Privacy statement; Processing of personal data in relation to other statutory tasks of the police

1 Controller

National Police Board
Postal address: P.O. Box 1000, 02151 Espoo
Street address: Vuorimiehentie 3, Espoo
Telephone: 0295 480 181 (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 personal data in relation to other statutory tasks of the police 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)
- General Data Protection Regulation (EU) 2016/679
- Data Protection Act (1050/2018)

- Police Act (872/2011)
- Firearms Act (1/1998)
- Identity Card Act (663/2016)
- Passport Act (671/2006)
- Money Collection Act (255/2006)
- Lotteries Act (1047/2001)
- Act on Detecting and Preventing Money Laundering and Terrorist Financing (444/2017)
- Private Security Services Act (1085/2015)
- Act on the Marketing and Use of Explosives Precursors (73/2021)
- Lost Property Act (778/1988)
- 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 specified in the Police Personal Data Act in order to carry out tasks related to licence administration and such statutory supervisory duties specifically imposed on the police that are not related to the prevention, uncovering or investigation of crimes, to referring investigated offences to a prosecutor for consideration of charges or to protecting the public safety from threats and the prevention of such threats.

In addition to the basic personal data, the police processes the following personal data:

1) data concerning applications, permits, statements, notifications and decisions
2) data concerning any obstacles to the granting of a permit and permit validity and data required for granting a permit and for clarifying the preconditions for permit validity, including health information and other information included in the special categories of personal data
3) data concerning the actions taken by the authority
4) photos and sample signatures provided to the police, the Ministry for Foreign Affairs or foreign affairs administration authority when a person applies for a permit or a decision the preparation of which requires the photo or sample signature of the person
5) biometric fingerprint data collected from and facial photo taken of the applicant at the time of applying for a passport or identity card in order to carry out the duties laid down in the Identity Card Act and Passport Act

6) information needed to safeguard the safety of a person subjected to a measure or the occupational safety of an official: information concerning a person's health and its monitoring or the treatment of his/her condition, information on the likelihood of danger to the public or unpredictability of the subject or person and information that describes or is intended to describe a criminal act, punishment or other consequence of a crime
7) data concerning any administrative consequences
8) data other than the data specified in sections 1–7 that is necessary in order to carry out other statutory duties of the police, excluding information belonging to the special categories of personal data.

As part of the supervision pursuant to the Lotteries Act and Act on Detecting and Preventing Money Laundering and Terrorist Financing, the police process the personal data of the customers of gambling operators and other entrepreneurs and communities the supervision of which the police is responsible for based on the above-mentioned Acts. Such personal data is processed to the extent necessary in order to carry out the supervisory duties.

Unless otherwise provided elsewhere by law, when deciding on permits and carrying out supervision, the police process personal data, information source data and other personal data intended for the carrying out of other statutory duties of the police, with such information being related to the performing of investigation and supervisory duties, for purposes other than the original purposes of processing when deciding or issuing an opinion on the granting or validity of an authorisation if it has been laid down that a requirement for the granting or validity of the authorisation is the applicant's or holder's reliability, suitability or other such attribute whose assessment requires information on the health, intoxicant use, criminal guilt or violent behaviour of the applicant or holder.

In the above-mentioned situations, in order to evaluate whether the requirements for granting a permit or the requirements related to permit validity are met, the police also uses the notifications provided by the National Bureau of Investigation, which are based on the personal data referred to in section 7, subsection 2 of the Act on the Processing of Personal Data by the Police. Such notifications must include the information that is required in order to evaluate whether the requirements for the granting of a permit or permit validity are met. The National Bureau of Investigation may issue a notification if:

1) based on information intended for the prevention or uncovering of crimes, the applicant or permit holder is in recurring and permanent contact with a person who, according to a court decision, has been deemed to be guilty of participation in the activities of an organised crime group or with a person who, in an ongoing pre-trial investigation or consideration of charges, is suspected of participation in such activities and in case such connections may expose the applicant or permit holder to inappropriate external influencing and, therefore, compromise the protection of the interests that form the basis of the preconditions laid down concerning the granting of permits and permit validity or
2) the National Bureau of Investigation deems, based on information intended for the prevention or uncovering of crimes and based on any other reports, that there are reasonable grounds to suspect that the applicant or permit holder is guilty of participation in the activities of an organised crime group and disclosing the information is necessary in order to protect the interests that form the basis of the preconditions laid down concerning the granting of permits and permit validity from the actions and influence of organised crime groups.

The police process personal data specified in the Police Personal Data Act for purposes other than the original purpose of processing, taking into consideration the legal restrictions for processing personal data, in order to

1) prevent or uncover crimes
2) investigate crimes for which the maximum punishment prescribed by law is imprisonment
3) find wanted persons
4) support a person’s innocence
5) prevent significant risks to life, health or freedom or major damage to the environment or property
6) protect national security
7) establish a person’s identity when undertaking a police measure that necessarily requires verification of identity and
8) direct police operations.

The data referred to above is used as a source of information for basic and extended background checks in the manner and to the extent laid down in the Act on Background Checks.

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.

The police process special categories of personal data in order to carry out other statutory duties of the police only if the processing is necessary for the purpose of processing.

Biometric data processed in order to carry out the duties laid down in the Identity Card Act and Passport Act may be used for purposes other than the original purpose of processing only if it is necessary in order to identify a victim of a natural disaster, major accident, other catastrophe or crime or if the victim has not otherwise been identified. Only persons whose work duties require that they use the data have the right to use the data. Data collected for comparison purposes may only be used for the time required to perform the comparison, after which such data must be immediately erased.

The fingerprint data of a passport applicant may, based on the applicant's consent, be later used for preparing an identity verification document applied for by the applicant in question.

Data included in a firearms notification referred to in section 114 of the Firearms Act may not be used for any other purpose than for processing the firearm permit.

6 Regular disclosure of data

The police disclose personal data related to other statutory duties of the police through a technical interface or as sets of data to the Finnish Security Intelligence Service, Customs, Border Guard, Defence Forces, prosecutors, courts of law, Legal Register Centre, Criminal Sanctions Agency and other competent authorities as specified in the Act on Data Protection in Criminal Matters, for the purpose of performing the statutory duties laid down in section 1 of said Act.

Furthermore, the police disclose personal data related to other statutory duties of the police through a technical interface or as sets of data to other authorities for the performance of duties laid down in the Act applicable to the authority or pursuant to the Police Personal Data Act or some other Act within the scope and under the permit conditions set out in more detail in separate data permits.

In addition, the police disclose personal data related to other statutory duties of the police in relation to an individual matter or as sets of data to competent authorities of other member states of the European Union and the European Economic Area who process personal data in order to prevent, investigate and uncover crimes, take legal action in connection to a crime or enforce criminal sanctions. This includes protection from and prevention of threats to public safety. The party obtaining the data has the right to process personal data on the same conditions that the police is allowed to process the data in question.

The police disclose personal data related to other statutory duties of the police in connection with an individual matter or as sets of data to Eurojust and other institutions established on the basis of the Treaty on the Functioning of the European Union, the duties of which include upholding social order and the judicial system, maintaining public order and security or preventing and solving crimes and considering the filing of charges, for the purpose of performing these duties.

The police disclose personal data related to other statutory duties of the police in connection with an individual matter or as sets of data to competent law-enforcement authorities in member states of the European Union at their request, provided that the data and intelligence information are needed to prevent or investigate crimes. A competent authority is obliged to disclose the above personal data to a competent law-enforcement authority in charge of criminal investigation or security intelligence in another member country unprompted if the disclosure can be assumed to contribute to the prevention or solving of crimes as per section 3, subsection 2 of the Act on Extradition on the Basis of an Offence Between Finland and Other Member States of the European Union (1286/2003).

The police disclose personal data related to other statutory duties of the police in connection with an individual matter or as sets of data to the International Criminal Police Organization (ICPO-Interpol) pursuant to Chapter 7 of the Act on Data Protection in Criminal Matters, for the purpose specified in section 1, subsection 1 of said act.

The police disclose personal data related to other statutory duties of the police in connection with an individual matter or as sets of data pursuant to Chapter 7 of the Act on Data Protection in Criminal Matters:

1) personal data to the competent authorities referred to in international agreements or other arrangements concerning the taking back of illegal

immigrants and people who are illegally resident, for the purposes of the duties specified in the international agreements and arrangements in question

2) personal data related to the acquisition, possession, transfer, import and export of firearms, firearm components, cartridges, and particularly dangerous projectiles to authorities responsible for gun control in other countries, provided that the disclosure of information is necessary for gun control.

Biometric data processed for purposes related to the performing of the duties laid down in the Identity Card Act and Passport Act may only be disclosed for purposes specified in section 15, subsection 2.

7 Erasure and archiving of personal data

Personal data processed in order to perform licence administration and supervisory duties is erased no later than twenty years from the decision or its expiry, the end of the validity period specified in the decision or the creation of the personal data entry.

The following are exceptions to the time limits concerning erasure:

1) data related to firearms notifications specified in the Firearms Act is erased no later than three years from the creation of the data entry
2) personal data processed pursuant to section 42 c of the Firearms Act is erased no later than thirty years from the disposal of the item; data may, however, be processed for purposes laid down concerning other statutory duties of the police for no more than ten years after the item was disposed of
3) data related to lost property operations is erased no later than one year after the creation of the data entry
4) personal data included in notifications concerning suspected violations referred to in Chapter 7, section 9 of the Act on Detecting and Preventing Money Laundering and Terrorist Financing is erased in accordance with subsection 2 of the said section, with other personal data related to supervision referred to in the said Chapter erased no later than five years from the creation of the personal data entry
5) information concerning any administrative consequences is erased no later than five years from the creation of the personal data entry
6) personal data processed for purposes related to supervision specified in the Lotteries Act and Act on Detecting and Preventing Money Laundering and Terrorist Financing and concerning the customers of supervised gambling operators and other entrepreneurs and communities referred to in the said

Acts is erased immediately when it is no longer necessary to retain the data in order to carry out the supervisory duties.

However, personal data processed in order to perform licence administration and supervisory duties and personal data related to firearms notifications is erased no later than one year from the death of the data subject, provided that there are no special grounds for the further retention of the data. The necessity of the further retention of personal data must be evaluated at least every five years.

Information found inaccurate, which has been retained to protect the rights of the data subject, another party or a member of the police personnel, will be erased as soon as its retention is no longer necessary to protect such rights.

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.

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 licence administration and in order to carry out statutory supervisory duties separately laid down for the police in relation to the statutory duties of the police or in order to exercise the official authority of the police.

Article 18 of the Data Protection Regulation, which concerns the data subjects' right to restriction of processing, is not applied to the processing of personal data carried out by the police as referred to in 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).