Privacy statement; The records management, decision-making and archiving system of the police used in administrative case management

POL-2020-42051, ID-20369528, 28.10.2020

1 Controller

National Police Board
Postal address: P.O. Box 22, FI-00521 Helsinki, Finland
Street address: Asemapäällikönkatu 14, Helsinki, Finland
Telephone: +358 (0)29 548 0181 (exchange)
Email: kirjaamo.poliisihallitus@poliisi.fi

2 Contact person for enquiries concerning data protection

National Police Board
Emmi Savonen, Information Management Specialist
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 order to comply with the statutory obligations 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 provision.

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

- Act on the Openness of Government Activities (621/1999)
- Act on Information Management in Public Administration (906/2019)
- General Data Protection Regulation (EU) 2016/679,
- Data Protection Act (1050/2018)

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

The records management, decision-making and archiving system of the police used in administrative case management is an information system for the management and preparation of administrative matters, documents and tasks included in police operations, and for the related decision-making and archiving. The system is used by the National Police Board, the national Bureau of Investigation, the Police University College and police departments.

According to Section 18(1)(1) of the Act on the Openness of Government Activities (621/1999), the authorities must maintain an index of any matters submitted and taken up for consideration and any matters considered and decided, or otherwise ensure that their public documents can easily be located. The obligations stated in data protection legislation apply to an authority's case management record insofar as the entries made concern natural persons (e.g. in the capacity of the initiator). Personal data entered into the records for case management purposes are used to identify the clients, the matters being handled, and the documents.

In so far as the data requested by the data subject do not fall under the scope of the right of access stated in data protection legislation, the data subject also has the right to request documents on the basis of the Act on the Openness of Government Activities. According to Sections 14 and 15 of the Act on the Openness of Government Activities, decisions regarding right of access to documents are made primarily by the authority that is processing, or has processed the matter. The right of access to a document is governed in Chapter 3 of the Act on the Openness of Government Activities, and parties' right of access, among others, in Chapter 3 Section 11.

The police data management policy specifies the objectives, principles, responsibilities and methods of implementation within the police forces. The administrative case management of the police and the use of the system supporting it is steered by the guideline given in the records management, decision-making and archiving system of the police used in administrative case management.

6 Regular disclosure of data

No regular disclosure of data.

The provisions of the Act on the Openness of Government Activities are applied to the disclosure of personal data from the records management, decision-making and archiving system.

7 Erasure and archiving of personal data

Information is continuously updated on the basis of documents falling within the scope of administrative case management by the police and recorded as received and prepared.

Police matters in administrative case management and their data content are retained during their entire life cycle, as specified in the information management plan for administrative case management.

Some of the information must be permanently retained in accordance with the decisions of the National Archives of Finland, while some must be retained for a period specified by the National Police Board. The information management plan specifies the retention periods for each case category and document type.

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 website. The site offers detailed information on matters such as how data subjects can check their personal data; when the right to check the information can be restricted; how and on what grounds the information can be rectified or erased; 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 their data, the data subject must make a sufficiently specific request: it must indicate which purpose for processing, data system, personal data file or part of a personal data file it refers to. An insufficiently specific request shall not be realised. The data subject may bring along an assistant.

When wishing to exercise the right to check their data, the data subject must provide reliable proof of identity. In case the controller is unable to confirm the data subject's identity, the controller may ask the data subject to provide further information required to confirm the data subject's identity. The right to obtaining a copy of the information shall not have a harmful effect on the rights and freedoms of others.

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 to the Data Protection Ombudsman, controller (National Police Board) or police department.

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 and restriction of the 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 General Data Protection Regulation 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 may present the request to rectify or erase personal data or restrict its processing to the controller or another police unit. The request must be sufficiently specific: it must indicate whose personal data it refers to; to which personal data held by the police the request to rectify or erase data or restrict processing refers; why the data subject considers the data to be incomplete, inaccurate or incorrect in terms of the purpose of processing; which changes the data subject request to be made to the data in question and why the processing of the personal data should be restricted. The controller has the right to request additional information in order to verify identity.

If the controller refuses the data subject's request to have the personal data rectified, completed or erased, the controller must inform the data subject of this refusal and its grounds in writing.

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 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 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 subject's right to object to the processing of data and the right to have the data transmitted from one system to another do not apply when the police process personal data in connection with statutory police duties.

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 implementation 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 records

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).