Privacy statement; Processing of personal data in investigation and supervision duties

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 in matters concerning data protection

National Police Board
Tiina Narkilahti, 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 Legal basis for processing personal data

The police process personal data to perform investigation and supervision duties, to perform their statutory obligations and to exercise their public authority when the conditions laid down in data protection legislation are met. 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:

- The Act on the Processing of Personal Data by the Police (616/2019, hereafter the Police Personal Data Act)
- the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018, hereafter the Act on Data Protection in Criminal Matters)

- the Police Act (872/2011)
- the Police Decree (1080/2013)
- the Pre-trial Investigation Act (805/2011)
- the Coercive Measures Act (806/2011)
- the Decree on Pre-trial Investigation
- the Coercive Measures and Covert Data Acquisition (122/2014) and
- the 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 personal data specified in the Police Personal Data Act in order to carry out pre-trial investigations and police investigations; to solve crimes; and to perform tasks related to the consideration of filing charges, the maintenance of public order and safety or another supervisory task of the police, provided that the data relates to persons who are

1) suspected of an offence or participation in an offence
2) under 15 years of age and suspected of an offence
3) subject to pre-trial investigation, police investigation or a police measure
4) reporters of an offence or injured parties
5) witnesses
6) victims
7) directly related to field duties or supervisory duties specifically provided for in legislation or
8) providers of other further information related to a duty.

In addition to basic information on the above-mentioned persons, the police also process the following personal data:

1) details, descriptions and categorisations related to the police duty, measure or incident
2) identifying information to establish a person’s identity, including fingerprints, handprints and footprints; handwriting, voice and scent samples; DNA identifiers; and facial images and other biometric data; information on close relatives may be processed to find persons reported missing or identify unidentified deceased persons only with the consent of the person in question
3) information needed to safeguard the safety of a person subjected to a measure or the occupational safety of an official, information necessary for the person’s health and its monitoring or the treatment of their 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 the criminal act, punishment or other consequence of a crime (*safety data*) and

4) identification information of a decision of a judge or court and information on whether a person has been convicted, their charges or punishment waived, or their charges dismissed, left uninvestigated or set aside; and information on the finality of the decision.

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) solve 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 above data is used as a source of information for basic and extended background checks in the manner and to the extent determined 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 information in special categories of personal data in order to perform investigation and supervision duties only if such processing is essential for the purpose of processing.

6 Regular disclosure of data

The police disclose personal data related to investigation and supervision tasks 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.

The police disclose personal data related to investigation and supervision tasks in connection to an individual matter or as a set of data also to competent authorities of member states of the European Union and the European Economic Area that process personal data in order to prevent, investigate or uncover crimes, take legal action in connection to a crime or enforce criminal sanctions. This includes protection from and prevention of threats to general 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 investigation and supervision tasks in connection to an individual matter or as a set 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 investigation and supervision tasks in connection to an individual matter or as a set 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 solve 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(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 investigation and supervision duties to the European Union Agency for Law Enforcement Cooperation (Europol) in compliance with the Europol Regulation (EU) 2016/794 and the Act on the European Union Agency for Law Enforcement Cooperation (214/2017).

The police disclose personal data related to investigation and supervision duties on the basis of the Prüm Convention (54/2007) and the Prüm Decision (2008/615/JHA) to the member states party to the convention and to the extent specified in the Prüm Convention and Prüm Decision, especially to prevent terrorism and cross-border crime.

The police disclose personal data related to investigation and supervision duties in connection to an individual matter or as a set of data to the International Criminal Police Organization (ICPO-Interpol) on the basis of chapter 7 of the Act on Data Protection in Criminal Matters, for the purpose specified in section 1(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 Deletion and archiving of personal data

Information related to a criminal case that has been referred to a prosecutor for a decision will be deleted

1) five years after the criminal case was referred to the prosecutor if the punishment for the grossest suspected offence in the case is a fine or up to one year of imprisonment

2) ten years after the criminal case was referred to the prosecutor if the punishment for the grossest suspected offence in the case is from over more than one year to up to five years of imprisonment and
3) twenty years after the criminal case was referred to the prosecutor if the punishment for the grossest suspected offence in the case is more than five years of imprisonment.

However, the above data is not deleted earlier than one year after the period of limitation on the right to bring charges expires.

Information on criminal cases that were not referred to a prosecutor for decision will be deleted one year from the expiration of the period of limitation on the right to bring charges for the latest suspected crime, but no earlier than five years after the recording of the criminal case.

Information about distinctive identifiers used to verify identity will be deleted no later than ten years after the last entry regarding the person suspected of a crime was made. However, information will be deleted no later than ten years after the death of the data subject if the maximum punishment for the grossest offence used as basis for registration is no less than one year of imprisonment.

Identification information of persons who were under 15 years of age at the time of the offence will be deleted no later than one year after the last entry regarding the person suspected of a crime was made, unless one of the entries is related to a crime that is only punishable by imprisonment.

Information about distinctive identifiers used to verify identity, as well as information about distinctive identifiers of persons who were under 15 years of age at the time of the offence, will be deleted no later than one year after the entry was made, if investigation proves that no offence was committed or that there is no longer reason to suspect the person of the crime.

The above-mentioned personal data related to a criminal case may be retained for a longer period if it is needed for investigation or supervision purposes or other justified purposes or to safeguard the rights of the data subject, another party or a member of the police personnel. The necessity of the further retention of personal data must be evaluated at intervals of five years or less.

Other personal data processed during investigation and supervision duties will be deleted five years after the report or case was recorded, unless they are related

to a criminal case that is still being investigated. As an exception to the deletion principles for investigation and supervision duties

1) information related to the prohibition to pursue business will be deleted five years after the expiration of the prohibition period
2) information regarding a restraining order, visitation ban or protection measure as specified in the legislation regarding the application of the regulation of the European Parliament and Council on mutual recognition of protection measures in civil matters will be deleted five years from the date on the restraining order, visitation ban or protection measure
3) information regarding supervised probationary freedom or a monitoring sentence will be deleted five years after the supervised probationary freedom or monitoring sentence came to an end
4) other information related to warrants of apprehension, travel bans, prohibitions on keeping animals, hunting bans, prohibition of entry restricted to Finland, community sanctions or probationary freedom that is processed in order to reach, monitor, observe or protect persons will be deleted five years after the annulment or expiration of the warrant, ban or prohibition
5) personal data processed in order to find missing persons or identify unidentified deceased persons will be deleted no earlier than five years after the missing person was found or the deceased person identified; however, information on close relatives required in finding people reported missing and identifying unidentified deceased persons will be deleted at the data subject's request or as soon as the information is no longer needed for its processing purpose and
6) information on personal identifiers and travel document information processed in order to perform tasks specified in section 131 of the Aliens Act will be deleted ten years after the last entry regarding the data subject was made; if the data subject is granted Finnish citizenship, the information will be deleted one year after the controller received information about the granting of citizenship.

Information on personal identifiers and travel document information processed in order to perform tasks specified in section 131 of the Aliens Act, as well as the safety data of persons subject to measures related to investigation and supervision duties, will be deleted no later than one year after the death of the data subject.

However, the above-mentioned personal data may be retained for a longer period if it is needed for investigation or supervision purposes or other justified purposes or to safeguard the rights of the data subject, another party or a member of the police personnel. The necessity of the further retention of personal data must be evaluated at least every five years.

Information obtained in connection with the performance of police duties will be deleted without delay after it has been confirmed that the information is not needed to perform tasks related to preventing or uncovering crimes, to prevent or uncover crimes, to solve a crime for which the maximum punishment prescribed by law is imprisonment, to find a wanted person, to support someone's innocence, to prevent significant risks to life, health or freedom or major damage to the environment or property, to protect national security, to determine identity during a police operation that necessarily requires the verification of identity, or to direct police operations.

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 deleted as soon as its retention is no longer necessary to protect such rights.

8 Rights of the data subject

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.

Data subjects themselves do not have the right to access information source data, data in the National Schengen Information System pertaining to discreet checks or specific checks, information on the tactical and technical methods of the police included in the personal data referred to in sections 5–8 of the Act on the Processing of Personal Data by the Police, observation or information source data or data used in forensic investigations, or personal data obtained using methods referred to in chapter 5 of the Police Act and chapter 10 of the Coercive Measures Act and pursuant to section 157 of the Information Society Code.

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 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:

6) the latest technology
7) the implementation costs of the measures
8) the nature, extent, context and purposes of processing and
9) 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 privacy statements

The privacy statements of the police are publicly available in electronic format on the national police information network (www.poliisi.fi/en) 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).