal Matters.

When wishing to exercise the right to check the above-mentioned information, the data subject must submit the request to do so to the controller or police department in person and to prove his/her identity. The data subject may bring along an assistant. The request must be sufficiently specific: it must indicate, with sufficient accuracy, which personal data file or part of a personal data file it refers to.

A data subject's right to check information can be restricted if, taking into consideration the data subject's rights, it is necessary and proportionate in order to

1) prevent, uncover or solve crimes, take legal action in connection to a crime or avoid inconvenience in connection to the enforcement of criminal sanctions

2) safeguard investigation, clarification or similar procedures
3) preserve public safety
4) preserve national security or
5) protect the rights of other people.

If a data subject's right to check information is suspended, restricted or refused, the controller must, without undue delay, inform the data subject of this in writing. The grounds for the suspension, restriction or refusal must also be stated, unless doing so would jeopardise the purpose of the denial or restriction. If the data subject has not, within three months of making the request, received a written reply, this will be considered tantamount to refusing the right of access.

Data subjects have the right to request the Data Protection Ombudsman to investigate the legality of personal data and its processing if the right of access has been postponed, restricted or denied by virtue of the Act on Data Protection in Criminal Matters or other legislation. The request must be submitted in person to the Data Protection Ombudsman, controller (National Police Board) or police department, and the person submitting the request is required to prove their identity.

Data subjects have the right to refer matters to the Data Protection Ombudsman (request for action) if they consider the processing of their personal data to be in violation of the Act on Data Protection in Criminal Matters or other legislation on the processing of personal data.

Office of the Data Protection Ombudsman:
Street address: Lintulahdenkuja 4, 00530 Helsinki
Postal address: P.O. Box 800, 00531 Helsinki
Telephone exchange: 029 566 6700, Fax: 029 566 6735
Email (registry): tietosuoja@om.fi

8.2 Rectification or erasure of personal data and restriction of processing

The controller must, unprompted or at the demand of the relevant data subject and without undue delay, rectify or complete personal data that is inaccurate or incomplete for the purpose of its processing.

The controller must, unprompted or at the demand of the relevant data subject and without undue delay, erase personal data if its processing violates the requirements of the Act on Data Protection in Criminal Matters regarding legality,

purpose of use, necessity or accuracy, or the provisions regarding special categories of personal data.

However, instead of erasing the data, the controller must restrict its processing if:
1) the data subject contests the accuracy of the data, and its accuracy or inaccuracy cannot be verified (before removing this restriction, the controller must inform the data subject of the removal) or
2) the personal data has to be retained for evidence purposes.

The data subject can submit the request to have his/her personal data rectified or erased or to have its processing restricted to the controller or another police unit. The request must be sufficiently specific: it must indicate whose personal data it concerns, which personal data the data subject wishes to have rectified or erased or the processing of which data the data subjects wishes to have restricted, why the data subject finds the data incomplete, inaccurate or defective for its purpose of processing, what changes the data subject demands to the data, and why the processing of the data should be restricted. The controller is entitled to request further information to confirm the identity of the data subject.

A data subject's right to have personal data rectified or erased or to have the processing of data restricted can be restricted if, taking into consideration the data subject's rights, it is necessary and proportionate in order to
1) prevent, uncover or solve crimes, take legal action in connection to a crime or avoid inconvenience in connection to the enforcement of criminal sanctions
2) safeguard investigation, clarification or similar procedures
3) preserve public safety
4) preserve national security or
5) protect the rights of other people.

If the controller refuses the data subject's request to have data rectified, completed or erased or to have the processing of data restricted, the controller must inform the data subject of this refusal and its grounds in writing. The grounds for the refusal can be omitted fully or in part to the extent that this is necessary on the grounds specified in the previous section.

The data subject has the right to request the Data Protection Ombudsman to check the legality of personal data and its processing if, pursuant to the Act on Data Protection in Criminal Matters or some other law, the controller does not accept the data subject's request to have his/her data rectified, completed or

erased or to have the processing of this data restricted (contact information provided above).

When inaccurate personal data is rectified, the controller must notify the authority from which the inaccurate data was obtained. If personal data has been rectified or completed or if its processing has been restricted on the basis of section 25 of the Act on Data Protection in Criminal Matters, the controller must notify the recipients to which it has disclosed this data. The recipients must also rectify or erase this personal data or restrict its processing.

8.3 Other rights of the data subject

The data subject's right to object to the processing of data, right to have the data transmitted from one system to another and right not to be subjected to automated decision-making do not apply when the police processes personal data in connection with a statutory police duty related to the prevention and uncovering of crimes or in order to exercise the official authority of the police.

8.4 The data subject's right to exercise rights and have action taken free of charge

Generally, there is no fee for the notifications and information sent to a data subject on the basis of the Act on Data Protection in Criminal Matters or for the processing of the requests submitted by the data subject. However, if the requests of the data subject are clearly unreasonable or unfounded because of their frequency or for other reasons, the controller may charge a fee. The grounds for the fee amounts are specified in the Act on Criteria for Charges Payable to the State (150/1992). If the controller charges a fee on the above grounds, it must be able to demonstrate that the request is clearly unfounded or unreasonable.

9 Protection and control of personal data by the Police

The controller and the processor of personal data must ensure, through technical and organisational measures, that personal data is sufficiently protected, taking into consideration the threats posed to the data subject's rights by the processing. In particular, personal data must be protected from unlawful processing and accidental deletion, destruction and corruption. When planning and implementing measures, the following must be taken into consideration:

1) the latest technology
2) the implementation costs of the measures

3) the nature, extent, context and purposes of processing and
4) the threats posed to the rights of a natural person, which vary in probability and severity.

The basis of the National Police Board's technical, administrative and organisational information security is the information security and protection policy, which defines the goals, responsibilities, implementation measures and means of implementation in police administration. The information security policy is expanded upon in various separate regulations and guidelines.

The National Police Board has issued a guideline on internal legality control and certain other legal matters in the police. The guideline provides the basis for the planning and realisation of internal legality control by the police and the reporting of the results, also in regard to monitoring the use of information systems and the processing of personal data by the police.

In the legality control of the use of personal data files and the processing of personal data, special attention is paid to the accuracy of and need for the processed data, the appropriate use of the data, the correctness and validity of access rights, and the processing of data in accordance with the classification requirements for confidential documents and information. In the monitoring of the processing of special categories of personal data, special attention is paid to appropriate implementation of the technical and organisational protection measures required to safeguard data subjects' rights, as well as to making sure that personal data is only processed when it is necessary for the police to perform its statutory duties.

10 Availability of the privacy statements

The privacy statements of the police are publicly available in electronic format on the national police information network (www.poliisi.fi) and in the internal information network of the police (Intranet), and in paper format at all customer service points of the police.

In addition, privacy statements are stored in the police's administrative case management, decision-making and archiving system (Acta).