Privacy statement; National Visa Information System (Police Data)

1 Controller

National Police Board
Postal address: P.O. Box 1000, 02151 Espoo
Street address: Vuorimiehentie 3, Espoo
Telephone: +358 (0)29 548 0181 (exchange)
Email: kirjaamo.poliisihallitus@poliisi.fi

2 Contact person for enquiries concerning data protection

National Police Board
Jaana Nieminen, Senior Adviser
Contact information: see section 1

3 National Police Board's Data Protection Officer

National Police Board
Harri Kukkola, Senior Adviser
Contact information: see section 1

4 The legal basis for the processing of personal data

The police process the personal data saved to the National Visa Information System in order to comply with the statutory obligations of the police and in order to exercise the public authority of the police subject to meeting the conditions set out in the data protection legislation. According to the data protection legislation, statutory obligations can only be based on the law of the European Union or a member state, and public authority must have been granted through legislation or other legal provisions.

The processing of personal data by the police and the legal basis for such processing is governed by the following laws, among others:

- Act on the Processing of Personal Data by the Police (616/2019, hereafter referred to as the Police Personal Data Act)
- Finnish Immigration Service Personal Data Act (615/2020)
- General Data Protection Regulation (EU) 2016/679
- Data Protection Act (1050/2018)

- Police Act (872/2011)
- The Police Decree (1080/2013)
- Act on Background Checks (726/2014).

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

The police process the personal data saved to the National Visa Information System for the following purposes:
1) to deal with matters related to a foreign person's entry into, departure from and residence in Finland, to take the relevant decisions and to monitor the situation.

This involves the police processing the personal data saved to the National Visa Information System as it relates to their identity, their family connections, who represents them, their skills and expertise, their contact details, their travel documents, the card that shows that their application process has been initiated within the meaning of section 96 of the Aliens Act, and the other information described in section 7(2) of the Finnish Immigration Service Personal Data Act.

In connection with such duties, the police may also deal with any remarks that they see or that reach their attention and that, given the circumstances or a person's behaviour, can reasonably be thought to fall within the controller's competence and thus allow the controller to oversee the existence of the conditions that relate to a person's entry into the country and their stay here or to decide on the acquisition or loss of Finnish citizenship, or can be reasonably thought to relate to the relevant person's responsibility for the occupational safety of those he or she employs. The police may furthermore process the personal data of family members, those residing in the same household, those acting as hosts in Finland and the employers of foreign workers.

According to section 6(1) of the same Act, the police have the right to process the data it has stored in the National Visa Information System for the purpose described above for purposes other than the original one, i.e. processing, in compliance with sections 13(1) and (2) of the Act on the Processing of Personal Data by the Police.

The Act on the Processing of Personal Data by the Police is applied as a supplementary instrument in the processing of personal data in connection with the performance of police duties, where no special legislation contains provisions that deviate from that Act.

The police only process special categories of personal data in connection with the performance of police duties if this is absolutely necessary.

6 Regular disclosure of data

The right of access to data among the controllers of the National Visa Information System is laid down in section 12 of the Finnish Immigration Service Personal Data Act. Section 13 of the Act deals with other rights of access to data.

According to the Act on the Processing of Personal Data by the Police, the police may, provisions on secrecy notwithstanding, release through a user interface or as a data set personal data related to other statutory tasks of the police to other authorities for the performance of their tasks laid down in the law by virtue of the Act on the Processing of Personal Data by the Police itself or another Act, provided that the requirements of the Acts are met.

Under the Finnish Immigration Service Personal Data Act, the police may, provisions on secrecy notwithstanding, release personal data to the European Union's common information systems established by regulations issued pursuant to Chapter 2 of Title V of the Treaty on the Functioning of the European Union, as enacted in these regulations.

The Act on the Processing of Personal Data by the Police contains separate provisions on the right of the police to transfer personal data in connection with the duties referred to in Chapter 1, section 1 of the Police Act, provisions on secrecy notwithstanding, through a user interface or as a data set somewhere abroad for the purposes of international cooperation.

7 Erasure and archiving of personal data

Subject to an international obligation or the law, personal data processed on the basis of the Immigration Service Personal Data Act should be deleted as follows:
1) the customer number, name, date of birth, personal identity code, foreign identity number, any other code or number issued to identify a foreign person, nationality and the person's family connections should be deleted from a person's identification information ten years after they have died, or have acquired Finnish citizenship, or the details of matters relating to that person have been deleted;
2) the personal data and the details of matters relating to the person other than those referred to in section 1 should be deleted no later than five years after the

right of residence expires or five years after the last entry of the details of the most recent pending case;
3) special categories of personal data are deleted as soon as they become unnecessary to keep;
4) remarks are deleted when six months have passed since they were recorded.

Personal data that is found to be erroneous should be kept along with the corrected version if this is necessary in order to safeguard the rights of the data subject, other interested parties or the controller's staff. Such data should only be processed for the purpose mentioned. Personal data found to be erroneous must be deleted as soon as there is no longer any need to keep it in order to safeguard people's rights.

According to the Immigration Service Personal Data Act, separate provisions will be enacted concerning archiving tasks and the documentation to be transferred to the archives.

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

In principle, 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 Article 15 of the General Data Protection Regulation.

According to the Finnish Immigration Service Personal Data Act, section 41 of the Act on the Processing of Personal Data by the Police applies to the presentation of a request for right of access to data stored in the police register.

When wishing to exercise the right to check the above-mentioned data, 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.

The data subject does not have the right of access to data which has been collected concerning him or her, referred to in Article 15 of the Data Protection Regulation, if:

1) providing access to the data could compromise national security, defence, or public order and security, or hamper the prevention or investigation of offences
2) providing access to the data could seriously endanger the health or treatment of the data subject or the rights of the data subject or some other person or
3) the personal data is used in the performance of supervisory and inspection tasks and the refusal to provide access to the data is necessary to safeguard an important economic or financial interest of Finland or the European Union.

If only a part of the data concerning a data subject is such that it under subsection 1 falls outside the scope of the data referred to in Article 15 of the Data Protection Regulation, the data subject has the right of access to the remainder of the data concerning him or her. The data subject shall be informed of the reasons for the restriction, unless this undermines the purpose of the restriction.

Where the data subject does not have the right of access to data which have been collected concerning him or her, the information referred to in Article 15(1) of the Data Protection Regulation shall be provided to the Data Protection Ombudsman on the request of the data subject.

The controller must, without undue delay and no later than within one month from receiving the request concerning the right of access, provide the data requested by the data subject. If the request is of complex nature or if there are several requests, this time limit may be extended by no more than two months if

necessary. The controller must notify the data subject of the delay and state the reasons for the delay.

If the controller does not take action on the request of the data subject, the controller must inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action.

The data subject has the right to request that the Data Protection Ombudsman reviews the lawfulness of the personal data and the related processing if the data subject's right of access has been postponed, restricted or denied based on the Data Protection Act or some other law. 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 Data Protection Act 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

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 General Data Protection Regulation regarding legality, purpose of use, necessity or accuracy, or the provisions regarding special categories of personal data.

If the controller refuses the data subject's request to have data rectified, completed or erased, 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 review the legality of personal data and its processing if, pursuant to the Act on Data Protection 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 erased, the controller must notify the recipients to which it has disclosed the data in question. The recipients must also rectify or erase the personal data in question that the recipients retain.

8.3 Other rights of the data subject

The data subjects' 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 process personal data in connection with statutory police duties related to the processing of personal data as referred to in the Finnish Immigration Service Personal Data Act or the Act on the Processing of Personal Data by the Police.

Article 18 of the Regulation on the protection of natural persons with regard to the processing of personal data concerning the right of a data subject to the restriction of processing does not apply to the processing of personal data as referred to in the Finnish Immigration Service Personal Data Act or the Act on the Processing of Personal Data by the Police.

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

Generally, data subjects are not charged a fee for the notifications and information sent to a data subject on the basis of the Data Protection Regulation 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 monitoring 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).