

Privacy statement; Processing of personal data of covert human intelligence sources

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
Jaana Riikonen, 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 the processing of personal data

The police process personal data of covert human intelligence sources 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 Criminal Investigation Act (805/2011)
- the Coercive Measures Act (806/2011)
- the Decree on Pre-trial Investigation, Coercive Measures and Covert Data Acquisition (122/2014).

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

In addition to the basic personal data, the police process the following personal data concerning the covert human intelligence sources referred to in chapter 5, section 40 of the Police Act or in chapter 10, section 39 of the Coercive Measures Act:

- 1) information on the use and surveillance of covert human intelligence sources;
- 2) main contents of the information provided by a covert human intelligence source:

- 1) who, on reasonable grounds, are believed to have committed or about to commit a criminal offence for which the maximum punishment prescribed by law is imprisonment;
- 2) who are in contact with the person referred to in paragraph 1 or are met in the company of this person, and their contact or presence can be assumed to be connected to the offence due to its repetitive nature, the circumstances or the person's behaviour;
- 3) who are the target of observation pursuant to the Police Act or subject to some other police measure.

The police also process the data referred to above on the following persons, if necessary for use of covert human intelligence sources:

- 1) witnesses to an offence;
- 2) victims of crime;
- 3) reporters of an offence or injured parties.

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) information on a person's connections, lifestyle, financial situation, hobbies and other interests;
- 3) identifying information to establish a person's identity, including voice samples, facial images and other biometric data;
- 4) 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).

The police process information in special categories of personal data only if such processing is essential for the purpose of processing.

6 Regular disclosure of data

The police disclose personal data concerning the covert human intelligence sources to the Finnish Security Intelligence Service for the purpose of performing the statutory duties laid down in section 1 of the Act on Data Protection in Criminal Matters.

7 Deletion and archiving of personal data

Data concerning covert human intelligence sources are erased no later than ten years after the last entry.

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 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:

- 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 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).