Translation from Finnish
Legally binding only in Finnish and Swedish
Ministry of the Interior, Finland

Act on the Processing of Personal Data by the Police

(616/2019; amendments up to 209/2023 included)

Chapter 1
General provisions

Section 1
Scope of application

Unless otherwise provided elsewhere by law, this Act applies to the processing of personal data necessary for the performance of the duties of the police referred to in chapter 1, section 1 of the Police Act (872/2011), where:

1) the processing is wholly or partly performed by automated means; or

2) the personal data form, or are intended to form, a filing system or part thereof.

The provisions of chapter 7 apply to the processing of personal data necessary for the performance of the duties of the Finnish Security and Intelligence Service.

This Act also lays down provisions on access to information from certain European information systems for the prevention, detection and investigation of terrorist offences and serious crimes. (818/2022)

Subsection 3, added by Act 818/2022, enters into force on 7 February 2023.

Section 2
Relationship to other legislation

Unless otherwise provided in this Act,

1) the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018), hereafter the Criminal Matters Personal Data Act, applies to the processing of personal data for the purpose of preventing, detecting and investigating offences, referring them for consideration of charges, and safeguarding against threats to public security and preventing such threats;

2) the provisions on the openness of government activities apply to the right of access to data and to other disclosure of personal data contained in a filing system of a public authority.

Provisions on the processing of personal data are also laid down in Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereafter the Data Protection Regulation, as well as in the Data Protection Act (1050/2018).

The processing of personal data shall comply with the requirement of respect for fundamental and human rights, the principle of proportionality, the principle of minimum intervention, and the principle of intended purpose laid down in chapter 1 of the Police Act.

The processing of personal data shall not, without an acceptable reason, be based on a person's age, gender, origin, nationality, place of residence, language, religion, conviction, opinion, political activity, trade union activity, family relationships, state of health, disability, sexual orientation, or other reason related to that person.

Provisions on the punishment for a data protection offence are laid down in chapter 38, section 9 of the Criminal Code (39/1889).

Separate provisions are issued on the information gathering by the police and the related powers.

Section 3 (818/2022)
Definitions

In this Act:

1) *SIS Regulations* means Regulation (EU) 2018/1860 of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals, Regulation (EU) 2018/1861 of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, and Regulation (EU) 2018/1862 of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU;

2) *Schengen Information System* means the SIS system referred to in the SIS Regulations;

3) *National Schengen Information System* means the N.SIS system referred to in the SIS Regulations;

4) *Europol Regulation* means Regulation (EU) 2016/794 of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA;

5) *Eurodac Regulation* means Regulation (EU) No 603/2013 of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice;

6) *VIS Regulation* means Regulation (EC) No 767/2008 of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation);

7) *VIS Decision* means Council Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences.

Regulation (EC) No 1986/2006 of the European Parliament and of the Council was repealed by Regulation (EU) 2018/1862 of the European Parliament and of the Council. Regulation (EC) No 1987/2006 of the European Parliament and of the Council was repealed by Regulation (EU) 2018/1861 of the European Parliament and of the Council.

Chapter 2
Processing of personal data

Section 4
Processing of basic personal data

The police may process the following basic personal data for the purposes laid down in sections 5, 7, 9 and 11:

1) names;

2) date and place of birth;

3) personal identity code;

4) gender;

5) native language;

6) communication language;

7) civil status;

8) citizenship or lack of citizenship and nationality;

9) domicile and place of residence;

10) occupation and education;

11) contact details;

12) information in the documentation necessary to establish identity;

13) in the case of foreign nationals, the names, citizenship and nationality of the parents;

14) travel document information and other information concerning entry into the country and border-crossing;

15) customer number issued by the authorities;

16) information on the person's death or declaration of death;

17) information on guardianship, declaration of bankruptcy or imposition of a business prohibition;

18) information on completing military service.

Section 5
Processing of personal data in investigations and surveillance

The police may process personal data for the purposes of a criminal investigation, police investigation or performing other duties related to investigation of an offence or referral of cases for consideration of charges, and performing duties related to maintaining public order and security or other statutory surveillance duties of the police.

It is further required that the personal data referred to in subsection 1 concern a person who is:

1) suspected of an offence or complicity in an offence;

2) younger than 15 years of age and suspected of a criminal act;

3) a subject of a criminal investigation, police investigation or police action;

4) reporting an offence or is an injured party;

5) a witness;

6) a victim;

7) directly linked to a field operation of the police or a surveillance duty separately provided by law;

8) some other source of information relating to the duties of the police.

The data received in connection with the performance of police duties shall be destroyed immediately after it is established that the information is not needed for the processing purposes referred to in subsection 1 or section 13, subsection 1.

Section 6
Contents of personal data that are processed in investigations and surveillance

In addition to the basic personal data referred to in section 4, the police may also process the following personal data concerning the persons referred to in section 5:

1) specifications, descriptions and classifications relating to police duties, actions or operations;

2) personal identifying characteristics to establish identity, including fingerprints, handprints and footprints, handwriting, voice and odour samples, and DNA profiles, facial images and other biometric data; information on close relatives required in finding people reported missing and identifying unidentified deceased persons can only be processed with the consent of the person in question;

3) information for the purpose of safeguarding the safety of a person who is the subject of an action 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; and information that describes or is intended to describe a criminal act, punishment or other consequence of an offence;

4) identification information on a decision by the prosecutor or court; information on whether the person was convicted, his or her charges or punishment waived, or his or her charges dismissed, ruled inadmissible or dropped; and information on whether the decision is final; (209/2023)

Paragraph 4, as amended by Act 209/2023, enters into force on 1 October 2023.
Previous form of wording:

4) identification information on a decision by the prosecutor or court; information on whether the person was convicted, his or her charges or punishment waived, or his or her charges dismissed, ruled inadmissible or dropped; and information on whether the decision is final.

5) information regarding a restraining order referred to in the Act on Restraining Orders (898/1998) and a protection measure referred to in the Act on the Application of the Regulation of the European Parliament and of the Council on Mutual Recognition of Protective Measures in Civil Matters (227/2015), including location information obtained in the course of technical supervision of a restraining order referred to in section 15b of the Act on Restraining Orders. (209/2023)

Paragraph 5, as added by Act 209/2023, enters into force on 1 October 2023.

Section 7
Processing of personal data for the purpose of preventing and detecting offences

The police may process personal data for the purpose of performing duties relating to the prevention and detection of offences.

It is further required that the personal data referred to in subsection 1 concern persons:

1) in respect of whom there are reasonable grounds to believe that they have committed, or have an intention to commit, an offence for which the most severe punishment provided by law is imprisonment;

2) who are in contact with a person referred to in paragraph 1 or seen with such a person and the contacts or meetings can be assumed to have a link with the offence due to their regularity or the circumstances or behaviour of the person;

3) who are subjects of the surveillance referred to in chapter 5, section 13 of the Police Act or some other police action.

The police may also process the data referred to in subsection 1 on the following persons, provided that this is essential for the prevention or detection of an offence:

1) witnesses;

2) victims;

3) persons reporting an offence and injured parties.

The decision to commence the processing of personal data in connection with a crime analysis required for the prevention and detection of offences is taken by the controller or some other police unit assigned by the controller to carry out this duty.

In addition, the police may process information on observations made by police officers and information reported to the police regarding incidents or persons that, based on the circumstances or on the behaviour of the person, can reasonably be believed to be connected with criminal activity.

The data received in connection with the performance of police duties shall be destroyed immediately after it is established that the information is not needed for the processing purposes referred to in subsection 1 or section 13, subsection 1.

Section 8
Contents of personal data that are processed for the purposes of prevention and detection of offences

In addition to the basic personal data referred to in section 4, the police may also process the following personal data concerning the persons referred to in section 7:

1) specifications, descriptions and classifications relating to police duties, actions or operations;

2) details concerning the person's connections, lifestyle, financial situation, hobbies, and other interests;

3) personal identifying characteristics to establish identity, including voice samples, facial images and other biometric data;

4) information for the purpose of safeguarding the safety of a person who is the subject of an action or the occupational safety of an official, concerning the person's state of 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; and information that describes or is intended to describe a criminal act, punishment or other consequence of an offence; (209/2023)

Paragraph 4, as amended by Act 209/2023, enters into force on 1 October 2023. Previous form of wording:

4) information for the purpose of safeguarding the safety of a person who is the subject of an action or the occupational safety of an official, concerning the person's state of 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; and information that describes or is intended to describe a criminal act, punishment or other consequence of an offence.

5) information regarding a restraining order referred to in the Act on Restraining Orders and a protection measure referred to in the Act on the Application of a Regulation of the European Parliament and of the Council on Mutual Recognition of Protective Measures in Civil Matters, including location information obtained in the course of technical supervision of a restraining order referred to in section 15b of the Act on Restraining Orders. (16.2.2023/209)

Paragraph 5, as added by Act 209/2023, enters into force on 1 October 2023.

Where possible, an assessment of the reliability of the data provider or data source and the accuracy of the data shall be appended to the personal data obtained.

Section 9

Processing of data of covert human intelligence sources

In addition to the basic personal data referred to in section 4, the police may also process the following personal data concerning the covert human intelligence sources referred to in chapter 5, section 40 of the Police Act or in chapter 10, section 39 of the Coercive Measures Act (806/2011):

1) information on the use and surveillance of covert human intelligence sources;

2) main contents of the information provided by a covert human intelligence source.

Section 10
Processing of personal data related to the quality assurance of DNA samples

For the purpose of the quality assurance of DNA samples, the police may process the following personal data concerning persons other than those who are suspected of an offence or are unknown subjects linked to the offence:

1) names;

2) personal identity code;

3) DNA profile;

4) workplace.

However, such persons have the right to refuse to give a sample of their DNA and the processing of their personal data.

Section 11
Processing of personal data in other statutory duties of the police

The police may also process personal data for the performance of their duties related to licence services or such police surveillance duties separately provided by law that are not relating 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.

Section 12

Contents of personal data that are processed for the purpose of performing other statutory duties of the police

In addition to the basic personal data referred to in section 4, the police may also process the following personal data for the purposes specified in section 11:

1) information concerning an application, permit, licence, statement, notification or decision;

2) information concerning reasons against the issuance or continuing the validity of a permit or licence, as well as information required for establishing the fulfilment of the criteria for issuing or continuing the validity of a permit or licence, including health information and other special categories of personal data;

3) information concerning measures taken by the authorities;

4) a photograph or signature sample submitted to the police, the Ministry for Foreign Affairs or an authority of the Foreign Service when applying for a permit, licence or decision, preparation of which requires a photograph and signature sample of the applicant;

5) biometric fingerprint data and a facial image taken of the person applying for an identity card or passport to perform the duties laid down in the Identity Card Act (663/2016) or in the Passport Act (671/2006);

6) information for the purpose of safeguarding the safety of a person who is the subject of an action 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; and information that describes or is intended to describe a criminal act, punishment or other consequence of an offence;

7) information concerning administrative sanctions;

8) information other than that referred to in paragraphs 1–7 that is essential for performing duties referred to in section 11, excluding special categories of personal data.

As part of supervision pursuant to the Act on Preventing Money Laundering and Terrorist Financing (444/2017), and of supervision and compiling statistics in accordance with the Lotteries Act (1047/2001), the police may process personal data concerning the customers of a gambling company, and of another trader and corporation that they supervise pursuant to the foregoing Acts, to the extent that this is essential for performing the duty of supervision and compiling statistics. (1285/2021)

Section 13
Processing of personal data for purposes other than the initial purpose

Unless otherwise provided elsewhere by law, the police may process the personal data referred to in sections 5–9, 11 and 12 for the following purposes other than the initial purpose:

1) prevention or detection of an offence;

2) investigation of an offence for which the most severe punishment provided by law is imprisonment;

3) finding of wanted persons;

4) as evidence in support of innocence;

5) prevention of a significant danger to life, health or liberty, or substantial damage to the environment or property, or a substantial financial loss;

6) protection of national security;

7) establishing identity in the performance of a police action in which the establishment of identity is essential;

8) directing police operations.

Notwithstanding non-disclosure provisions, data in the filing system of the police may also be processed in oversight of legality, analysis, planning and development activities. Such data may also be used in training activities if the data are essential for carrying out the training.

With the consent of the person in question, the photograph and signature sample referred to in section 12, subsection 1, paragraph 4 may also be used for preparation of other administrative permits or decisions applied for by the person concerned than that for which the person initially submitted the photograph and signature sample.

The personal data referred to in section 12, subsection 2 may only be used for their initial purpose.

Section 14

Processing of personal data for purposes other than the initial purpose in considering and monitoring permits and licences

Unless otherwise provided elsewhere by law, the police may process the personal data referred to in sections 5, 6, 9, 11 and 12 for purposes other than the initial purpose when deciding or issuing an opinion on the granting or validity of a permit or licence, if it has been laid down that a requirement for the granting or validity of the permit or licence is the applicant's or holder's trustworthiness, suitability or other such attribute whose assessment requires information on the state of health, intoxicant use, criminal guilt, or violent behaviour of the applicant or holder.

The police may also use a notification drawn up by the National Bureau of Investigation on the basis of data concerning the persons referred to in section 7, subsection 2 for the purpose of assessing the conditions for granting or continuing the validity of a permit or licence under the circumstances referred to in subsection 1. The notification shall contain all the information necessary to assess the conditions for granting and the validity of the permit or licence. The National Bureau of Investigation may submit the notification if:

1) the permit or licence applicant or permit or licence holder has, on the basis of the information referred to in section 8, regular or permanent contacts with a person who has been found guilty by a court of participating in the activity of an organised criminal group or who is suspected of participating in such activities on the basis of a pending criminal investigation or consideration of charges, provided that the nature of such contacts may make the applicant or holder vulnerable to inappropriate external influencing and thus endanger the protection of the statutory preconditions for the granting or continuing the validity of the permit or licence; or

2) the National Bureau of Investigation considers that on the basis of the information referred to in section 8 and other possible examination, there are reasonable grounds to suspect that the permit

or licence applicant or the permit or licence holder is guilty of participating in the activity of an organised criminal group and that notifying the police of this matter is essential to protect the statutory preconditions for the granting or continuing the validity of the permit against actions or influencing by the organised criminal group concerned.

Section 15 (696/2021)
Processing of special categories of personal data

The police may process special categories of personal data only if the processing is strictly necessary for the purpose of the processing.

Biometric data processed for the performance of the duties laid down in the Identity Card Act and the Passport Act may only be used for purposes other than the initial purpose if this is strictly necessary for identifying a victim of a natural disaster, major accident, other disaster or criminal offence, or a victim who has otherwise remained unidentified. The right of access only pertains to persons who absolutely need this data for the performance of their duties. Data taken for comparison purposes may only be used for the duration of the comparison and shall be destroyed immediately thereafter.

Biometric data processed for the performance of duties laid down in the Identity Card Act and the Passport Act may also be used if this is strictly necessary to identify the applicant for an identity card or passport when he or she subsequently applies for an identity document and, with the consent of the person concerned, also for preparing such a document.

Biometric data processed for the performance of the duties laid down in section 131 of the Aliens Act (301/2004) may only be used for purposes other than the initial purpose in the circumstances referred to in subsection 2 and whenever the use of such data is strictly necessary for the purposes of prevention, detection or investigation of an offence referred to in chapter 11–14; chapter 17, sections 2–4, 7, 7c or 8a; chapter 34, section 3 or 5; chapter 34a; or chapter 46, section 1 or 2 of the Criminal Code. The right of access only pertains to persons who absolutely need this data for the performance of their duties. Data taken for comparison purposes may only be used for the duration of the comparison and shall be destroyed immediately thereafter.

Data processed for the purpose of quality assurance of DNA samples may only be used for the initial purpose. Such data may also be used for oversight of legality, analysis, planning and

development activities and in training activities if the data are essential for carrying out the training.

Information contained in a firearms notice referred to in section 114 of the Firearms Act (1/1998) may only be used for the purpose of processing data concerning firearm licences.

Chapter 3
Right to obtain information

Section 16
Right of the police to obtain information contained in certain registers and information systems

Notwithstanding non-disclosure provisions, the police have the right, in addition to what is laid down elsewhere by law, to obtain, with the aid of a technical interface or as a set of data, information contained in various registers for the purposes of carrying out their duties and maintaining their filing systems in accordance with the practices agreed upon with the relevant controller as follows:

1) from the transport register referred to in the Act on Transport Services (320/2017), information that is necessary for the performance of the statutory police duties;

2) from the prison and probation register referred to in the Act on the Processing of Personal Data at the Prison and Probation Service (1301/2021), information concerning a person suspected or convicted of an offence, a prisoner, a remand prisoner and a person serving a community sanction can be obtained: in accordance with section 19 of the said Act, for a statutory duty of a public authority laid down in section 1 of the Criminal Matters Personal Data Act; and in accordance with section 20 of the Act on the Processing of Personal Data at the Prison and Probation Service, for the purpose of a permit, licence or approval of the police that requires that a person be trustworthy, or for the purpose of processing a matter related to residence in Finland, international protection, removal from Finland, citizenship, or the imposition or withdrawal of an entry ban; (1308/2021)

3) from accommodation business operators, passenger information referred to in section 6, subsection 1 of the Act on Accommodation and Catering Operations (308/2006) for the purposes

of maintaining public order and security, preventing, detecting or investigating offences, and performing other statutory police duties;

4) from the register of fines referred to in the Act on the Enforcement of Fines (672/2002), information relating to offences and criminal sanctions for the purposes specified in section 50 of the said Act, as well as for licence and permit administration; from the criminal records referred to in the Criminal Records Act (770/1993), personal data for the purposes specified in sections 4 and 4a of the said Act; from judicial administration authorities, information on wanted persons; from the decision notification system referred to in the Act on the National Information System of the Judicial Administration (372/2010), information on decisions issued in criminal matters and their finality; and from the national record and case management system, information regarding criminal matters that are or have been pending at the prosecution service or courts of law;

5) from the Trade Register of the Finnish Patent and Registration Office, information on notifications and communications concerning traders for the purposes of preventing, detecting and investigating offences;

6) from the filing systems of the Border Guard and Customs, information that is necessary for the performance of police duties corresponding to the duties for which the data were collected and recorded, and for other purposes in cases referred to in section 13 and in section 14, subsection 1;

7) from the information systems of the Ministry for Foreign Affairs, information for the purpose of a criminal investigation, other investigation or performance of duties laid down for the police in the Aliens Act on staff members of a diplomatic or consular mission representing the sending state in Finland, staff members of the Finnish branch of an international organisation or staff members of other international organisations in a corresponding position, as well as on their family members and private personnel; (632/2020)

8) information from the electronic case management system for immigration affairs referred to in the Act on the Processing of Personal Data in the Immigration Administration (615/2020) and from the national visa information system for preventing and detecting offences, for criminal and other investigations, and for performing police duties laid down in the Aliens Act, the Nationality Act (359/2003) and the Act on the Treatment of Detained Aliens and on Detention Units (116/ 2002); (632/2020)

9) from teleoperators, information referred to in chapter 10, sections 6–8 of the Coercive Measures Act; chapter 5, sections 8 and 9 of the Police Act; and chapter 19 of the Act on Electronic Communication Services (917/2014);

10) from an authority requesting executive assistance, information necessary to provide the executive assistance;

11) from the information referred to in sections 13–17 of the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency (661/2009); (1162/2019)

12) from the Defence Forces, information on military service or fitness for military service concerning persons liable for military service, provided that this is essential for the evaluation of the suitability of an applicant or a holder of a permit or licence referred to in the Firearms Act, and a person for whom an application has been made for an approval referred to in the Firearms Act or who has received such an approval, as well as for the evaluation of the eligibility of an applicant or holder of a permit or licence referred to in the Passport Act or the Identity Card Act;

13) from the charger's certification register referred to in section 22 of the Charger Act (423/2016), information for the purposes of surveillance and emergency duties and for the prevention, detection and investigation of offences;

14) from the land information system referred to in the Act on the Land Information System and Related Information Service (453/2002) and from the residential and commercial property information system referred to in the Act on the Residential and Commercial Property Information System (1328/2018), information for the purposes of preventing, detecting and investigating offences;

15) from passenger data registers and vehicle staff registers of organisations and corporations, information for the purposes of preventing, detecting and investigating offences and referring them for consideration of charges, and apprehending wanted persons; provisions on the right to obtain information contained in the passenger name records of air carriers are laid down in the Act on the Use of Air Carriers' Passenger Name Record Data in the Prevention of Terrorist Offences and Serious Crime (657/2019).

The police have the right to obtain the information referred to in subsection 1 free of charge, unless otherwise provided elsewhere by law.

At the request of a controller disclosing personal data pursuant to subsection 1, the police are required to notify the controller of the processing of the personal data received.

The Act on the National Information System of the Judicial Administration (372/2010) was repealed by the Act on the National Data Repository of the Judicial Administration (955/2020).

Section 17
Disclosure of data from other authorities to the police by depositing online or as a set of data for the purpose of recording

Other authorities may disclose data to the filing systems of the police by depositing online or as a set of data for the purpose of recording, in accordance with the practices agreed upon with the relevant controller, as follows:

1) the Finnish Security and Intelligence Service may disclose information for the purpose of the prevention, detection and investigation of offences and protection of national security;

2) judicial administration authorities, the Criminal Sanctions Agency and the Legal Register Centre may disclose information concerning wanted persons; the Criminal Sanctions Agency may disclose personal identifying characteristics concerning persons serving or having served a sentence involving deprivation of liberty; and the Legal Register Centre may disclose information on restraining orders and business prohibitions, as well as on protection measures referred to in the Act on the Application of the Regulation of the European Parliament and of the Council on Mutual Recognition of Protection Measures in Civil Matters (227/2015);

3) Customs and military officials may disclose information on wanted persons, and Customs may disclose personal identifying characteristics and travel document information for the performance of duties laid down in section 131 of the Aliens Act, as well as information for the prevention and investigation of offences;

4) the Ministry for Foreign Affairs and Finnish missions may disclose information for the performance of the duties laid down for the Ministry for Foreign Affairs and Finnish missions in the Passport Act; the Ministry for Foreign Affairs may disclose information on staff members of a diplomatic or consular mission representing the sending state in Finland, staff members of the Finnish branch of an international organisation or staff members of other international organisations in a corresponding post, as well as on their family members and private personnel;

5) the Border Guard may disclose information referred to in sections 5–8 processed for the performance of the duties laid down for the Border Guard in the Border Guard Act (578/2005), Act on Crime Prevention by the Border Guard (108/2018) or elsewhere by law, as well as information in accordance with sections 11 and 12 of this Act processed for the performance of the duties laid down for the Border Guard in chapter 1, section 1, subsection 2 of the Police Act or elsewhere by law;

6) game and fisheries wardens of Metsähallitus may disclose information regarding measures taken while carrying out game and fisheries control within their mandate;

7) Emergency Response Centre officials may disclose information for ensuring the safety of a person recorded in the emergency response centre data system or occupational safety;

8) the Finnish Immigration Service may disclose information regarding national entry bans and decisions on denial of admittance or stay or deportation, as well as information concerning police actions relating to executive assistance.

At the request of a controller disclosing personal data pursuant to subsection 1, the police are required to notify the controller of the processing of the personal data received.

Section 18 (818/2022)
Access to information from certain European information systems to prevent, detect and investigate terrorist and serious offences

The National Bureau of Investigation, the Finnish Security and Intelligence Service and Customs have the central access points referred to in Article 3, paragraph 3 of the VIS Decision for obtaining information from the Visa Information System in order to prevent, detect and investigate the following offences:

1) the terrorist offences referred to in chapter 34a, sections 1, 1a, 2–4, 4a–4c, 5 and 5a–5d of the Criminal Code;

2) the offences referred to in section 3, subsection 2 of the Act on Surrender Procedures between Finland and Other Member States of the European Union (1286/2003).

The National Bureau of Investigation has a National Access Point referred to in Article 3, paragraph 2 of the Eurodac Regulation for submitting requests for comparison of fingerprint data with Eurodac data in order to prevent, detect and investigate the following offences:

1) the terrorist offences referred to in chapter 34a, sections 1, 1a, 2–4, 4a–4c, 5 and 5a–5d of the Criminal Code;

2) offences referred to in section 3, subsection 2 of the Act on Surrender Procedures between Finland and Other Member States of the European Union for which the most severe punishment provided by law is at least three years' imprisonment.

The National Bureau of Investigation is also the verifying authority referred to in Article 6, paragraph 1 of the Eurodac Regulation.

Council Decision 2008/633/JHA was repealed by Regulation (EU) 2021/1134 of the European Parliament and of the Council.

Section 18a (1207/2022)
Access to information from the Entry/Exit System and the ETIAS Central System to prevent, detect and investigate terrorist and serious offences

The National Bureau of Investigation and Customs have the central access points referred to in Article 29 of Regulation (EU) 2017/2226 of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No

1077/2011, hereafter referred to as the EES Regulation, for obtaining information from the Entry/Exit System to prevent, detect and investigate the following offences:

1) the terrorist offences referred to in chapter 34a, sections 1, 1a, 2–4, 4a–4c, 5 and 5a–5d of the Criminal Code;

2) offences referred to in section 3, subsection 2 of the Act on Surrender Procedures between Finland and Other Member States of the European Union for which the most severe punishment provided by law is at least three years' imprisonment.

The National Bureau of Investigation and Customs have the central access points referred to in Article 50 of Regulation (EU) 2018/1240 of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, hereafter referred to as the ETIAS Regulation, for obtaining information from the ETIAS Central System to prevent, detect and investigate the following offences:

1) the terrorist offences referred to in chapter 34a, sections 1, 1a, 2–4, 4a–4c, 5 and 5a–5d of the Criminal Code;

2) offences referred to in section 3, subsection 2 of the Act on Surrender Procedures between Finland and Other Member States of the European Union for which the most severe punishment provided by law is at least three years' imprisonment.

Section 18a, added by Act 1207/2022, enters into force on a date to be set by decree.

Section 19
Conditional fine

The police may obligate the party from whom they are entitled to obtain the information referred to in section 16, subsection 1, paragraph 15 to disclose the information within a reasonable time. The police may impose a conditional fine to enforce compliance with this duty. The decision to impose a conditional fine shall be complied with regardless of any request for a review concerning the decision. However, a conditional fine may not be imposed if there is reason to suspect the party in question of an offence and the material requested is related to a matter subject to

suspicion of an offence. In other respects, the provisions on conditional fines are laid down in the Act on Conditional Fines (1113/1990).

Section 20
Processing of personal data received in connection with international cooperation

The processing of personal data received from a third county or an international organisation or agency shall comply with the conditions set by the provider of the data concerning non-disclosure, the obligation to remain silent, restrictions on the use of the data, onward transfer of the data, and returning of the disclosed data.

Unless otherwise provided in subsection 1, the police may use the disclosed personal data for purposes other than those for which they were disclosed in compliance with section 13, subsection 1.

Chapter 4
Disclosure of personal data

Section 21
Disclosure of personal data to another competent authority referred to in the Criminal Matters Personal Data Act

Notwithstanding non-disclosure provisions, the police may, with the aid of a technical interface or as a set of data, disclose the personal data referred to in sections 5–9, 11 and 12 to the Finnish Security and Intelligence Service, Customs, the Border Guard, prosecutors, courts, the Legal Register Centre, the Criminal Sanctions Agency, and other competent authorities referred to in the Criminal Matters Personal Data Act for the performance of the authority's statutory duties referred to in section 1 of the said Act.

Section 22
Other disclosure of personal data to authorities

Notwithstanding non-disclosure provisions, the police may, with the aid of a technical interface or as a set of data, disclose personal data referred to in sections 5–8, 11 and 12 for the performance of a statutory duty of the authorities as follows:

1) to the Finnish Transport and Communications Agency, information in accordance with sections 197 and 217 of the Act on Transport Services that is essential for the performance of its statutory duties;

2) to the Emergency Response Centre Agency, information for the performance of the duties laid down in the Act on Emergency Response Centre Operations (692/2010) in order to ensure initial measures or occupational safety or to provide assistance to the unit in question, while complying with the provisions concerning restrictions on the right to obtain information laid down in section 19, subsection 2 of the same Act, as well as the safety information referred to in section 6, paragraph 3 of this Act for recording in the emergency response centre data system;

3) to rescue authorities for rescue operations referred to in section 32 of the Rescue Act (379/2011);

4) to the Border Guard, information for the purpose of border control and maintaining border security and order along the border, for other purposes corresponding to the initial purpose, and for other purposes in cases under sections 16 and 17 of the Act on the Processing of Personal Data by the Border Guard (639/2019);

5) to social welfare authorities for considering matters concerning the means of support of an alien;

6) to Customs for customs control, tax supervision, control of entry and exit of persons, and performing related border checks, for serving summonses and other notifications, for other purposes corresponding to the initial purpose, and for other purposes in cases pursuant to section 15 of the Act on the Processing of Personal Data by Customs (650/2019);

7) to the employment and economic development authorities for considering matters concerning residence permits for employed persons and entrepreneurs;

8) to the Ministry for Foreign Affairs and Finnish missions for considering matters concerning passports or other travel documents, visas, and residence permits for employed persons and entrepreneurs or other residence permits within their mandate;

9) to the Finnish Immigration Service for considering and deciding on matters concerning aliens and Finnish citizenship which are laid down by law or decree to be its duties, as well as for carrying out the statutory supervisory duties of the Finnish Immigration Service;

10) to courts of law for considering cases concerning firearms, firearm components, cartridges or specially dangerous projectiles;

11) to enforcement officers in accordance with chapter 3, section 67 of the Enforcement Code (705/2007) for an enforcement inquiry or other execution of enforcement measures;

12) to public officials specified in sections 1 and 6 of the Process Servers Act (505/1986) for the purpose of summoning the person concerned to a trial for imposing a conversion sentence for unpaid fines, and to process servers for the purpose of serving a summons, the basic personal data, occupational safety information and data on persons under arrest processed for the purposes specified in section 5 of this Act;

13) to game and fisheries wardens of Metsähallitus for carrying out game and fisheries control within their mandate;

14) to municipalities acting as road maintenance authorities and the Finnish Transport Infrastructure Agency, traffic accident data for the promotion of traffic safety;

15) to the occupational safety and health authorities, the information in accordance with Directive 2006/22/EC of the European Parliament and of the Council on minimum conditions for the implementation of Council Regulations (EEC) No 3820/85 and (EEC) No 3821/85 concerning social legislation relating to road transport activities and repealing Council Directive 88/599/EEC for the monitoring of driving and rest times;

16) to the Digital and Population Data Services Agency or the State Department of Åland for the duty referred to in section 38 of the Nationality Act; (632/2020)

17) to the Defence Forces, Customs, the Border Guard and the Criminal Sanctions Agency for the purpose of evaluating suitability to bear a firearm in the case of a person employed by them who is entitled to carry a firearm in his or her official work or service duties.

Notwithstanding non-disclosure provisions, the biometric data processed for the performance of the duties laid down in the Identity Card Act and in the Passport Act may only be disclosed to the authorities referred to in subsections 4, 6, 8 and 9 of this section for the purposes of establishing identity and document authentication, provided that this is strictly necessary for considering matters concerning the person's entry or residence in or exit from the country.

Besides the provisions of subsection 1, notwithstanding non-disclosure provisions, the police may on justifiable grounds disclose, with the aid of a technical interface or as a set of data, personal data to other authorities, provided that these are essential for the performance of a statutory duty of the authorities.

Prior to the disclosure of any personal data, the recipient shall provide the controller with a reliable report on the appropriate protection of the personal data disclosed.

The quality of the data to be disclosed shall be verified and, where possible, the data shall be supplemented by information that allows the recipient to evaluate the accuracy, completeness, timeliness and reliability of the data. If it transpires that incorrect data have been disclosed or that data have been disclosed unlawfully, the recipient shall be notified of the matter without delay.

Section 23
Disclosure of personal data via a public information network

Notwithstanding non-disclosure provisions, the police may disclose, via a public information network, information for the purpose of informing the general public and receiving leads from the public, where this is necessary due to crime prevention, returning property to its owner, or investigative reasons. In such cases, personal data may only be retrieved based on individual searches.

Notwithstanding non-disclosure provisions, the police may also disclose, via a public information network, information for the purpose of informing the general public and receiving leads from the public, where this is particularly necessary due to the urgency of the matter, a dangerous situation, crime prevention, returning property to its owner, or investigative reasons. Personal data may only be disclosed in a manner other than that referred to in subsection 1 if this is materially important for the performance of a duty laid down in chapter 1, section 1, subsection 1 of the Police Act and disclosure of the data does not conflict with a legitimate interest of the data subject.

Data received from another authority may only be disclosed with the consent of the authority that disclosed the data.

Section 24
Disclosure of personal data to private organisations or traders via e-services

Notwithstanding non-disclosure provisions, the police may disclose the permit or licence data processed for the purposes laid down in section 11 to private organisations or traders, if this is necessary for the performance of their statutory duties. In such cases, personal data may only be retrieved in the e-service based on individual searches.

Section 25
Disclosure of personal data to law enforcement authorities of a Member State of the European Union or of the European Economic Area

Notwithstanding non-disclosure provisions, the police may disclose personal data referred to in sections 5–8, 11 and 12 to competent authorities of another Member State of the European Union or of the European Economic Area who process the data for the purpose laid down in Article 1(1) of Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA under the same conditions as the police may process the said personal data.

Notwithstanding non-disclosure provisions, the police may also disclose personal data referred to in sections 5–8, 11 and 12 to Eurojust and other agencies established pursuant to the Treaty on the Functioning of the European Union responsible for safeguarding legal and social order, maintaining public order and security, or preventing and investigating offences and referring them for consideration of charges, for attending to the said duties.

The information referred to in subsections 1 and 2 may also be disclosed as a set of data.

Besides the provisions in this Act and in the Criminal Matters Personal Data Act, provisions on the disclosure of personal data to law enforcement authorities of the Member States of the European

Union are laid down in the Act on the National Implementation of the Provisions of a Legislative Nature of Council Framework Decision on Simplifying the Exchange of Information and Intelligence between Law Enforcement Authorities of the Member States of the European Union and on the Application of the Framework Decision (26/2009).

Section 26 (818/2022)
Disclosure of personal data in the National Schengen Information System

Notwithstanding non-disclosure provisions, the police may disclose information from the National Schengen Information System to the Finnish Security and Intelligence Service, the Border Guard, Customs, the Defence Forces, a prosecutor, the Finnish Immigration Service, the Finnish Transport and Communications Agency, the Emergency Response Centre Agency, the Ministry for Foreign Affairs and a Finnish diplomatic or consular mission in compliance with the provisions of the SIS Regulations.

Section 27 (818/2022)
Disclosure of personal data to common information systems of the European Union

Notwithstanding non-disclosure provisions, the police may disclose the personal data referred to in sections 5–8, 11 and 12:

1) to the Schengen Information System;

2) to the Eurodac system referred to in the Eurodac Regulation;

3) to the Visa Information System referred to in the VIS Regulation.

The information shall be disclosed in compliance with the provisions of the SIS Regulations and the Regulations referred to in subsection 1.

The National Bureau of Investigation serves as the SIRENE Bureau referred to in the SIS Regulations.

Section 27a (1207/2022)

Disclosure of personal data to the Entry/Exit System and the European Travel Information and Authorisation System

Notwithstanding non-disclosure provisions, the police may disclose the personal data referred to in sections 5–8, 11 and 12:

1) to the Entry/Exit System referred to in the EES Regulation;

2) to the European Travel Information and Authorisation System referred to in the ETIAS Regulation.

The data shall be disclosed in compliance with the provisions of the Regulations referred to in subsection 1.

The information for the ETIAS watchlist referred to in Article 34 of the ETIAS Regulation shall be disclosed through the national ETIAS unit referred to in section 18 of the Border Guard Act.

Section 27a, added by Act 1207/2022, enters into force on a date to be set by decree.

Section 28
Disclosure of personal data to Europol

Notwithstanding non-disclosure provisions, the police may disclose personal data to the European Union Agency for Law Enforcement Cooperation in compliance with the Europol Regulation and the Act on the European Union Agency for Law Enforcement Cooperation (214/2017).

Section 29 (818/2022)

Section 29 was repealed by Act 818/2022, which enters into force on a date to be set by decree. Previous form of wording:

Section 29
Disclosure of personal data to Eurodac

Notwithstanding non-disclosure provisions, the police may disclose personal data to Eurodac in accordance with the Eurodac Regulation. The national Eurodac unit and the designated authority for law enforcement purposes referred to in Article 5(1) of the Eurodac Regulation is the National Bureau of Investigation.

Section 30
Disclosure of personal data pursuant to the Prüm Treaty and Prüm Decision

The provisions of Articles 3, 9 and 12 of the Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, hereafter the Prüm Decision, apply to the disclosure of DNA, fingerprint and vehicle registration data on the basis of a match search pursuant to the Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration (Finnish Treaty Series 54/2007), hereafter the Prüm Treaty, and pursuant to the Prüm Decision.

Besides the provisions of Article 5, 10 and 14 of the Prüm Decision, section 25 of this Act applies to disclosure of personal data following a match referred to in subsection 1.

Section 31
Other disclosure of personal data abroad

Notwithstanding non-disclosure provisions, the police may disclose personal data in compliance with chapter 7 of the Criminal Matters Personal Data Act.

Notwithstanding non-disclosure provisions, the police may disclose:

1) personal data to the competent authorities referred to in international treaties or other arrangements concerning the readmission of persons entering the country and residing there without authorisation for the performance of the duties referred to in the said international treaties or arrangements;

2) personal data relating to the acquisition, possession, transfer, import and export of firearms, firearm components, cartridges and especially dangerous projectiles to an arms control authority of another state, provided that the disclosure of data is essential for the purpose of arms control;

3) personal data processed for the performance of the duties laid down in section 131 of the Aliens Act to the European Border and Coast Guard Agency, in compliance with the provisions of Regulation (EU) 2019/1896 of the European Parliament and of the Council on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624.

(1250/2020)

The biometric data processed for the performance of the duties laid down in the Identity Card Act and in the Passport Act may be disclosed only for the purposes in accordance with section 15, subsection 2.

The information referred to in this section may also be disclosed as a set of data.

Disclosure of information shall comply with international agreements that are binding on Finland. International cooperation and information exchanges are prohibited where there are reasonable grounds to suspect that a person could be subject to the death penalty, torture, other treatment that violates human dignity, persecution, arbitrary deprivation of liberty or unfair trial on account of such cooperation or information exchange. (818/2022)

Section 32
Decisions on disclosing data

The decision on the right to disclose, with the aid of a technical interface or as a set of data, information in the filing system of the police and on the right of the authorities referred to in chapter 3 to disclose information, with the aid of a technical interface or as a set of data, to the information system of the police is taken by the controller or another police unit assigned by the controller to carry out this duty.

When deciding on disclosure, the quality of the data to be disclosed shall be taken into account to ensure the data protection and data security of the data subject.

Chapter 5
Erasure and archiving of personal data

Section 33
Erasure of personal data relating to criminal matters

Data concerning a criminal matter referred to the prosecutor for a decision are erased:

1) five years after the referral of the criminal matter to the prosecutor, if the most serious offence suspected in the criminal matter may result in a fine or a maximum imprisonment of one year;

2) ten years after the referral of the criminal matter to the prosecutor, if the most serious offence suspected in the criminal matter may result in an imprisonment of more than one year and no more than five years;

3) twenty years after the referral of the criminal matter to the prosecutor, if the most serious offence suspected in the criminal matter may result in an imprisonment of over five years.

The data referred to in subsection 1 are, however, erased at the earliest one year after the expiration of the limitation period for bringing charges for the offence.

Data on criminal matters other than those referred to in subsection 1 are erased one year after the expiration of the limitation period for bringing charges for the latest suspected offence, but no earlier than five years after the recording of the criminal matter.

Personal identifying characteristics processed to establish identity are erased no later than ten years after the last entry concerning the person suspected of an offence. However, the data are erased no later than ten years after the death of the data subject if the most serious punishment for the most severe offence recorded is a minimum imprisonment of one year.

The personal identifying characteristics of a data subject who was under 15 years of age at the time of committing the offence are erased no later than five years after the recording of the last entry concerning the person suspected of an offence, unless any of the entries concern an offence for which the only sanction is imprisonment.

The data referred to in subsections 4 and 5 are erased no later than one year after the entry, if, during the investigation, it was ascertained that no offence was committed or that there is no longer reason to suspect the person in question of an offence.

However, personal data relating to a criminal matter referred to in subsections 1–5 may be retained, if this is necessary for investigative, surveillance or other justified reasons or to ensure the rights of the data subject, other parties or employees of the police. The necessity of retaining personal data shall be reviewed at least every five years.

Logging and monitoring data concerning data processing based on the Prüm Treaty and the Prüm Decision are retained and erased in compliance with Article 39(4) and (5) of the Prüm Treaty and Article 30(4) and (5) of the Prüm Decision.

Section 34
Erasure of other personal data processed in investigations and surveillance

Personal data processed in investigation and surveillance duties other than those referred to in section 33 are erased five years after the recording of the relevant report or matter, unless they are connected to a criminal matter under investigation.

By derogation from subsection 1:

1) data concerning a business prohibition are erased five years after the end of the prohibition;

2) data concerning a restraining order, a prohibition to visit or a protection measure referred to in the Act on the Application of the Regulation of the European Parliament and of the Council on Mutual Recognition of Protection Measures in Civil Matters are erased five years after the imposition of the restraining order, prohibition to visit or protection measure;

3) data concerning probationary liberty under supervision or monitoring sentence are erased five years after the end of the probationary liberty under supervision or monitoring sentence;

4) other data concerning a warrant of apprehension, travel ban, prohibition to keep animals, hunting prohibition, national entry ban, community sanction or conditional release processed for

the purpose of finding, monitoring, surveillance or protection of individuals are erased three years after the cancellation or expiry of the warrant or prohibition;

5) personal data processed for the purpose of finding people reported missing or identifying unidentified deceased persons are erased no earlier than five years after the finding of the missing person or identification of the unidentified deceased person; however, information on close relatives necessary for the purpose of finding people reported missing and identifying unidentified deceased persons are erased at the request of the data subject or immediately once they are no longer necessary for the purpose of the processing;

6) personal identifying characteristics processed for the performance of the duties laid down in section 131 of the Aliens Act and travel document information are erased ten years after the last entry concerning the data subject; however, if the data subject is granted Finnish citizenship, the data are erased, one year after the date on which the controller was notified of the granting of the citizenship.

The data referred to in subsection 2, paragraph 6 and section 6, paragraph 3 are erased no later than one year after the death of the data subject.

The personal data referred to in subsections 1–3 may nevertheless be retained, if this is necessary for investigative, surveillance or other justified reasons or to ensure the rights of the data subject, other parties or employees of the police. The necessity of retaining personal data shall be reviewed at least every five years.

Section 35
Erasure of personal data relating to the prevention and detection of offences

Personal data relating to the prevention and detection of offences are erased no later than ten years after the last entry concerning an offence, criminal activity or action. The data referred to in section 7, subsection 5 are, however, erased no later than six months after making the entry, and the data referred to in section 8, subsection 1, paragraph 4 are erased no later than one year after the death of the data subject.

However, personal data referred to in subsection 1 may be retained, if this is necessary for investigative, surveillance or other justified reasons or to ensure the rights of the data subject,

other parties or employees of the police. The necessity of retaining personal data shall be reviewed at least every five years.

Section 36
Erasure of data concerning covert human intelligence sources

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

Section 37
Erasure of personal data processed for the quality assurance of DNA samples

Personal data processed for the quality assurance of DNA samples are erased at the request of the data subject or immediately once they are no longer necessary for the purpose of the processing.

The necessity of retaining the personal data shall be reviewed at least once a year.

Section 38 (696/2021)
Erasure of personal data processed in other statutory duties of the police

Personal data processed for the performance of licence services or surveillance duties are erased no later than twenty years after the relevant decision or lapse thereof, expiry of the period of validity indicated in the decision, or entry of the personal data.

By derogation from paragraph 1:

1) data contained in a firearm notice referred to in the Firearms Act are erased no later than three years after making the entry;

2) personal data processed pursuant to section 42c of the Firearms Act are erased thirty years after the disposal of the item in question; however, the data may be processed only for the purposes laid down in section 11 of this Act for a period of ten years after the disposal of the item;

3) personal data concerning lost-and-found services are erased no later than one year after making the entry;

4) personal data included in reports on suspected violations referred to in chapter 7, section 9 of the Act on Preventing Money Laundering and Terrorist Financing are erased in accordance with subsection 2 of the said section and other personal data relating to supervision in accordance with the said chapter are erased no later than five years after making the entry;

5) data concerning administrative sanctions are erased no later than five years after making the entry;

6) personal data concerning the customers of gambling operators, traders or corporations under supervision processed for the purpose of supervision in accordance with the Lotteries Act and the Act on Preventing Money Laundering and Terrorist Financing are erased once retaining the data is no longer necessary for the performance of the supervision duty;

7) the fingerprint data taken in an application of an identity card applicant referred to in section 17, subsection 3 of the Identity Card Act are erased no later than 30 days after the identity card is issued.

However, the personal data referred to in subsection 1 and subsection 2, paragraph 1 are erased no later than one year after the death of the data subject, unless there are special reasons to retain the data. The necessity of retaining personal data shall be reviewed at least every five years.

Section 39
Data found to be incorrect

Notwithstanding the provisions of the Criminal Matters Personal Data Act and the Data Protection Regulation on the rectification of incorrect data, any data 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. Such data may only be used for the stated purpose.

Subsection 2 was repealed by Act 818/2022, which enters into force on a date to be set by decree. Previous form of wording:

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

Any data found to be incorrect and retained pursuant to subsection 1 shall be erased immediately once the storing of the data is no longer necessary to ensure the relevant rights.

Section 40
Archiving information

Separate provisions are issued on archiving duties and documents to be archived.

Chapter 6
Rights of a data subject

Section 41
Implementing the right of access of the data subject

For the purpose of implementing the right of access of the data subject referred to in section 23 of the Criminal Matters Personal Data Act and the right of access by the data subject referred to in Article 15 of the Data Protection Regulation, the controller provides access to the necessary personal data and other information, unless the controller has ordered some other police unit to provide the requested information.

The data subject shall, when exercising his or her right of access, make a request to this effect in person to the controller or some other police unit referred to in subsection 1 and prove his or her identity. The request may also be submitted by using the strong electronic identification referred to in the Act on Strong Electronic Identification and Electronic Trust Services (617/2009), if such service is available.

Section 42
Limitations to the right of access

By derogation from section 23 of the Criminal Matters Personal Data Act, the right of access does not apply to:

1) the personal data referred to in section 9;

2) personal data concerning discreet checks, inquiry checks and specific checks of the National Schengen Information System; (818/2022)

3) information concerning the tactical and technical methods of the police, observation data, personal data of covert human intelligence sources or data used for forensic investigation purposes included in the personal data referred to in sections 5–8;

4) 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 or pursuant to section 157 of the Act on Electronic Communication Services.

Provisions on the exercise of the rights of the data subject through the Data Protection Ombudsman are laid down in section 29 of the Criminal Matters Personal Data Act. The request relating to the exercise of the rights shall be made to the Data Protection Ombudsman or to the police in accordance with section 41, subsection 2 of this Act. A request made to the police shall be referred to the Data Protection Ombudsman without delay.

Section 43 (818/2022)
Section 43 was repealed by Act 818/2022, which enters into force on a date to be set by decree. Previous form of wording:

Section 43
Exercise of the right of access to data in the data file maintained by the technical support function of the Schengen Information System

Besides the provisions of section 41, everyone has the right to request the supervisory authority referred to in Article 115 of the Convention implementing the Schengen Agreement on the gradual abolition of checks at common borders (Finnish Treaty Series 23/2001) to check that the collection, recording, processing and use of their personal data in the data file maintained by the technical support function of the Schengen Information System takes place in a lawful and correct manner. The request shall be made to the Data Protection Ombudsman or to the police in accordance with section 41, subsection 2 of this Act. A request made to the police shall be referred to the Data Protection Ombudsman without delay.

Section 44

Exercise of the right of access in the case of personal data processed pursuant to the Prüm Treaty and Prüm Decision

Besides the provisions of section 42, everyone has the right to request the Data Protection Ombudsman to verify that the processing of their personal data pursuant to the Prüm Treaty and Prüm Decision takes place in accordance with the law. The request shall be made to the Data Protection Ombudsman or to the police in accordance with section 41, subsection 2 of this Act. A request made to the police shall be referred to the Data Protection Ombudsman without delay.

Section 45

The right of the data subject to restriction of processing

Article 18 of the Data Protection Regulation on the right to restriction of processing does not apply to the processing of personal data referred to in this Act.

Chapter 7

Processing of personal data by the Finnish Security and Intelligence Service

Section 46

Scope of application

This chapter lays down provisions on the processing of personal data under section 1, subsection 1 of this Act that are necessary for the performance of the duties of the Finnish Security and Intelligence Service referred to in section 10 of the Act on Police Administration (110/1992).

The provisions of the Criminal Matters Personal Data Act apply to the processing of personal data that are necessary for the performance of the duties of the Finnish Security and Intelligence Service referred to in subsection 1, excluding section 10, subsection 2, section 54 and chapter 7 of the Act, unless otherwise provided in this chapter.

The processing of personal data shall comply with the requirement of respect for fundamental and human rights, the principle of proportionality, the principle of minimum intervention, and the principle of intended purpose laid down in chapter 1 of the Police Act.

The processing of personal data shall not, without an acceptable reason, be based on a person's age, gender, origin, nationality, place of residence, language, religion, conviction, opinion, political activity, trade union activity, family relationships, state of health, disability, sexual orientation, or other reason related to that person.

Provisions on the punishment for a data protection offence are laid down in chapter 38, section 9 of the Criminal Code.

Provisions of the Act on the Openness of Government Activities (621/1999) apply to the non-disclosure of personal data, unless otherwise provided in this chapter.

Section 47
Controller

The controller of the personal data referred to in this chapter is the Finnish Security and Intelligence Service.

Section 48
Processing of personal data by the Finnish Security and Intelligence Service

The Finnish Security and Intelligence Service may only process personal data that are necessary for the protection of national security, prevention, detection and investigation of activities and schemes threatening state or social order or state security, or prevention and detection of offences threatening state or social order or state security.

Separate provisions are issued on the personal data processed for the purpose of security clearances.

Section 49
Processing of basic personal data

The Finnish Security and Intelligence Service may process the following necessary basic personal data referred to in section 48, subsection 1:

1) personal identity code and date of birth;

2) identification data relating to physical characteristics, as well as audio and video recordings;

3) other identification data than those referred to in paragraphs 1 and 2;

4) nationality and family relations;

5) place of residence;

6) education and occupation and work and service history;

7) contact details;

8) information on the person's death or declaration of death;

9) identification data that can be linked to a legal or natural person;

10) information relating to legal persons;

11) essential information relating to travelling;

12) essential information on activities or behaviour of a person.

In addition, the Finnish Security and Intelligence Service may process special categories of personal data that are essential for the performance of their duties.

Section 50
Disclosure of personal data

Notwithstanding non-disclosure provisions, the Finnish Security and Intelligence Service may disclose personal data for the performance of their duties to other authorities or organisations entrusted with a public service task.

Furthermore, notwithstanding non-disclosure provisions, the Finnish Security and Intelligence Service may disclose personal data to other police units for the processing purposes referred to in section 13 and to other authorities or organisations entrusted with a public service task for the purposes referred to in chapter 4. The provisions of chapter 5a, section 44 apply to the disclosure, for the purpose of crime prevention, of data acquired by means of an information gathering method.

The Finnish Security and Intelligence Service may record personal data referred to in subsections 1 and 2 in the filing systems of the police in accordance with section 17.

Notwithstanding non-disclosure provisions, the Finnish Security and Intelligence Service may also disclose in individual cases personal data to private organisations or individuals, if there are serious reasons for this and this is essential for the performance of the duties of the Finnish Security and Intelligence Service.

Section 51
Disclosure of personal data for the purposes of international cooperation

Notwithstanding non-disclosure provisions, the Finnish Security and Intelligence Service may disclose personal data to foreign security and intelligence services or foreign authorities responsible for protecting national security, safeguarding legal and social order, maintaining public order and security, or preventing and investigating offences and referring them for consideration of charges, as well as to the International Criminal Police Organization (Interpol) and the European Union Agency for Law Enforcement Cooperation (Europol), provided that the disclosure is essential for the performance of the duties of the Finnish Security and Intelligence Service.

Notwithstanding non-disclosure provisions, the Finnish Security and Intelligence Service may also disclose the data referred to in subsection 1 to the parties specified in the subsection, provided that the data are essential for the performance of the duties of the relevant foreign authorities.

The Finnish Security and Intelligence Service may disclose personal data to international information systems in accordance with sections 26–29.

When deciding on disclosing data, attention shall also be paid to the human rights situation of the receiving state, the implications of the disclosure for the international relations of Finland, and

international treaties and other obligations binding on Finland. Furthermore, attention shall be paid to the data protection level of the receiving state and the implications of the disclosure for the rights of the data subject.

International cooperation and information exchanges are prohibited where there are reasonable grounds to suspect that a person could be subject to the death penalty, torture, other treatment that violates human dignity, persecution, arbitrary deprivation of liberty or unfair trial on account of such cooperation or information exchange.

Extensive disclosure of special categories of personal data is prohibited.

Where necessary, conditions regarding the intended use of the data and forwarding of the data shall be appended to the disclosed data.

Section 52
Right to obtain information

The Finnish Security and Intelligence Service has the right to obtain the data processed pursuant to chapter 2 that are necessary for the performance of its duties.

The Finnish Security and Intelligence Service has the right to obtain the data referred to in chapter 3 in a manner laid down in the chapter for the performance of its duties. The Finnish Security and Intelligence Service has the right to impose a conditional fine in accordance with section 19.

The Finnish Security and Intelligence Service is entitled to receive the biometric data collected in the context of border control and maintaining border security and order along the border that are essential for safeguarding national security. The data must be retained separately from other information processed by the Finnish Security and Intelligence Service. The data may only be processed to perform a single function under the conditions laid down in this chapter. (1207/2022)

Subsection 3, added by Act 1207/2022, enters into force on a date to be set by decree.

The Finnish Security and Intelligence Service has the right to obtain the information free of charge, unless otherwise provided elsewhere by law.

Section 53

Processing of personal data received in connection with international cooperation

The processing of personal data received from a foreign security and intelligence service shall comply with the conditions set by the provider of the data concerning non-disclosure, the obligation to remain silent, restrictions on the use of the data, forwarding of the data and returning of the disclosed data.

Section 54

Right of the Finnish Security and Intelligence Service to maintain a filing system

Where the controller has the right laid down elsewhere by law to disclose, notwithstanding non-disclosure provisions, personal data contained in its filing system with the aid of a technical interface or as a set of data, the Finnish Security and Intelligence Service may compare the data in the filing system in question with the contents of its own filing systems for the purpose of maintaining its information system. All unnecessary data shall be destroyed immediately after performing the comparison. Unnecessary data may not be recorded.

Where the initial or other than initial purpose of the processing of personal data is national security, the Finnish Security and Intelligence Service also, notwithstanding non-disclosure provisions, has the right to compare within its information system a data set compiled from another information system, provided that this is essential for the processing of data in a high security-level information system. The data set shall be destroyed immediately after the need for the comparison has ended. Data compiled for the purpose of comparison shall be kept separate from other data processed by the Finnish Security and Intelligence Service.

The Finnish Security and Intelligence Service has the right to obtain the information free of charge, unless otherwise provided elsewhere by law.

Section 55

Processing of personal data for purposes other than the initial purpose

In addition to the provisions laid down in section 5, subsection 3 of the Criminal Matters Personal Data Act, notwithstanding non-disclosure provisions, information in the information system of the

Finnish Security and Intelligence Service may also be processed for oversight of legality, planning and development activities. Such data may also be used in training activities if the data are essential for carrying out the training.

Section 56
Limitations to the right of access

The right of access by the data subject does not apply to the personal data processed by the Finnish Security and Intelligence Service pursuant to this chapter.

Provisions on the exercise of the rights of the data subject through the Data Protection Ombudsman are laid down in section 29 of the Criminal Matters Personal Data Act. The request relating to the exercise of the rights shall be made to the Data Protection Ombudsman or to the police in accordance with section 41, subsection 2 of this Act. A request made to the police shall be referred to the Data Protection Ombudsman without delay.

Section 57
Erasure of information

The personal data referred to in section 48 and subsection 1 are erased no later than 25 years after making the last entry, unless there are special reasons to retain the data. The necessity of retaining personal data shall be reviewed at least every five years.

The information recorded in accordance with section 52, subsection 3 shall be erased in accordance with the provisions of section 40, subsection 2, paragraph 5a of the Act on the Processing of Personal Data by the Border Guard. (1207/2022)

Subsection 2, added by Act 1207/2022, enters into force on a date to be set by decree.

Section 58
Data found to be incorrect

Data 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 Finnish Security and Intelligence Service. Such data may only be used for the stated purpose.

Any data found to be incorrect and retained pursuant to subsection 1 shall be erased immediately once the storing of the data is no longer necessary to ensure the relevant rights.

Section 59
Archiving information

Separate provisions are issued on archiving duties and documents to be archived.

Chapter 8
Miscellaneous provisions

Section 60 (818/2022)
Controller

The controller of the personal data referred to in chapter 2 and of the National Schengen Information System, and the N.SIS Office referred to in the SIS Regulations is the National Police Board.

Section 61
Entry into force

This Act enters into force on 1 June 2019.

This Act repeals the Act on the Processing of Personal Data by the Police (761/2003), hereafter the Repealed Act.

The provisions in force at the time of the entry into force of this Act may be applied to the erasure of the personal data referred to in this Act for a period of four years of the entry into force of the Act. During the transitional period, sections 23, 24 and 26 of the Repealed Act apply to the erasure of the personal data referred to in sections 7, 8, 11 and 12, as set out in the provisions in force at the time of the entry into force of this Act. During the same period, section 22 of the Repealed Act applies to the erasure of the personal data referred to in sections 5 and 6, as set out in the provisions in force in acts 529/2005 and 851/2006.