Validity
1 February 2023 - 31 January 2028

Legal basis
Section 4, Police Administration Act (110/1992)

Amends/repeals
2020/2012/66, 23.1.2012 Implementation of data subjects' rights in the police: Right of access, correction of data and informing

Target groups
The police

Rights of data subjects and data protection at the police

Contents

NATIONAL POLICE BOARD
Vuorimiehentie 3, P.O. Box 1000, FI-02151 ESPOO, Finland
kirjaamo.poliisihallitus@poliisi.fi
Tel. +358 295 480 181, Fax +358 295 411 780

1 Purpose and scope of application

Processing of personal data is a key element in police operations and the duties of almost all officials working in the police administration involve processing of personal data. Systematic and careful processing of personal data ensures the responsible and efficient processing of information needed in police operations, and at the same time, attainment of the objectives set for the police, and the quality of police operations, can be promoted.

The controller is obliged to ensure that data subjects' privacy protection is ensured responsibly and transparently at all stages of the lifecycle of personal data processing.

The purpose of these instructions is to describe the entity and principles of personal data processing in the police and how the police comply with the principles and obligations related to data protection, regarding the implementation of data subjects' rights, and to serve as an operational guideline for police personnel relating to the exercise of data subjects' rights, and as an informative document for data subjects.

These instructions supplement the National Police Board's instruction issued on information management in the police[1].

2 Intention of data protection at the police

In police operations, it is ensured that information necessary in the operations is produced, managed and kept up-to-date based on uniform procedures and principles, ensuring privacy protection. In addition, secure and efficient information flow and information management, both internally and externally, are ensured.

The information management policy of the police is the highest standard steering information security, data protection and information lifecycle management of the police, that is, information management of the police as a whole. The information management policy defines the objectives for information management in the police and specifies the key procedures and implementation methods as well as the responsibilities and roles for the attainment of these objectives.

Personal data is collected in the police for specific, explicit and lawful purposes and this data shall not be processed in ways non-compatible with these purposes. Personal data is processed for the purpose of performing the official, statutory duties of the police and for exercising police powers for the purposes and to the extent specified by law. The police ensure that the personal data processed are adequate, relevant and limited to what is necessary for the lawful purposes for which the data are processed. The

[1]Information management policy of the police (POL-2022-59874, 25 October 2022)

processing of personal data is carefully planned, and the appropriate instructions and training are provided.

Personal data processed in police duties are accurate and up-to-date. The police implement all necessary measures to ensure that personal data that are inaccurate with regard to the purposes for which they are processed, are erased or rectified without delay. Personal data are kept in a form which permits identification of data subjects only for as long as necessary for the purposes for which the personal data are processed. The information systems and procedures of the police are implemented in compliance with the principle of data protection by design and by default.

The police facilitate implementation of the statutory rights of data subjects. Comprehensive information is provided about police data filing systems, personal data processed by the police for various purposes, and the rights of data subjects. Data subjects are provided with the possibility to exercise their right of access and demand that the data be rectified, erased and processing restricted as provided by law. At the same time, implementation of data subjects' other rights is ensured.

3 Legal basis for personal data processing

According to the Constitution of Finland (731/1999), the exercise of public powers shall be based on an Act. In all public activity, the law shall be strictly observed. In police operations, legislation guides all processing of personal data.

From the viewpoint of personal data processing, the key act for the police is the Act on the Processing of Personal Data by the Police (616/2019, Police Personal Data Act) that includes provisions supplementing general legislation that are applied to the processing of personal data necessary for performing the police duties referred to in Chapter 1, section 1 of the Police Act (872/2011). The entry into force of the General Data Protection Regulation of the EU (EU 2016/679, General Data Protection Regulation) and the Data Protection Act (1050/2018) supplementing and specifying it, and the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018, Criminal Matters Personal Data Act) has differentiated the legislative basis so that it is no longer possible to apply the same regulations to all processing of personal data.

The Criminal Matters Personal Data Act is applied to personal data processing by the police in the context of preventing, detecting or investigating criminal offences or referring them for consideration of charges, or safeguarding against, and preventing threats to, public security in connection with preventing, detecting or investigating criminal offences or referring them for consideration of charges.

The Criminal Matters Personal Data Act is also applied to police operations that concern disturbances in which it is not known in advance whether they

constitute an offence. Such operations include also the exercise of police powers provided for in the Police Act or other legislation for example in connection with demonstrations, large sports events and riots. Such operations also include maintaining law and order that the police authorities or other law enforcement authorities are tasked with when it is necessary for safeguarding against, and preventing threats to, public security and basic interests of society safeguarded by law, which may result in a criminal offence.

The Criminal Matters Personal Data Act applies to personal data processing by the police:

- For the purposes of conducting a criminal investigation, police investigation or performing other duties related to the referral of cases for consideration of charges, and performing duties related to maintaining public order and security or performing other police surveillance duties provided by law (including monitoring of permits and licenses in connection with field duties of the police),
- For the purpose of performing duties related to the prevention and detection of criminal offenses,
- For the purpose of quality assurance of DNA samples,
- Regarding information of covert human intelligence sources when targeted at purposes provided for investigation and supervisory duties or for prevention and detection of criminal offences, and
- When data is processed for the purpose of duties referred to in Chapter 1, section 1, subsection 1 of the Police Act, related to protecting national security.

The General Data Protection Regulation and the supplementing Data Protection Act apply to processing of personal data:

- In duties related to licensing functions
- In the context of performing such police surveillance duties separately provided by law that are not related to the prevention, detection or investigation of offences, referring them for consideration of charges, or safeguarding against threats to public security or preventing such threats (in particular, monitoring of permits and licenses not in connection with field duties of the police)
- Regarding information of covert human intelligence sources when targeted at purposes provided for in other statutory duties of the police,
- In the context of other duties pursuant to Chapter 1, section 1, subsection 2 of the Police Act that do not relate to preventing, detecting or investigating criminal offences or referring them for consideration of charges, or safeguarding against, and preventing threats to, public security, and in human resource, financial, facility and materials administration.

The Act on the Openness of Government Activities (621/1999, Act on Openness) applies to the right to access personal data and to other

disclosure of personal data from a personal data filing system controlled by an authority. In addition to general legislation governing data protection, the Act on Information Management in Public Administration (906/2019, Information Management Act), materially influences processing of personal data by the police.

Provisions that apply to personal data processing related to police duties are included in the Criminal Investigation Act (805/2011), the Coercive Measures Act (806/2011), the Act on Preventing Money Laundering and Terrorist Financing (444/2017), the Act on the Financial Intelligence Unit (445/2017), the Act on witness protection programme (88/2015), the Act on Emergency Response Centre Operations (692/2010), the Act on the Establishment of Cause of Death (459/1973), the Act on the Processing of Personal Data in the Field of Immigration Administration (615/2020) and the Act on the Use of Airline Passenger Name Record Data for the Prevention of Terrorist Offences and Serious Crime (657/2019).

Provisions on police powers concerning obtaining of information are laid down in the same regulations that regulate other police powers. The provisions of general data protection legislation and Police Personal Data Act are complied with in the processing of personal data obtained under police powers, unless stricter preconditions or requirements regarding personal data processing are included in the regulations on police powers or other specific legislation.

4 Key concepts relating to the rights of data subjects

Personal data means any information relating to an identified or identifiable natural person (data subject), directly or indirectly. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question, or from another procedure.

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person.

Data concerning health means personal data related to the physical or mental health of a natural person, which reveal information about his or her health status.

Personal data processing means any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data or which is legally responsible for the filing system in question.

Personal data breach means a breach of information security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

5 Roles and responsibilities in matters related to rights of data subjects

5.1 Roles and responsibilities in other documents

Upper level roles and responsibilities related to data protection, information security and information lifecycle management in the police are described in the information management policy of the police. More precise roles and responsibilities related to the implementation of the rights of data subjects in the police are defined in this document.

5.2 National Police Board

The National Police Board is responsible for ensuring that the responsibilities, obligations, processes and procedures related to matters concerning the rights of data subjects are defined in the police. Moreover, the National Police Board is responsible for ensuring that up-to-date national instructions with appropriate contents have been issued on the implementation of the rights of data subjects in the police, data subjects have available comprehensive and up-to-date general information material on nationwide personal data processing in the police, the personnel has been provided with training as required by their tasks, and that adequate operational preconditions are in place for tasks related to the rights of data subjects.

5.3 Police units

Police units are responsible for ensuring the availability of sufficient resources, competence and guidance in the unit for tasks related to the implementation of the rights of data subjects and that the tasks are

organized, managed, supervised and the related responsibilities are allocated in accordance with data protection legislation and instructions issued by the National Police Board.

Police departments act as the other police units referred to in section 41, subsection 2 of the Police Personal Data Act, who, in addition to the controller, receive requests regarding the exercise of data subjects' right of access, and who provide the necessary personal data and other data for checking as instructed in these instructions, and otherwise implement tasks related to the rights of data subjects as defined in these instructions.

Police units shall appoint a right of access contact person for tasks related to the implementation of the rights of data subjects and assign a sufficient number of other personnel and a sufficient number of backup persons for them for the tasks related to the implementation of the rights of data subjects. The tasks in line with their roles must be recorded in the job descriptions of persons working in data protection tasks and the police unit shall facilitate the successful management of such duties. The police unit shall ensure that the right of access contact person has sufficient knowledge of legislation that applies to the processing of personal data and data protection practices, and the capabilities for managing the tasks under the contact person's responsibility.

The police unit shall ensure that the police unit's internal processes and procedures related to exercising the right of access are appropriately and comprehensively implemented in the police unit's area of operation so that it is possible for data subjects to make requests to several customer service points of the police as appropriate.

Police units shall also ensure that comprehensive information material[2] with up-to-date contents and contact details of the unit's right of access contact person are available for data subjects, in paper document format, at all customer service points of the police. Police units shall also monitor and supervise that instructions and legislation in force are complied with in tasks related to the rights of data subjects.

5.4 Right of access contact person

The right of access contact person is tasked with providing guidance and advice to data subjects in data protection matters and take care of the practical measures and tasks related to the implementation of the right of access in the unit, in line with their job description. The right of access contact person's duties also include supporting the head of the unit and the person in charge of data protection appointed by the unit, and collaborate with the National Police Board in matters related to the rights of data subjects.

[2] The contents and subject matter correspond to the Police personal data filing systems folder, previously ordered to be made available.

6 Rights of the data subject

Provisions on the rights of the data subject applicable to police operations are mainly included in Chapter 4 of the Criminal Matters Personal Data Act, and Article 3 of the General Data Protection Regulation. The Data Protection Act and Police Personal Data Act also include provisions on the rights of the data subject and restrictions thereto. In addition to the aforementioned, provisions on the rights of the data subjects are also included in other EU regulations steering the processing of personal data in the police and national special legislation, such as the legal basis for the Schengen Information System and the Europol regulation.

In many cases, the information content of subject matters and the related information material processed in connection with police duties is such that information related to many other persons can be processed in the same context. Therefore, particular attention must be paid to appropriately securing other persons' data protection rights in connection with the implementation of the rights of the data subject.

The controller shall facilitate the exercise of data subject rights. In the police, tasks and obligations related to data subjects' rights are implemented based on the procedures and principles defined in these instructions.

6.1 Informing of the data subject

High-quality, transparent information about personal data processing builds trust in police operations and provides data subjects with the possibility to exercise their statutory rights.

In the online service of the police, information about data protection is centralized at https://poliisi.fi. In the section of the website on data protection, 'Processing of personal data by the police', in addition to general information material on data protection, public privacy statements and records of processing activities and forms for exercising the right of access and for demanding deletion or rectification of data or restricting data processing are placed available for all.

The controller shall also maintain a record in writing of personal data processing activities under its responsibility. That record shall contain the information specified in detail by law. The record of processing activities is primarily intended for the organization's internal use only, and it will be made available to the supervisory authority on request separately to supervise compliance with data protection legislation. For the purpose of informing the data subject, the record of processing activities can also be prepared by the police as a partly or fully public document, if this is appropriate and there is no need to include confidential data in the public part of the record.

The police carry out informing as necessary, including in customer service situations, in the forms and documents used in connection with customer service and, when possible, when performing field work duties. Information about camera surveillance in properties and technical supervision by the police in field work is provided on information signs or by sufficient informing otherwise decided on in advance.

Data subjects are primarily informed using the following information methods:

Intention, responsibility/reliability

- The information management policy and other public instructions and orders of the police administration related to information security and data protection

Information documents and methods

- Privacy statements and records of processing activities (public parts)
- Information on privacy policies and data protection in the police online service
- Information material in paper document format at customer service points of the police
- Informing in electronic services and in connection with customer service
- Responding to queries by citizens regarding data protection
- Information included in decisions and notifications of the police
- Through the Police's Data Protection Officer, police unit's person in charge of data protection and right of access contact person

6.2 Right of access of the data subject

6.2.1 General information

Provisions on right of access are laid down in section 23 of the Criminal Matters Personal Data Act and provisions on the right of access by the data subject (data subject's right of access) are laid down in Article 15 of the General Data Protection Regulation.

Right of access by the data subject is key with regard to the implementation of data subjects' rights. The data subjects' basic right of access to their personal data facilitates, among others, that the data subjects can be aware of, and verify, the lawfulness of the processing of their personal data and enable the data subjects to decide whether their personal data are correct and up-to-date.

6.2.2 The principles and scope of exercising the right of access

In the Police Personal Data Act, provisions on the national information systems of the police and other personal data filing systems of the police have nowadays been replaced with provisions on the purposes of use of personal data necessary for the police for performing their statutory duties

and information contents of the personal data processed (purpose-based regulation).

In the Act, filing systems refer particularly to a logical, not physical filing systems. The concept of a logical filing system means that all information used for the same purpose are considered to belong to the same filing system, regardless of how and where the information is stored and that short-term files and various generations of records generated in information processing are not considered to be different filing systems when they are held by the controller and used for the purposes of use specified for the filing system.

The starting point is that the data subjects have the right to obtain information from the controller as to whether their personal data is processed. If the data is processed, the controller must submit to the data subject a copy of the personal data processed or provide access to the data in another separately agreed manner. Based on the right of access, the data subject also has the right to know whether the controller does not process information concerning the data subject.

The right of access cannot be exercised through another person but the person exercising the right of access can be accompanied by an assistant. Basically, custodians have right of access to information concerning the child in their custody. The right to exercise the right of access may also be based on an order issued by a court of law, as for example guardians have right of access to the personal data of their principal on their behalf, if the right related to the right of access is included in the order issued to the guardian.

According to the Administrative Procedure Act (434/2003), a minor aged fifteen years or more and the person who has custody of him or her, or his or her other legal representative, both severally have the right to be heard in a matter concerning the minor’s person or personal interests or rights. Therefore, a child aged 15 years or more has an independent right of access to his or her personal data. A child under the age of 15 years also has right of access to his or her personal data if the child understands what this means, in view of his or her age, development level and quality of the matter. Assessment of the right of self-determination of a child under the age of 15 years, and the aforementioned criteria, is conducted on a case by case basis.

Provisions on the erasure and archiving of personal data processed in connection with duties related to the scope of application of the Police Personal Data Act are laid down in Chapter 5 of the Police Personal Data Act.

Data subjects do not have the right of access to their personal data as defined in these instructions when the purpose of the personal data is only in accordance with section 7 of the Archives Act (831/1994) (for example the archive index of investigation and executive assistance).

6.2.3 Deadlines and principles related to the processing of a right of access matter

The deadline related to the processing of a right of access matter depends on the legislation to the scope of which the personal data processing falls, at which the request to exercise the right of access is targeted. However, the basic principle is that personal data requested by data subjects are always provided for checking without delay, regardless of deadlines.

Personal data falling within the scope of the General Data Protection Regulation must basically be provided for checking within one month of the request being submitted. If necessary, the deadline may be extended by two months at most, considering the complexity and number of requests. In this case, the controller must inform the data subject of the extension of deadline within one month of receiving the request, and give the reasons for the delay.

Personal data falling within the scope of the Criminal Matters Personal Data Act must be provided for checking no later than within three months of the request being submitted. According to the Criminal Matters Personal Data Act, the controller is also considered to have refused the right of access if the controller, within three months after the making of the request, has not replied to the data subject in writing.

Notwithstanding the above, personal data saved in the National Schengen Information System must, in accordance with the legal basis in force for the Schengen Information System, must be provided for checking no later than within two months of the request being submitted. After the reforming legal basis has entered into force, the deadline will be shortened to one month.

In many cases, the police receive requests to exercise the right of access which are targeted at the same time at, for example, personal data falling within the scope of both the General Data Protection Regulation and Criminal Matters Personal Data Act. In such cases, it may be appropriate to provide right of access to personal data several times in order to be able to follow the deadlines provided in legislation. In this case, it is recommended that the data subject be informed of why they initially only have right of access to a part of their personal data.

6.2.4 Submitting and receiving a request to exercise the right of access

The method of submitting and receiving a request to exercise the right of access depends on the legislation to the scope of which the personal data processing falls, at which the request to exercise the right of access is targeted.

According to the Police Personal Data Act, the data subject shall, when exercising his or her right of access, make a request to this effect in person at a police department customer service point or on the controller’s premises and prove his or her identity, if the request is targeted at personal data falling within the scope of the Police Personal Data Act. The

procedure laid down in the Police Personal Data Act also applies to personal data processing falling within the scope of another Act, if separately stipulated in the Act on the matter. Within the police, the National Bureau of Investigation and the Police University College do not accept requests to exercise the right of access, with the exception of personal data for which the police unit itself bears controller's responsibility.

Basically, the Police Personal Data Act also allows the request to be submitted by using the strong electronic identification referred to in the Act on Strong Electronic Identification and Electronic Trust Services (617/2009). However, such a service has not yet been introduced in the police, and therefore requests to exercise the right of access cannot, for the time being, be submitted or received using electronic services.

The Police Personal Data Act applies to processing of personal data for example in investigations and surveillance duties, for the purpose of preventing and detecting offences, in connection with international police cooperation and in other statutory duties of the police, unless otherwise provided on the matter. Other statutory duties of the police falling within the scope of the Police Personal Data Act include duties related to license administration services or such police surveillance duties separately provided by law that are not related to the prevention, detection or investigation of offences, referring them for consideration of charges, or safeguarding against threats to public security or preventing such threats.

Requests to exercise the right of access to personal data not falling within the scope of the Police Personal Data Act can be submitted to the controller in a personally signed document or corresponding verified manner, or in person at the controller's premises, unless otherwise provided by law.

Specific forms have been designed to facilitate the exercise of the right of access, among which the appropriate document according to the content of the request shall be selected for the right of access matter. The request may also be submitted in another document. The person receiving the right of access form or corresponding document in the police unit shall verify the identity of the person submitting the request, and record this as necessary in the document. The person receiving the request shall also ensure that the personal data and contact details recorded in the right of access document, and other entries, are recorded in the document to a sufficient extent, and clearly.

The right of access forms placed available for all on the police website (https://poliisi.fi) are as follows:

- Use of right of access
- Verification request to the Data Protection Ombudsman
- Exercising right of access to the European Union Agency for Law Enforcement Cooperation (Europol)

The request for right of access must be sufficiently specific so that it indicates, with sufficient precision, which police filing system or part of it, or purpose of personal data processing, it refers to. Sufficient specification of the request with regard to police data is essential because the police process significant amounts of data on data subjects for various purposes in a number of different filing systems, where the set of data may be centralized, decentralized or dispersed on a functional or geographical basis.

If the document containing the request for right of access submitted to the police is deficient or unclear in content, the party responsible for handling the request must urge the data subject to complete the document by a certain deadline, unless this is apparently unnecessary for the purpose of resolving the matter. In this case, the data subject must also be informed of how the request must be completed or specified. From the viewpoint of the purpose of processing, the request is deficient for example if it is targeted at all police data and information systems, and not individualized.

If the right of access targets audio and video recordings collected by means of technical devices, the data subject shall, in order to facilitate retrieval of the data, specify the case or purpose for which the audio and video recording data has been collected, and according to the situation, also the scene of the incident and, as precisely as possible, the time when the recording has been made for example using a camera surveillance system. In some cases, the person submitting the request may need to enclose their picture with the request for right of access for the purpose of retrieving the data.

In the police, a request for exercising the right of access submitted in person by the data subject is received by such customer service points of the police unit where the customer service point has been ordered to receive requests for right of access. In the customer service situation, the data subject shall be assisted in submitting the request, insofar as possible, and also in filling in the documents, should the situation so require. A copy of the request document for exercising the right of access will be given to the data subject in connection with the customer service situation, after the reception markings have been recorded on the request.

The documents related to the case of right of access, and other information related to the case, shall be submitted without undue delay to persons handling right of access matters in the police unit, in line with the internal process and procedural guidelines defined by the police unit.

The request documents shall be stored in the police’s administrative case management, decision-making and archiving system (Acta) for further processing of the matter, as separately instructed.

6.2.5 Processing of the right of access matter and tasks in the police unit

The right of access matter is processed and handled primarily by the police unit to which the request has been submitted, unless otherwise ordered, instructed or agreed on the matter. If the processing of the request in question does not fall within the scope of the powers or duties of the police unit, the police unit must transfer the processing of the matter as necessary, without delay, to a public authority or party considered competent in the case. The data subject must always be informed about the transfer of the processing of the case.

Police departments, as other police units referred to in section 41, subsection 2 of the Police Personal Data Act, process and implement the right of access, basically for personal data collected for the following purposes of processing:

- Personal data processing in investigation and supervision operations
- Personal data processing in prevention or detection of criminal offences
- Personal data processing in police assignments related to emergency calls (police data in the Emergency Response Centre information system)
- Personal data processing in police assignments for which the police are responsible pursuant to immigration legislation (police data in the case management system of immigration matters)
- Personal data processing in other statutory duties of the police
- Personal data processing in the National Schengen Information System
- Personal data filing systems for which the police unit itself bear controller’s responsibility, and the related personal data processing
- Record data stored in the police’s administrative case management, decision-making and archiving system (Acta)

The filing systems and datasets under the responsibility of police departments to implement the right of access are specified in more detail in Appendix 1.

The National Police Board processes right of access matters related to filing systems and datasets that include personal data, others than those mentioned in the Appendix, for which the National Police Board serves as the controller. The police unit having received a request shall, without delay, transfer the right of access matter in this respect for processing by the National Police Board. If the situation is open to interpretation or otherwise unclear, procedures shall be agreed with the National Police Board’s information management before transferring the matter.

In the processing of the right of access matter, it must be taken into consideration that information systems in joint use may contain logically separated data for which several public authorities bear controller’s responsibility. For example, data for which Finnish Customs and Finnish Border Guard bear controller’s responsibility, are processed in the Data System for Police Matters (PATJA). The police only service requests

related to exercising the right of access for data for which the police bear controller's responsibility. In connection with a right of access matter processed by the police for a data subject, there is no right to reveal the existence of other data related to the data subject, for which other controllers bear controller's responsibility.

The police unit having received the request shall primarily also perform the checks of filing systems required by the request and print out or extract in another manner from the information systems the data needed for implementing the right of access and other processing. Regarding certain information systems and datasets, procedural instructions differing from the aforementioned have been issued, and they are included in detail in Appendix 2.

More detailed procedural instructions related to the Data System for Police Matters (PATJA) will be described separately in the Data System for Police Matters (PATJA) right of access manual to be prepared.

Before data is handed out for checking, personal data related to other persons (outsiders) must be carefully removed from the material so that no external party can convert the data to make it identifiable again (anonymization). However, personal data of public authorities having participated in statutory duties related to the report or case shall not, in principle, be removed from the material unless there is a specific need to restrict access to data in this respect on the basis of reasons based on the law.

Correspondingly, data that do not fall within the scope of the right of access, or the disclosure of which to outsiders is prohibited for another reason, shall be removed from the material. If it is necessary to restrict the right of access to only a part of the data, the information requiring restriction shall be removed from the dataset as described above and the remaining information handed out for checking.

According to the Criminal Investigation Act, information on audio and video recordings may be provided only by allowing the recording to be examined at the criminal investigation authority, if in view of the contents of the recording, there is reason to assume that providing the information in another manner may lead to a violation of the protection of the privacy of an individual depicted in the recording. With regard to emergency call recordings saved in the Emergency Response Centre information system, the procedure for providing information is described in the Instruction for the processing of police assignments in emergency and field operations[3]. Right of access to audio recordings is provided, when the preconditions are met, primarily in the form of transcriptions.

Personal data related to other persons must be removed from audio and video recordings before the information is provided for checking, if it is at all

[3] Instruction for the processing of police assignments in emergency and field operations (POL-2019-74271, 23.01.2020) Appendix 1

possible and feasible with regard to the purpose, content and extent of the recording. Information can be anonymized for example with the help of Photoshop or other image processing software by masking or another suitable method facilitated by the system. Particular attention shall also be paid in connection with the measures to not disclosing the identity of for example the person having filed the report, or another person, who has justified reason to suspect that their personal or their family's health or safety can be threatened if their identity is revealed to outsiders.

6.2.6 Implementation of the right of access

The right of access is primarily implemented by delivering a copy to the data subject of the personal data processed, by post as an Advice of Delivery letter. The copies given to the data subject shall be appropriately labelled 'Confidential'. If it is not possible to use the required labelling, for technical or other similar reasons, the labelling and the reasons thereto can be expressed otherwise in writing or verbally[4].

In addition to the information provided for checking, the privacy statement applicable to personal data processing, or a public report on processing measures to fulfil the data subject's other right of access to information, shall be enclosed with the material. If the information related to personal data processing listed below cannot be handed over in a statement, the information must be provided to the data subject in another appropriate manner.

In connection with exercising the right of access, the data subject has the right to obtain also the following information related to the processing of their personal data:

- All information available of the origin of the data
- The purposes of the processing, legal basis and categories of personal data subject to processing
- Recipients or recipient groups of deliveries of data
- The period of personal data storage
- The data subject's right to request the controller to rectify or erase their personal data or restrict the processing of their personal data
- The data subject's right to request the Data Protection Ombudsman to take action and the Data Protection Ombudsman's contact information

By separate request, data subjects have the right to exercise the right of access to their data by visiting a police department or the controller's office in person. By separate request, the material can also be delivered to the data subject in electronic format, appropriately encrypted, unless compliance with the request causes unreasonable harm to official activities due to the high number of documents, or difficulties in converting the document into electronic format.

[4] Order regarding secure information processing in the police (POL-2020-69511, 17.12.2020)

The data related to the right of access matter shall be provided in an intelligible form to the data subject. Providing access to data means viewing of the information (documents or printouts) to the extent that they are stored concerning the data subject personally, in police filing systems and to which the data subject himself or herself has right of access.

If abbreviations are used in the printouts received from personal data filing systems of the police, the meaning of the abbreviations must be explained to the data subject in order to avoid any misunderstandings.

If the data subject prefers to exercise the right of access to their personal data by visiting police premises in person, the data to be viewed must primarily be printed on paper for the purpose of exercising the right of access. In such cases of exercising the right of access, it must be ensured that the measures are undertaken in appropriate premises, taking the obligations related to data protection and information security into consideration. Particular attention must be paid to the fact that right of access to data may not be provided by displaying the data directly to the data subject in the information systems or in any other way that endangers information security.

In connection with the right of access matter, at least the following documents and information shall be saved in the police's administrative case management, decision-making and archiving system (Acta) in connection with the processing of the right of access matter:

- The request document related to exercising the right of access, with appendices
- Decisions on transferring the matter, if any, related to the right of access matter
- Requests for clarification and measures according to Appendix 2, and the responses received to these, with appended materials
- Copy of data in the filing system to which the data subject was provided right of access, or information of that the filing system subjected to the right of access did not include data concerning the person exercising the right of access
- Printout of the right of access query system from the Data System for Police Matters (PATJA), if this system was the subject of the request
- The necessary itemization of the data in the filing system regarding which the right of access has been postponed, restricted or denied, with case-specific justifications
- The documents and replies sent to the data subject

6.2.7 Restrictions to the right of access, indirect right of access and log data

6.2.7.1 Restrictions to the right of access

Data subjects' right of access is restricted by law with regard to certain datasets in the police's personal data filing systems, and purposes of

processing. In addition to the Police Personal Data Act, restrictions to the right of access are laid down including in sections 24 and 28 of the Criminal Matters Personal Data Act, and with regard to personal data falling within the scope of the General Data Protection Regulation, in Article 3 of the General Data Protection Regulation and section 34 of the Data Protection Act. Provisions related to restrictions to the right of access may be included in other legislation as well.

Data subjects' direct right of access is restricted on the basis of the Police Personal Data Act with regard to data explained in further detail hereafter. The restrictions only apply to personal data processed within the scope of the Criminal Matters Personal Data Act and supplement the provisions of the Act on the Processing of Personal Data in Criminal Matters on case-specific restrictions to the right of access. The data subjects themselves do not have right of access to:

- Data of covert human intelligence sources referred to in section 9 of the Police Personal Data Act
- Personal data in the Schengen Information System relating to discreet surveillance or specific checks
- Information concerning the tactical and technical methods of the police included in the personal data referred to in sections 5–8 of the Police Personal Data Act
- Observation data, personal data of covert human intelligence sources or data used for forensic investigation purposes
- Personal data acquired using the intelligence gathering methods in accordance with Chapter 5 of the Police Act and Chapter 10 of the Coercive Measures Act (806/2011) or pursuant to section 157 of the Act on Electronic Communication Services (917/2014).

On the basis of the above provision, for example the following datasets and data saved in the personal data filing systems of the police are excluded from the data subject's right of access:

- Information corresponding to the information system of suspects, referred to in the repealed Police Personal Data Act, processed by the police for the purpose of preventing and detecting offences (Espa data)
- Classification and surveillance data concerning a person or act
- Information processed for the purpose of crime serialization
- Information processed for the purpose of assessing significance
- Among information of personal identifying characteristics, keywords, distinguishing marks or features/special ID marks, photographs, fingerprints and handprints, DNA samples and their classification data, and footwear prints
- Information processed for the purpose of safeguarding the safety of a person who is the subject of an action of the police or the occupational safety of an official, concerning the person's health and its monitoring or the treatment of his or her condition and concerning the danger

presented by or unpredictability of the subject or the person (security information)
- Information saved in police data in the Emergency Response Centre information system, necessary for the personal safety of the person or occupational safety, such as concerning the danger presented by or unpredictability of the subject or the person
- Information related to the security of detention of persons apprehended, arrested or imprisoned on the basis of the Criminal Investigation Act, Coercive Measures Act, Police Act or other provision
- Warrant of apprehension information saved in the wanted persons file and prepared for the purpose of surveillance of the person
- Warrant of apprehension information saved in the searched vehicles file of persons under surveillance and moving in motor vehicles

Provisions on the processing of personal data by the Finnish Security Intelligence Service are laid down in Chapter 7 of the Police Personal Data Act and the Finnish Security Intelligence Service also serves as the controller of the personal data referred to in that Chapter. No right of access applies to personal data processed by the Finnish Security Intelligence Service on the basis of Chapter 7 of the Police Personal Data Act.

Provisions on money laundering data filing system are laid down in section 3 of the Act on the Financial Intelligence Unit. The National Bureau of Investigation's Financial Intelligence Unit is the controller of the money laundering data filing system. The data subjects themselves do not have right of access to information in the money laundering data filing system, with the exception of the information related to decisions regarding the freezing of funds, referred to in section 2, subsection 1(7) of the Act.

In individual cases, a data subject's right of access to information can be limited, provided that certain preconditions are met, also on the following grounds laid down in the Data Protection Act and the Criminal Matters Personal Data Act if, considering the data subject's rights, it is necessary and proportionate in order to:

- Avoid detriment to the prevention, detection, investigation or prosecution of criminal offences or the enforcement of criminal sanctions
- Safeguard any other investigation, examination or other procedure of an authority
- Protect public security
- Protect national security
- Protect the rights of other persons

When implementing the right of access, it must be taken into consideration that if the right of access of the data subject is postponed, restricted or refused, completely or partially, the data subject must be informed of this in writing without undue delay. In this case, the grounds for the

postponement, restriction or refusal must also be included in the notification issued in the case, unless this would undermine the purpose of the refusal or restriction. However, it is possible that sometimes even the provision of upper level information only may jeopardize the purpose of the restriction (for example, information of an ongoing criminal investigation). In such situations, the controller is not obliged to reveal the reasons for the restriction.

The controller is obliged to maintain information of the grounds for the postponing, restricting or refusing of the right of access and this information must be available for supervisory authorities, by request, for the purpose of investigating in arrears whether the grounds for postponement, restriction or refusal of the right of access have been appropriate and sufficient. If the information in question has not been included in the notification issued to the data subject, the grounds must be documented in a separately prepared document.

If the implementation of right of access has been postponed with regard to a certain dataset, the information in question must be made accessible without undue delay when the grounds for postponing the right of access have expired. The police unit responsible for the right of access matter must monitor and supervise that the right of access is implemented appropriately also with regard to the postponed datasets.

The documents related to restricting the right of access and other information related to the matter shall be stored in the police's administrative case management, decision-making and archiving system (Acta) for further processing of the matter.

6.2.7.2 Indirect right of access

The data subject has the right to request the Data Protection Ombudsman to verify the lawfulness of the processing of personal data excluded from the data subject's personal right of access on the basis of the Police Personal Data Act and Act on the Financial Intelligence Unit, as provided in the Criminal Matters Personal Data Act (indirect right of access).

The data subject shall submit the request to exercise the indirect right of access either directly to the Data Protection Ombudsman or the National Police Board, or a police department, in person and by verifying his or her identity. The police unit having received the request shall record the information related to receiving the request and verifying identity in the request document and send it, without delay, to the Data Protection Ombudsman for processing.

The Data Protection Ombudsman verifies the lawfulness of personal data through the National Police Board. The National Police Board coordinates and obtains from police administration the reports required in the matter, the register data related to the verification and other information necessary

for the verification, and issues a statement on the matter on the basis of the clarification performed and received in the case.

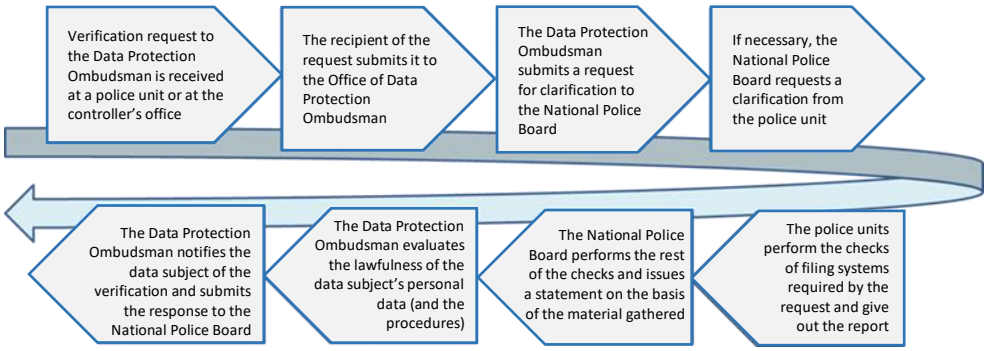

Figure: The process in the police related to exercising indirect right of access

The Data Protection Ombudsman has informed that in the verification process described above, particular attention is paid to the method of processing the data, the necessity and correctness of the data processed, the time of saving the data and the possibility for the data subjects to exercise their rights. The Data Protection Ombudsman has also stated that in the response given to the data subject, the information gained in the verification or whether the information system or data filing system contains information about the data subject at all, will not be disclosed.

The documents related to the indirect right of access case and other related information must be stored in the police's administrative case management, decision-making and archiving system (Acta) for further processing of the matter.

6.2.7.3 Log data

The controller and the processor of personal data shall ensure that logs are kept for the collection, alteration, consultation, disclosure, transfer, combination and erasure of personal data in their automated processing systems.

The logs of consultation and disclosure shall make it possible to establish the justification, date and time of the consultation and disclosure and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

The logs shall be used solely for verifying the lawfulness of processing, for internal monitoring, for ensuring the integrity and security of the personal data, and for criminal proceedings.

The right of access under data protection legislation applies to the data subject's personal data. The data saved in the usage log concern the persons who have or have had the right to use the police information system for which log data has been collected of the processing of data in the system (= users of information system). According to a decision by the Supreme Administrative Court, the person registered in the actual

information system of the police has no right of access to the data in the police user log system, because the log data are not personal data concerning the data subject[5].

A separate order has been issued on the management of log data in the police[6].

6.3 Rectification or erasure of personal data and restriction of processing

6.3.1 General information

Personal data processed in connection with the statutory duties of the police must be precise and up-to-date with regard to the purpose of processing. The police must ensure that all necessary measures are implemented to ensure that personal data that are inaccurate with regard to the purposes for which they are processed, are erased or rectified without delay.

Due to the extent and special characteristics of personal data processing by the police, the procedures and principles related to maintaining and updating of the data are planned and implemented specifically for each information system, as required by the information security and data protection requirements of the police. Regular information maintenance and updating measures related to personal data processing are performed as separately instructed, either directly on the basis of the user rights of the persons using the information system, or on the basis of a separate request to the system administrator of the information system.

6.3.2 Deadlines and principles related to the rectification, erasure and restrictions of personal data 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 police shall also prevent the spreading of such data if the data may risk the data subject's privacy protection or the data subject's rights.

With regard to personal data falling within the scope of the General Data Protection Regulation, the controller must deliver to the data subject, without undue delay, and principally no later than within one month of the request being presented, details of the measures undertaken as consequence of the request. If necessary, the deadline may be extended by two months at most, considering the complexity and number of requests. In this case, the controller must inform the data subject of the extension of deadline within one month of receiving the request, and give the reasons for the delay. If the controller fails to carry out measures based

[5] Supreme Administrative Court (KHO:2014:69, 8.5.2014) and decision of the Data Protection Ombudsman (Record no. 7681/152/18, 4.8.2020)
[6] Management of log data in the police (POL-2021-4922, 15.12.2021)

on the data subject's request, the controller must inform the data subject, without delay and no later than within one month of receiving the request, of the reasons thereto.

The controller also must, unprompted, or at the demand of the relevant data subject, and without undue delay, erase the data subject's personal data if their processing violates the requirements of the Criminal Matters Personal Data Act regarding legality, purpose of use, necessity or accuracy, or the provisions regarding special categories of personal data.

According to the Police Personal Data Act, any data in the filing system that are found to be incorrect may be kept with the rectified data if this is necessary to ensure the rights of the data subject, other parties or employees of the police. Because in this case, incorrect data may not be used for purposes other than the abovementioned, the possibility of the data being processed for other purposes must be prevented by technical means or in another appropriate way. Any data found to be incorrect shall be erased immediately as soon as the storing of the data is no longer necessary to ensure the relevant rights.

However, data found to be incorrect may not be retained in the National Schengen Information System.

Instead of erasing the data, the controller shall, however, restrict the processing of the data if the data subject contests the accuracy of the data and their accuracy or inaccuracy cannot be ascertained; or the personal data must be maintained for the purposes of evidence. The data subject's right to restrict personal data processing, as provided in the General Data Protection Regulation, does not, however, apply to personal data processing referred to in the Police Personal Data Act.

Restriction of processing must be implemented in the information systems for example by transferring the data to another system, or by preventing users from accessing personal data, the processing of which is restricted, by using technical means, or in another appropriate way. The restriction of personal data processing must be indicated clearly in connection with data whose processing is restricted.

Before removing the restriction of processing, the controller must inform the data subject about the matter, if processing has been restricted on the basis of the data subject having denied the accuracy of the data and it has not been possible to verify their accuracy or incorrectness.

6.3.3 Receiving a request and measures in police units

The data subject has the right to submit the request related to the rectification, erasure and restricting the processing of personal data for which the police bear controller's responsibility, in person to any police unit. Should the data subject so wish, the request may also be submitted by email or by post.

The National Police Board handles, in a centralized manner, all requests by data subjects concerning the rectification and erasure of personal data and restrictions of personal data processing, regarding personal data for which the National Police Board bears controller's responsibility. The police unit having received such a request shall transfer the matter without delay to the National Police Board. The party having presented the request shall be informed about the transfer of the matter. Simultaneously, the party having presented the request shall be informed that the National Police Board will reply directly to the party having presented the request.

If a request addressed to a police unit concerning the rectification or erasure of personal data and restrictions of personal data processing is targeted at data for which the National Police Board does not bear controller's responsibility, the police unit shall, as described above, transfer the processing of the matter to the competent controller.

The request concerning the rectification or erasure of personal data and restrictions of personal data processing should be sufficiently specific to indicate whose personal data the matter concerns, which personal data with the police the request to rectify or erase concerns (for example, presentation of full particulars of reports), why the data subject finds the data in question incomplete, inaccurate or incorrect for the purpose of processing, and what changes the data subject demands to be made to the data or why, according to the data subject, the data should be erased.

If it can be established in a customer service situation in a police unit that the request document submitted to the police concerning the rectification or erasure of personal data and restrictions of personal data processing, or request otherwise submitted, is clearly deficient or unclear by content, the data subject shall be assisted in submitting and specifying the request with sufficient precision and, if necessary, assisted in completing the documents related to the matter. Apparently deficient and unclear requests shall also be transferred to the National Police Board for further processing of the matter.

The forms available for all on the police website (https://poliisi.fi/en/deletion-and-rectification-of-data) concerning the rectification or erasure of personal data and restrictions of personal data processing are as follows:

- Rectification or erasure of personal data or restriction of processing personal data
- Rectification or erasure of personal data or restriction of processing personal data in the National Schengen Information System
- Rectification, erasure or restriction of access to personal data to the European Union Agency for Law Enforcement Cooperation (Europol)

If the controller refuses the data subject's request concerning the rectification or erasure of personal data or restrictions of personal data processing, the controller must inform the data subject of this refusal and

its grounds in a written certificate. However, information on the refusal or grounds thereto may be omitted wholly or partly to the extent that this is necessary on the grounds mentioned in section 28 of the Criminal Matters Personal Data Act.

When inaccurate personal data is rectified, the controller must also notify the authority from which the inaccurate data was obtained. If personal data has been rectified or erased, or if the processing of personal data has been restricted, the controller must notify the recipients to which the controller has disclosed this data, except in case this proves impossible or requires disproportionate efforts. The recipient must rectify or erase the personal data in question or restrict the processing of such personal data.

If the rectification or erasure of incorrect personal data has been performed by a police unit subordinate to the National Police Board, the police unit in question is obligated to clarify, as far as possible, whether the personal data in question has been disclosed to third parties. If data has been disclosed, the police unit shall, in the manner stated above, also inform the recipients to whom the police have disclosed the incorrect data in question.

The documents related to rectification and erasure of personal data and restriction of the processing of personal data and other necessary information shall be stored in the police's administrative case management, decision-making and archiving system (Acta). If the matter is transferred, a separate document shall be prepared and saved in connection with the material related to the matter.

6.3.4 Restrictions to data subjects' rights in matters related to the rectification and erasure of personal data and restrictions of personal data processing

Restrictions to the data subjects' rights related to the rectification and erasure of personal data and restrictions of personal data processing are laid down by law, including in sections 26 and 28 of the Criminal Matters Personal Data Act, and with regard to personal data falling within the scope of the General Data Protection Regulation, in Article 3 of the General Data Protection Regulation and, with regard to restrictions to processing, in section 45 of the Police Personal Data Act. Provisions related to the rectification and erasure of personal data and restrictions of personal data processing may be included in other legislation as well.

In individual cases, data subjects' right to the rectification and erasure of personal data and restrictions of personal data processing can be limited, provided that certain preconditions are met, also on the following grounds laid down in the Criminal Matters Personal Data Act if, considering the data subjects' rights, it is necessary and proportionate in order to:

- Avoid detriment to the prevention, detection, investigation or prosecution of criminal offences or the enforcement of criminal sanctions

- Safeguard any other investigation, examination or other procedure of an authority
- Protect public security
- Protect national security; or protect the rights of other people

6.3.5 Other measures required for personal data that is detected in police units and which is incorrect or incomplete with regard to the purpose of processing

When assessing the correctness and up-to-date status of data, it must be taken into account that the authority, within the limits of its jurisdiction and discretion, decides on the contents of documents or information recorded in an information system, taking into consideration the legal principles, obligations and restrictions related to data protection and processing of personal data. For example, information recorded in a crime report on malicious accusation are basically not incorrect from the perspective of personal data processing as referred to in data protection legislation, even though the data subject may regard the information in question to be incorrect, and factually unfounded from his or her viewpoint.

Neither do the police primarily change the information on its decisions, recorded in the Data System for Police Matters, on the basis of decisions made by prosecutors and courts, so that entries in police data filing systems remain and describe the situation in force at the conclusion of the pre-trial investigation. However, from the viewpoint of safeguarding data subjects' rights, the National Police Board has found it necessary that by separate request of the data subject, information on the decisions of the prosecutor and court of law can be added to the end of the report section of the crime report, to the extent provided in section 6, subsection 1(4) of the Police Personal Data Act.

If an information security incident or personal data breach is involved in an error or deficiency detected in the processing of personal data or information content of personal data, the procedure in the case must comply with the instructions and principles issued on management of incidents in the police.[7] A separate incident report must be made in the incident reporting system even if a pre-trial investigation or other such measures are undertaken in the case.

Regarding data for which the National Police Board bears controller's responsibility, the National Police Board decides in a centralized manner on whether it is necessary to report a personal data breach to the supervisory authority and also takes care of submitting the related report. Other controllers in the police administration are under the same obligation with regard to their data.

[7] Order on digital security in the police (POL-2022-12548, 19.4.2022)

The data subject must be informed of a personal data breach when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. However, there is no duty to report if:

- The controller has implemented appropriate technical and organizational protective measures on the personal data subjected to the breach that effectively prevent the misuse of the personal data; or
- After the breach, the controller has undertaken measures to ensure that the breach is not likely to pose a risk to implementing the rights of the data subject

Instead of a report to the data subject, the controller may inform about the information security breach in a public notice, if the submitting of a report to the data subject would require disproportionate efforts. Reporting to the data subject may also be postponed or restricted or not carried out if the preconditions pursuant to section 28 of the Criminal Matters Personal Data Act are met.

The information security officer of the police unit that received the report on the incident is primarily responsible for managing the information security incident and the measures required by the incident. The unit processing the case of the incident is also primarily responsible for the notification to the data subject, unless otherwise ordered or agreed with the National Police Board. If, in the case of severe and critical information security incidents, a crisis management group has been separately formed to manage the incident, the crisis management group also decides on the notifications submitted to the data subject, and the procedures required for the purpose.

The Criminal Matters Personal Data Act also includes the controller's obligation to communicate a personal data breach to another controller located in Finland or another EU Member State if the breach concerns data transferred by or to the latter controller. The information security officer of the police unit that received the report on the incident is primarily responsible for notifications to the aforementioned parties, unless otherwise agreed on or ordered.

6.4 Other rights of the data subject

The police process personal data mainly for the purposes of performing the police's statutory duties, and therefore certain rights of the data subjects defined in data protection legislation may be restricted by law. For example, the data subject's right to erasure of data based on the principle of the 'right to be forgotten', the right to data portability or the right to object the processing of personal data do not apply when personal data is processed in police duties falling within the scope of the Police Personal Data Act or other statutory duties of the police.

The extent and scope of data subject's rights shall be assessed both in connection with the planning of personal data processing and processing of requests related to data subject's rights specifically for each purpose of

use, particularly when personal data is processed solely in connection with the scope of the General Data Protection Regulation.

6.5 Appeal and the right to refer the case to the Data Protection Ombudsman for processing

According to the Data Protection Act, a data subject has the right to refer a matter to the Data Protection Ombudsman for consideration, if he or she considers that the relevant legislation is being infringed in the processing of personal data concerning him or her. Section 34 of the Data Protection Act lays down provisions on the procedure if the data subject does not have the right of access to data which have been collected concerning him or her. In that case, the data referred to in Article 15, paragraph 1 of the Data Protection Regulation must be submitted to the Data Protection Ombudsman by request of the data subject.

According to the Criminal Matters Personal Data Act, the data subject has the right to request the Data Protection Ombudsman to verify the lawfulness of the personal data and their processing if the right of access of the data subject has been postponed, restricted or refused by virtue of the Criminal Matters Personal Data Act or another Act, or if the controller does not accept the request of the data subject to rectify, supplement or erase personal data or to restrict their processing. According to the Criminal Matters Personal Data Act, if a data subject considers that the Criminal Matters Personal Data Act or another Act concerning the processing of personal data is being infringed in the processing of his or her personal data, he or she has the right to refer the matter to the Data Protection Ombudsman (request for measures).

The data subject has the right to receive, by separate request, an administrative decision, referred to in the Administrative Judicial Procedure Act, on decisions made by the police administration on data subject's rights, which may be appealed by way of appeal to the administrative court as provided in the Administrative Judicial Procedure Act (586/1996). The competent administrative court is defined on the basis of the data subject's registered domicile.

6.6 The exercise of the rights of the data subject and provision of measures free of charge

The communications, decisions and information given to the data subject by the police in accordance with data protection legislation, and the consideration of the requests made by the data subject are basically free of charge for the data subject.

The controller may collect a charge for the measure if the requests of the data subject are manifestly unreasonable or unfounded because of their recurrence or for another reason. Provisions on the criteria for and amounts of the charges are laid down in the Act on Criteria for Charges Payable to the State (150/1992) and the Decree of the Ministry of the Interior on chargeable performances by the police issued on its basis. The

controller must be able to prove that the request is manifestly unreasonable or unfounded if a charge is collected for a measure related to the matter.

Requests can be considered unreasonable for example if they are recurring. Based on the justifications of new data protection legislation, requests to the controller on exercising the right of access more often than once per year are not necessarily unreasonable in all cases, so that collecting a charge is always subject to a case-by-case consideration and assessment.

Because the controller must, if necessary, be able to prove that the request is manifestly unreasonable or unfounded, a sufficient explanation, with justification, must be documented in connection with the matter related to the request, of why a charge was collected for the measure. In line with the procedure of good administration, the data subject should be informed about eventual costs in advance, if it is possible and apparently necessary from the viewpoint of processing of the matter.

6.7 Other matters related to data subject's rights that must be taken into consideration

The police have also received such requests on exercising the data subject's right of access whereby the data subject actually exercises the right of access in order to deliver information to another party, such as another public authority or organization, based on a request submitted by that party or on the basis of an obligation imposed on the data subject.

No public authority or any other party have the right to oblige a data subject to submit to them information received by the data subject on the basis of exercising the data subject's right of access, and thus use the data subject's right of access as a method for obtaining information. The Deputy Data Protection Ombudsman has, in connection with a matter processed at the Deputy Data Protection Ombudsman's own initiative, found that acting in the aforementioned manner, the controller's personal data processing measures have been contrary to Article 6, paragraph 1, and Article 10 of the General Data Protection Regulation[8].

If the police become aware, in connection with the processing of a right of access matter or in another context, of indications of activities as the one described above, a notification of the case must be submitted both to the Registry of the Office of the Data Protection Ombudsman and the Police's Data Protection Officer.

In cases as the one described above, the request to exercise the right of access shall, however, primarily be processed and carried out in the police in line with the standard procedure, because it is not possible to restrict the data subject's right of access solely on the grounds that the data subject decides to exercise their right of access in order to submit personal data further to a third party.

[8] Deputy Data Protection Ombudsman's decision (Record no. 7635/162/21, 13.1.2022)

The police have received information requests other than those related to exercising the right of access also in order to check the data subject's criminal history in the case of persons applying to become a child's support person, by obtaining a written consent from the applicant for the social welfare authority to request an extract of the applicant's possible criminal records and sanctions, and house calls and apprehensions from the local police authority.

The Act on the Investigation of the Criminal History of Volunteers Working with Children (148/2014) lays down provisions on the procedure to check the criminal history of volunteers working with underage children. According to section 5 of the Act, the organizer of voluntary activities has the right, provided that the preconditions included in detail in the provision are met, to request from the Legal Register Centre a criminal record extract, referred to in section 6, subsection 2 of the Criminal Records Act (770/1993), concerning the volunteer, if the volunteer has given an advance written consent for requesting the criminal record extract. Provisions on the personal data processing in question have been laid down in a specific law, referred to in Article 10 of the General Data Protection Regulation.

Based on the provisions in general law, the criminal history of volunteers working with children cannot be clarified more extensively than stated above, for example on the basis of section 20 of the Act on the Status and Rights of Social Welfare Clients (812/2000) or on the legal basis laid down in the General Data Protection Regulation.

Neither is consent as the legal basis for personal data processing freely given, as required in the General Data Protection Regulation, in such specific cases where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and where refusing to give consent may have apparently negative consequences regarding the data subject's rights, in the matter being processed.

The Deputy Data Protection Ombudsman has, in connection with a case initiated by the data subject, found that when acting in the manner described in detail in the decision, the controller's personal data processing measures have been contrary to Articles 5, 6, 10, 12 and 25 of the General Data Protection Regulation[9].

In connection with the processing of other information requests, the police shall pay particular attention to the legal basis for requesting the information and to what extent, and on which preconditions laid down by law, information can be delivered. For example, delivering information on the basis of section 20 of the Act on the Status and Rights of Social Welfare Clients, requires that the information delivered is such that it has a material impact on the customer relationship and necessary because of a

[9] Deputy Data Protection Ombudsman's decision (Record no. 6689/186/20, 15.1.2021)

statutory duty of the public authority. Also, general principles of interpretation of the law, and provisions restricting the use of information influence the consideration of disclosure of data.

The material must also be delivered in such form and to such extent that misunderstandings of the matter underlying the data cannot arise with the recipient. The printouts from the Data System for Police Matters (PATJA) are primarily designed for internal use of the police and are not usually suitable as such for delivery to external parties. The recommended procedure is to record the data to be disclosed in a separate document, which can contribute to ensuring that no extra data are delivered.

When the request for information is targeted at data in the Data System for Police Matters (PATJA), case-specific assessments shall pay attention particularly to the following:

- The time elapsed from the act
- The age of the subject of the report at the time of the act
- The recurrence of the acts and the disregard they indicate for the rights of others, or lack of judgment
- The severity of the consequences of the act
- The nature or significance of the act in relation to the assignment as basis for the information request

The end result related to the delivery of information consists of simultaneous consideration of the criteria related to the subject matter and overall assessment. The significance of the criminal act and its relation to the assignment for which the information is requested can be regarded as the key assessment criteria.

Information in the archive directory of investigation and executive assistance can be used in order to find documents and cases possibly relevant in the case, transferred to archive, but the information disclosed must always be based on the information in the original archived documents.

In order to avoid any misunderstandings, it may be good to explain the background related to individual cases to the extent necessary. Information on consequences related to the case investigated, if such information is already known to the police or, alternatively, information on that the police do not have such information on consequences, can also be included in the information disclosed. However, the police do not primarily have the obligation to separately find out information on consequences regarding all decisions of prosecutors and courts of law on behalf of the parties requesting the information, because they can request the information directly from the authorities in question.

If the police become aware, in connection with the processing of requests for information or in another context, of an outside party regularly submitting apparently inappropriate information requests to the police, as

described above, a notification must be submitted about this to the Police's Data Protection Officer.

7 General procedures and principles in personal data processing

7.1 Accountability

The General Data Protection Regulation and the Criminal Matters Personal Data Act require verifiability of the lawfulness of personal data processing. The police must be able to prove that personal data is processed by the police in accordance with statutory requirements.

The accountability principle obliges the police to ensure that the police can prove the lawfulness of each personal data processing measure throughout the lifecycle of the data. In the implementation of verifiability, high-quality, adequate documentation, monitoring and supervision of personal data processing activities, and reporting, are emphasized. In order to implement transparency of informing, privacy statements and other information material for data subjects are publicly available on the poliisi.fi website.

In police operations, personal data are processed only for the purposes specified by law and in the ways described in privacy statements or statements of processing procedures, procedural instructions and orders. Information on the lawfulness of operations is collected in connection with processing to prove the legality of processing.

7.2 Obligation of defined purpose of processing and duty of care

In police operations, all personal data processing must be in compliance with the law and appropriately justified with regard to police duties. The personal data processed and the procedures of processing are specified in writing before the personal data is collected. The purpose of personal data processing shall always be defined so that duties in which the personal data in question are being processed are made clear. The personal data processed shall be sufficiently protected. The personnel processing personal data have received training for their duties. Introduction to and training in information security and data protection are provided on a regular basis.

The planning of personal data processing takes into account good information processing and management procedures, the requirement of data protection by design and by default and the information management policy and principles of the police, other instructions for personal data processing by the police and requirements resulting from legislation on personal data processing.

In police operations, the necessary technical and organizational measures to ensure and prove that personal data processing is carried out in accordance with legal requirements, are implemented, taking into account the nature, scope, context and purposes of personal data processing, as

well as the risks, varying in probability and severity, targeted at the rights and freedoms of natural persons. In this context, also the appropriate technical and organizational measures are implemented to ensure that, by default, only personal data that are necessary for each specific purpose of the processing are processed.

The National Police Board and other police units ensure that the obligation of defined purpose of processing and duty of care is implemented internally by providing high-quality instructions and procedural descriptions. Responsibilities for personal data processing activities are allocated comprehensively and monitored and supervised systematically. A data protection cooperation network will be established in the police administration to support data protection work in police units and the internal flow of information in the administration.

Data protection is taken into account in all police operations and particularly in the planning and development of operations. Data protection is specifically taken into account in the development and introduction of information systems. The project work model of the police requires assessment of data protection at the preliminary assessment stage of information system projects and planning of data protection properties in the operational and technical requirement specification. The decision to introduce an information system requires that the data protection criteria specified for the project are fulfilled. Fulfilment of information security and data protection requirements is verified by conducting an audit before the introduction of the information system.

During the data protection assessment at the preliminary assessment stage, a separate decision is made on whether a statutory impact assessment should also be carried out. The impact assessment shall be carried out when the development project involves such identified data protection risks whose management methods are appropriate for investigating in an impact assessment process. The assessment presents at least a general description of the planned processing measures, an assessment of the risks targeted at data subject's rights and freedoms, the measures intended to tackle the risks and the protective measures, security measures and mechanisms that secure personal data protection and prove compliance with data protection legislation.

The diligence and quality of data protection activities shall also be ensured by way of regular audits and inspections of data protection activities and personal data processing.

7.3 Legal basis, purposes and necessity of personal data processing

The processing of personal data is allowed only when a legal basis and purpose for the processing can be proven to exist in the law. In police operations, the right to process personal data is primarily based on performing the duties provided in section 1 of the Police Act, as provided in

the Police Personal Data Act. Separate provisions on information acquisition related to police operations are laid down in legislation on police powers related to the duties of the police. The Police Personal Data Act also lays down specific provisions on the key purposes of personal data with regard to police duties. When performing police duties, only personal data necessary for performing the statutory duties of the police, and for exercising police powers, are processed.

In addition, the requirement to respect fundamental and human rights, the principle of proportionality, the principle of minimum intervention, and the principle of intended purpose, as laid down in Chapter 1 of the Police Act, are always complied with in the processing of personal data. In the processing of personal data, the police also comply with the requirement of data minimization. All personal data processed by the police must be adequate and relevant in relation to the purposes for which they are processed.

Processing of personal data in the police is primarily based on the duties laid down in Chapter 1, section 1 of the Police Act. Accordingly, personal data processing is justified in the following duties:

- Securing the rule of law
- Maintaining public order and security
- Preventing, detecting and investigating crimes and submitting cases to prosecutors for consideration of charges
- Maintaining security in cooperation with other public authorities and with communities and residents
- Engaging in international cooperation pertaining to police duties
- Duties related to licensing functions
- Providing individuals with such assistance as falls within police duties
- Finding those who have gone missing or fallen victim to an accident
- Other duties laid down by law

Provisions on the right of the police to use personal data for purposes other than the initial purpose while performing the duties laid down in Chapter 1, section 1 of the Police Act, are laid down in the Police Personal Data Act and it is permitted only when the preconditions laid down by law are met.

7.4 Quality and accuracy

The police ensure the quality and adequate accuracy of all personal data processed. The personal data processed by the police for the purposes of police duties is sufficiently accurate, the integrity and up-to-date status of the personal data is ensured, and the processing of personal data is necessary for performing the duties in question. The police take every reasonable step to ensure that inaccurate, incomplete or outdated personal data are not transferred or made accessible.

Appropriate and comprehensive manuals, orders and operational instructions have been provided regarding the collection methods of data

and the criteria for entering the data in information systems, and other operating methods and procedures related to the processing of personal data. Entry of personal data in information systems is also guided by instructions of user interfaces and the restrictions of entering data implemented in the user interfaces, the formal requirements for information, and data quality checks.

Data quality is maintained with regular batch processing to ensure the accuracy, integrity and precision of data and with automated updates from external registers, including the Population Information System. Insofar as possible, the accuracy of data is also verified on the basis of data received from data subjects themselves, through data maintenance measures implemented by persons responsible for information management in the police, and information management inspection activities as specified in rules of procedure and job descriptions.

The requirements for data quality are taken into account in system development, particularly as part of the specification and testing of information systems' operational and content-related requirements. Information systems are implemented so that if necessary, and insofar as possible, personal data that concern data subjects in different positions with regard to the matter processed, are clearly kept separate, and that personal data based on facts are kept separate from personal data based on personal assessments.

With regard to the disclosure and transfer of personal data, ensuring data quality and lawfulness of personal data processing are secured also in the receiving party's operations by way of agreements and data permits.

7.5 Erasure, retaining and archiving of data as part of the lifecycle of data

The right to process personal data in the statutory duties of the police is mainly based on special legislation on the police. Thus, the Police Personal Data Act and other special legislation concerning the police include provisions on the erasure, retaining and archiving of data. The law includes separately defined principles and deadlines for the erasure of data and for the right to retain data in special situations provided by law. Separate provisions are laid down on retaining data found incorrect in connection with corrected data.

Personal data is erased from other personal data filing systems of the police governed by general data protection legislation (including the user log system, user right management system, access control systems and case management systems of the police) when the need ends to use and process data, specified and assessed in advance. Unnecessary personal data or personal data that has become unnecessary, personal data that is incorrect, incomplete or outdated, are not processed.

When the need for or right to process personal data no longer exists, the data will primarily be erased or destroyed, unless the data has been separately ordered or provided for to be retained further, or to be archived.

7.6 Processing of special categories of personal data

Special categories of personal data include personal data revealing ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and genetic data, biometric data for the purpose of unique identification of a natural person and data concerning health or a natural person's sex life or sexual orientation.

The processing of special categories of personal data is allowed only if the personal data processing is provided by law, relates to the consideration of a criminal case in the prosecution service or in court; the processing is necessary for protecting a vital interest of the data subject or of another natural person; or the processing relates to data which the data subject has manifestly made public. Further preconditions include that the processing of such data is strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject. Profiling that results in discrimination against natural persons on the basis of special categories of personal data is, however, prohibited at all times.

The data content in the key information systems of the police, whose processing is allowed, and the purposes of use of data are limited in accordance with the information system and personal data filing system specific data contents specified in the Police Personal Data Act, which often also include special categories of personal data.

7.7 Processing of personal identity code

The personal identity code is a special identifier allocated to a person for the purpose of uniquely identifying persons. A personal identity code may be processed only if it is necessary to uniquely identify the data subject in order to perform a statutory duty of a competent authority, in order to implement the rights or obligations of the data subject or the controller or when personal data is processed for historical or scientific research purposes or statistical purposes.

A personal identity code shall not be unnecessarily entered into documents printed out from or drawn up based on a personal data filing system, nor for unnecessary processing in information systems and visible for example in case management systems, such as in case header data in the police’s administrative case management, decision-making and archiving system.

The necessity of entering a personal identity code into documents printed out from information systems shall always be assessed on a case-by-case basis when planning the processing of personal data, taking the purpose of the document into consideration alongside the party to which the document

will possibly be delivered. Particular attention shall be paid to whether it is necessary to include a personal identity code in various decision documents in license administration, considering the fact that the decision relates primarily to administrative matters initiated by the data subjects themselves.

According to section 44 of the Administrative Procedure Act, as a rule, a written administrative decision shall indicate the authority that made the decision and the date when it was made; the parties whom the decision directly concerns; the reasons for the decision and specific information about what a party is entitled or obliged to do or how the matter was otherwise decided; and the name and contact details of the person from whom a party may request further information on the decision, if necessary.

In the decision on entering the personal identity code into invoices, the Data Protection Ombudsman has taken a stand also on the processing of personal identity code in administrative decisions. According to the Data Protection Ombudsman's decision, the reason for processing of personal identity code (including entering it into documents) cannot be that it makes the activities more convenient. Regarding the preparedness of systems, Article 32 of the General Data Protection Regulation shall also be taken into account, as in practical terms, it requires that the controller has implemented such technical capacities that the provisions laid down in the Regulation can be concretely implemented. Furthermore, the personal identity code is not intended to be used as a method for identification, and identification alone cannot constitute grounds for processing of the personal identity code.[10]

7.8 Impact assessment and prior consultation

The purpose of impact assessment is to help identify, assess and manage the risks involved in personal data processing and it is intended as an ongoing process for the identification and management of risks.

An impact assessment shall be carried out for example when the purpose of personal data processing is a systematic and extensive profiling of persons, the processing in question relates on a large scale to special categories of personal data or criminal convictions, new technologies are used in the processing of personal data or a systematic monitoring of a publicly accessible area on a large scale is carried out, and the processing of personal data is likely to result in a high risk to the rights and freedoms of data subjects.

The impact assessment by the police produces at least a general description of the planned processing measures, an assessment of the risks targeted at data subject's rights and freedoms, the measures intended to tackle the risks and the protective measures, security measures and

[10] Data Protection Ombudsman's decision (Record no. 8205/154/18, 14.5.2020)

mechanisms that secure personal data protection and prove compliance with data protection legislation.

In the police, impact assessments are often linked to project and system work procedures and procurements. The need for an impact assessment and preparation for it are taken into account already at the planning or surveying stage of ICT projects, when operations are planned. As part of the information systems' coordination teams, at least a documented, standard-format, light data protection assessment of all significant development measures is produced.

The unit responsible for the development of each police information system and the project owner bear the main responsibility for conducting a data protection assessment and impact assessment, and for producing the required documentation. If necessary, the impact assessment can also be prepared concerning a certain purpose of use entity of data. Data protection experts and the Police's Data Protection Officer provide guidance and support to carrying out the impact assessment and, if necessary, refer the case to the police's internal impact assessment process.

During the impact assessment, the supervisory authority must be separately consulted before personal data processing begins, if the impact assessment proves, or it is otherwise recognized that regardless of the planned protective measures, the processing will involve significant risks to the data subjects' rights or the data processing, particularly due to the use of new technologies, mechanisms or procedures, will result in a significant risk in terms of the data subject's rights.

In connection with the prior consultation, the impact assessment documentation required for the processing of the matter, and other material requested by the supervisory authority, shall be delivered to the supervisory authority. In the police, the prior consultation procedure shall be implemented in a centralized manner through the National Police Board's information management regarding the filing systems for which the National Police Board bears controller's responsibility. Other controllers in the police administration are responsible for conducting an impact assessment for their part. The Police's Data Protection Officer plays a guiding and consulting role in the prior consultations.

The police shall be prepared for possible prior consultation of the supervisory authority already when planning and allocating resources to projects and other development measures. This requirement shall be taken into consideration also when defining the requirement level for the documentation of projects and planning of personal data processing functions.

The instructions and other comments possibly issued by the supervisory authority shall be complied with in the personal data processing subjected to the prior consultation.

7.9 Protection of data and information security

The starting point of information security in the police is to ensure the continuity of operations both in normal situations and during incidents and exceptional circumstances. The starting point is the reliable and lawful processing of data. Personal data are processed securely and in compliance with good information management practices.

The key objective of information security efforts is to secure the reliable reputation of the police. Trust is maintained through efficient, modern and appropriately protected processing of data. The overall objective of operations is a high standard of information security management for police data at the national and international level.

The police ensure protection of personal data and information security by implementing adequate and appropriate technical and administrative protective measures. The secrecy and other protection of personal data filing systems and the data included in them are secured, including by way of the following measures and based on the following principles:

- User authorization management and supervision of the police enable system users to access data and services necessary for performing their duties, and ensure that only persons authorized to use police data and services have access to them.
- Systematic and careful processing of log data implements supervision of system usage, clarification of misuse, clarification of information security incidents and system errors, and statistics of usage volumes. Logging ensures the legal protection of data subjects and those who process data subjects' data.
- Unauthorized alteration of information and any other unauthorized or inappropriate processing is prevented through user rights administration, supervision of use and appropriate and sufficient security arrangements and technical functionalities of information networks, information systems and information services.

National Police Commissioner Seppo Kolehmainen

Senior Adviser Harri Kukkola

The document is digitally signed in the case processing system. The Police 13.01.2023 at 13:35. The authenticity of the signature can be verified at the Registry.

Appendices	Appendix 1: Information systems and data the implementation of which police departments are responsible for inspecting (Usage restriction SECURITY LEVEL IV) Appendix 2: Exceptional procedures related to checking of register data# (Usage restriction SECURITY LEVEL IV)
Distribution	National Police Board Units Police Units
For the attention of	Police Department of the Ministry of the Interior Police Authority in the Åland Island Finnish Security Intelligence Service Office of the Data Protection Ombudsman Government security network (TUVE) at Valtori *Sinetti* collection of norms / Advisory Staff Poliisi.fi website / Advisory Staff