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

Act on the Processing of Personal Data by the Border Guard (639/2019)

By decision of Parliament, the following is enacted:

Chapter 1
General provisions

Section 1
Scope of application

Unless otherwise provided elsewhere by law, this Act applies to the processing of personal data for the performance of the duties laid down for the Border Guard, 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.

In addition to what is provided elsewhere by law, this Act also lays down provisions on the right of the Border Guard to obtain data from authorities and private organisations and persons.

Section 2
Relationship with other legislation

Provisions on the processing of personal data are 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).

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, safeguarding against threats to public security and preventing such threats, protecting national security, and in military administration of justice;

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.

Section 3
Principles to be complied in the processing of personal data and prohibition of discrimination

The processing of personal data shall comply with the principle of proportionality, the principle of minimum intervention, the principle of intended purpose and the requirement of respect for fundamental and human rights laid down in chapter 2 of the Border Guard 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.

Section 4
Processing of data belonging to special categories of personal data

The Border Guard may process data belonging to special categories of personal data only if the processing is strictly necessary for the purpose of the processing.

Section 5
Definitions

In this this Act:

1) *maintenance of border security* means the measures taken in Finland and abroad to prevent breaches of provisions on crossing the national or external border;

2) *maintaining order along the border* means implementing and supervising compliance with provisions on the national border and border crossing points and provisions on international cooperation between border authorities;

3) *Schengen Borders Code* means Regulation (EC) 2016/399 of the European Parliament and of the Council establishing a Community Code on the rules governing the movement of persons across borders;

4) *legislative basis for the Schengen Information System* means Regulation (EC) No 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II), Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II), and Regulation (EC) No 1986/2006 of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates;

5) *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.

Chapter 2
Processing of personal data

Section 6
Processing of basic personal data

The Border Guard may process the following basic personal data for the purposes laid down in sections 7, 8, 10, 12, 13 and 15:

1) names;

2) personal identity code;

3) gender;

4) date and place of birth;

5) citizenship or lack of citizenship and nationality;

6) native language;

7) communication language;

8) civil status;

9) domicile and place of residence;

10) occupation and education;

11) information on conscription and service;

12) contact details;

13) information in the documentation necessary to establish identity;

14) customer number issued by the authorities;

15) travel document information and other information concerning border-crossing;

16) in the case of foreign nationals, the names, citizenship, nationality and contact details of the parents;

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

18) information on guardianship, declaration of bankruptcy or imposition of a business prohibition.

Section 7

Processing of personal data in border control and to maintain border security and order along the border

The Border Guard may process personal data to carry out border control laid down in the Schengen Borders Code, to maintain border security and order along the border and to conduct an investigation referred to in section 27 of the Border Guard Act.

In performing a duty referred to in subsection 1, the Border Guard may, in addition to the basic personal data referred to in section 6, also process the following personal data:

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

2) the information referred to in Annex II of the Schengen Borders Code;

3) the recordings of the technical monitoring referred to in section 29 of the Border Guard Act;

4) information on the movements and location of persons and vehicles in the vicinity of the border and on passengers and crew in cross-border passenger transport;

5) information for imposing a financial penalty on a carrier;

6) information for handling a matter relating to a border zone permit and a border crossing permit;

7) border zone notifications and other notifications submitted to the Border Guard;

8) information on the operation and composition of the border control authorities of other states and the border situation in Finland and in the European Union;

9) personal identifying characteristics to establish identity, including facial images;

10) 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.

Section 8

Processing of personal data for the purpose of investigating offences and maintaining public order and security

The Border Guard may process personal data for the purpose of performing a duty relating to investigating an offence or referring a case for consideration of charges and for maintaining public order and security.

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 or an action by the Border Guard;

4) reporting an offence or is an injured party;

5) a witness;

6) a victim;

7) some other source of information relating to the duty.

The data received in connection with the performance of the duties of the Border Guard 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 16, subsection 1.

Section 9

Contents of personal data that are processed for the purpose of investigating offences and maintaining public order and security

In addition to the basic personal data referred to in section 6, the Border Guard may also process the following personal data concerning the persons referred to in section 8:

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

2) personal identifying characteristics to establish identity, including fingerprints, handprints and footprints, handwriting, voice and odour samples, DNA profiles, facial images and other biometric data;

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 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;

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

Section 10
Processing of personal data for the purpose of preventing and detecting offences

The Border Guard 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; or

3) who are subjects of the surveillance referred to in section 21 of the Act on Crime Prevention by the Border Guard (108/2018) or other action by the Border Guard.

The Border Guard may also process the data referred to in subsection 1 concerning a witness, a victim and an injured party of an offence and persons reporting an offence or other observation if this is essential for the prevention or detection of an offence.

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

In addition, the Border Guard may process information on observations made by border guards and information reported to the Border Guard 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 the duties of the Border Guard 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 16, subsection 1.

Section 11
Contents of personal data that are processed for the purpose of prevention and detection of offences

In addition to the basic personal data referred to in section 6, the Border Guard may also process the following personal data concerning the persons referred to in section 10:

1) specifications, descriptions and classifications relating to Border Guard 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.

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 12
Processing of data of covert human intelligence sources

In addition to the basic personal data referred to in section 6 of this Act, the Border Guard may also process the following personal data concerning the persons specified in section 36 of the Act on Crime Prevention by the Border Guard:

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 13
Processing of personal data in military administration of justice

The Border Guard may process personal data to perform a duty relating to the criminal investigation or military discipline procedure (*military administration of justice*) referred to in section 31, subsection 3 of the Act on the Administration of the Border Guard (577/2005).

It is further required that the data referred to in subsection 1 are connected to a person who is or has been subject to criminal investigation or coercive measures or who acts as an informant, witness, injured party or other person to be heard.

Section 14

Contents of the personal data processed in military administration of justice

In addition to the basic personal data referred to in section 6, the Border Guard may also process the following personal data concerning the persons specified in section 13:

1) specification, descriptions and classifications relating to Border Guard duties, actions or operations;

2) personal identifying characteristics to establish identity, including voice samples and facial images;

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 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;

4) information on military discipline decisions and on matters considered by the prosecutor and the court as military court cases, information on the service of and request for a review of a decision or a sentence and information on the enforcement of the sanction;

5) information concerning the supervision of the military discipline procedure.

Section 15
Processing of personal data in other statutory duties of the Border Guard

The Border Guard may process personal data to perform its statutory duties relating to surveillance, customs, search, rescue and emergency medical care and other statutory duties of the Border Guard.

In addition to the basic personal data referred to in section 6, the Border Guard may also process the following personal data when performing the duties specified in subsection 1:

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

2) information on maritime traffic and the location of vessels;

3) information on administrative sanctions;

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.

Section 16
Processing of personal data for purposes other than the initial purpose

Unless otherwise provided elsewhere by law, the Border Guard may process the personal data referred to in sections 7–11 and 13–15 for the following purposes which are other than their 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) 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) carrying out border control laid down in the Schengen Borders Code;

8) determination of the fitness for service and the planning and arrangement of service;

9) placement in emergency conditions or preparedness;

10) military rank promotions or rewards;

11) establishing identity in the performance of a Border Guard action in which the establishment of identity is essential;

12) directing Border Guard operations.

Data in the filing system of the Border Guard may, notwithstanding secrecy provisions, 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.

Section 17
Processing of personal data for purposes other than the initial purpose in the consideration of permits and licences

Unless otherwise provided elsewhere by law, the Border Guard may process the personal data referred to in sections 7–9 and 13–15 for purposes other than their 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 reliability, 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.

Section 18
Controller

The controller of the personal data referred to in this Act is the Border Guard Headquarters.

Chapter 3
Right to obtain information

Section 19
Right to obtain information from public authorities

Notwithstanding secrecy obligation, the Border Guard has the right to obtain any information and documents from a public authority, and a body or a person entrusted with a public service task that are necessary to carry out an official duty unless disclosure of such information or documents to the Border Guard or use of such information as evidence is prohibited or restricted by law.

The decision on obtaining confidential information is made by an official with the power of arrest unless otherwise agreed upon with the party who disclosed the information.

Section 20
Right to obtain information from a private organisation or person

At the request of a border guard with the power of arrest, the Border Guard has the right to obtain information for the purpose of preventing, detecting or investigating an offence investigated by the Border Guard, notwithstanding business, banking or insurance secrecy binding on members, auditors, managing directors, board members and employees of an organisation. The Border Guard has the same right to obtain information needed in an investigation referred to in section 27 of the Border Guard Act if an important public or private interest so requires.

In individual cases and on request of an official with the power of arrest, the Border Guard has the right to obtain from a telecommunications operator and a corporate or association subscriber contact information on a network address that is not listed in a public directory or data identifying a network address or terminal equipment to perform a Border Guard duty. Similarly, the Border Guard has the right to obtain postal address information from organisations engaged in postal services.

For licence administration purposes, the Border Guard has the right to obtain information from private organisations and persons as provided in section 19.

Section 21
Conditional fine

The Border Guard may obligate a party to disclose the information referred to in section 20 within a reasonable time if the information is necessary to prevent or investigate an offence investigated by the Border Guard. The Border Guard 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 22

Right to obtain information contained in certain registers and information systems

Notwithstanding secrecy provisions, the Border Guard has the right, in addition to what is laid down elsewhere by law, to obtain information as follows for the purpose of carrying out its duties:

1) from maritime authorities and vessel traffic service providers, information on maritime traffic, its surveillance and the location of vessels from the maritime surveillance information systems, the ship reporting system, the port traffic information systems and other vessel traffic information systems to perform the surveillance duty at sea laid down for the Border Guard;

2) from aviation, fishing, maritime, environmental and rescue authorities and from the police, Customs and the Defence Forces, information on vehicles, traffic, operational preparedness of the authorities and their alerting for the purposes of the maintenance of border security, rescue duties or for the performance of the surveillance duty at sea or on the land border laid down for the Border Guard;

3) from the emergency response centre data system, information to ensure a person's own safety or the occupational safety of a Border Guard official in connection with the performance of a statutory duty of the Border Guard;

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 border management, criminal investigation, other investigation, a rescue duty, a task referred to in the Act on the Security of Certain Ships and Associated Port Facilities and on Monitoring Maritime Security (485/2004) and to impose a financial penalty on a carrier and an oil discharge fee;

5) 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;

6) from the information systems of the Ministry for Foreign Affairs, information on members of the staff of diplomatic and consular missions representing their sending state in Finland, bodies of international organisations in Finland and international bodies in similar positions and members of their families and persons privately employed by them, for the purposes of the maintenance of border security, criminal investigation and other investigation and for the performance of duties laid down for the Border Guard in the Aliens Act;

7) from the surveillance information system referred to in section 29 of the Act on the Sanction System and Surveillance of Common Fisheries Policy (1188/2014), information for fishing supervision, waterway transport surveillance, border management, criminal investigation, other investigation, a rescue duty, a task referred to in the Act on the Security of Certain Ships and Associated Port Facilities and on Monitoring Maritime Security and to impose a financial penalty on a carrier;

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

9) from organisations and corporations, information on passengers and personnel of a vehicle for a task to be carried out in the cooperation referred to in the Act on Cooperation between the Police, Customs and the Border Guard (687/2009); provisions on the right to obtain information from air carriers' passenger name records 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).

Section 23

Disclosure of data from other authorities to the Border Guard by depositing online

The Border Guard may authorise the following authorities to disclose data by depositing them online in its filing system:

1) judicial administration authorities, the Criminal Sanctions Agency and the Legal Register Centre;

2) the police, Customs and the Defence Forces;

3) the Foreign Service of Finland.

Section 24
Information on persons in a vehicle crossing the external border

Notwithstanding secrecy provisions, the Border Guard has the right to obtain and process information concerning the passengers of organisations and corporations and the personnel of vehicles for the purpose of carrying out border control and maintaining border security.

The driver of a vehicle entering or leaving the country and crossing the external border shall submit to the border control authorities of the point of entry or exit information on the persons in the vehicle. The captain of a ship or an aircraft, and the owner or holder of a train or another means of transport, or their representative shall submit to the border control authorities of the point of entry or exit the passenger and crew list, or in some other manner information on the personnel, passengers and other persons in the means of transport, unless the information has already been submitted under section 25 or 26.

The passenger and crew list shall state the last and first names of each person entered in the list, their date of birth, gender and nationality, and the nationality and registration information of the means of transport and the place of arrival and departure.

The information referred to in subsections 2 and 3 shall be submitted also for traffic crossing internal borders if border control has been temporarily reintroduced at the internal borders in accordance with Title III, Chapter 2 of the Schengen Borders Code or section 15 of the Border Guard Act.

Section 25
Air passenger data

In addition to the provisions in section 24, natural persons and legal person whose professional it is to provide passenger transport by air shall submit to border control authorities, at their request, information referred to in this section on passengers whom they carry to an authorised border

crossing point through which these persons enter or leave the territory of European Union Member States (*air passenger data).*

The air passenger data shall include the number and type of the travel document used by the passenger, his or her citizenship or lack thereof, full name, date of birth, the border crossing point of entry into or exit from the territory of European Union Member States, the code of transport and its departure and arrival times, the total number of passengers carried on that transport and the initial point of embarkation. The data shall be submitted immediately after check-in closure. The data shall be submitted electronically or, if this is not possible, by any other appropriate means.

This section also applies to traffic crossing internal borders if border control has been temporarily reintroduced at the internal borders in accordance with Title III, Chapter 2 of the Schengen Borders Code or section 15 of the Border Guard Act.

Section 26
Passenger and crew data in vessel and rail transport

Natural persons and legal persons who professionally carry out passenger or goods transport by ship or by rail shall submit to border control authorities the data on passengers and crew referred to in section 24, subsections 2 and 3 prior to arrival at border check.

In rail transport, the data shall be submitted no later than when the train has departed from the last station at which it has taken on passengers. The provisions of the Schengen Borders Code and other statutes apply to the obligation to submit information on vessel traffic in advance.

This section also applies to traffic crossing internal borders if border control has been temporarily reintroduced at the internal borders in accordance with Title III, Chapter 2 of the Schengen Borders Code or section 15 of the Border Guard Act.

Section 27
Processing of passenger and crew data

The passenger and crew data referred to in sections 24–26 may be processed to facilitate border checks and to combat illegal entry and illegal immigration. The data may also be processed in another duty laid down for the Border Guard, the police or Customs.

In connection with the processing referred to in subsection 1, the passenger and crew data may be compared to registers and databases necessary for the processing.

Section 28
Sanctions

Provisions on the financial penalty to be imposed on carriers who violate their obligation under sections 25 and 26 are laid down in section 179 of the Aliens Act.

Provisions on a violation of the Aliens Act are laid down in section 185 of the Aliens Act.

Section 29
Transfer of the data to the Border Guard

The Border Guard has the right of access to the data referred to in this chapter free of charge, unless otherwise provided by law. This data may also be accessed with the aid of a technical interface or as a set of data as agreed upon with the controller on the practical procedure.

The Border Guard shall, on request, submit to the controller who disclosed the personal data information regarding the processing of personal data it has accessed with the aid of a technical interface, as a set of data or online.

Section 30
European Union Visa Information System

Provisions on the right of the Border Guard to obtain data contained in the Visa Information System of the European Union are laid down in 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).

Provisions on the right of the Border Guard to obtain data contained in the Visa Information System of the European Union for the purpose of preventing and investigating offences to be investigated by the Border Guard that are referred to in section 3, subsection 2 of the Act on Extradition on the Basis of an Offence between Finland and Other Member States of the European Union (1286/2003) are laid down in 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 the prevention, detection and investigation of terrorist offences and of other serious criminal offences. The data shall be requested via the Border Guard Headquarters.

Section 31
Processing of personal data received in connection with international cooperation

The processing of data received from a third country or an international organisation or agency shall comply with the conditions set by the provider of the data concerning secrecy, non-disclosure, 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 Border Guard may process the disclosed data for purposes other than those for which they were disclosed in compliance with section 16, subsection 1.

Chapter 4
Disclosure of personal data

Section 32
Disclosure of personal data to another competent authority referred to in the Criminal Matters Personal Data Act

Notwithstanding secrecy provisions, the Border Guard may, with the aid of a technical interface or as a set of data, disclose personal data referred to in sections 7–15 to the police, Customs, the Defence Forces, 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 33

Other disclosure of personal data to authorities

Notwithstanding secrecy provisions, and in addition to what is provided elsewhere by law, the Border Guard may, with the aid of a technical interface or as a set of data, disclose personal data referred to in sections 7–15 for the performance of a statutory duty of the authorities as follows:

1) to the police for performing border checks, for purposes corresponding to the initial purpose for processing personal data and for other purposes in cases referred to in section 13 and section 14, subsection 1 of the Act on the Processing of Personal Data by the Police (616/2019);

2) to Customs for customs control, tax supervision, performance of border checks and for serving summonses and other notifications, for purposes corresponding to the initial purpose for processing personal data and for other purposes in cases referred to in section 15 of the Act on the Processing of Personal Data by Customs;

3) to rescue authorities for carrying out rescue operations;

4) to the Emergency Response Centre Agency for performing the duties laid down in the Act on Emergency Response Centre Operations (692/2010), for ensuring initial measures or occupational safety, or for supporting the unit in question, taking into account the provisions of the said Act concerning restrictions on the right to obtain information;

5) to the Finnish Transport and Communications Agency, information in accordance with sections 197 and 217 of the Act on Transport Services (320/2017) that is essential for the performance of its statutory duties;

6) to the Finnish Transport Infrastructure Agency for vessel traffic management;

7) to environmental authorities for tasks concerning the prevention of pollution of waters from ships and supervision of marine protection;

8) 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;

9) 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;

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

11) to social welfare authorities for considering matters concerning the means of support of an alien or for arranging his or her social welfare or healthcare;

12) to enforcement officers in accordance with chapter 3, section 67 of the Enforcement Code (705/2007) for attending to enforcement matters;

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

Notwithstanding secrecy provisions, and in addition to what is provided in subsection 1, the Border Guard may, on justifiable grounds, , with the aid of a technical interface or as a set of data, disclose to an authority personal data that are essential for the performance of a statutory duty of the authority.

Section 34
Disclosure of personal data via a public information network

Notwithstanding secrecy provisions, the Border Guard may, via a public information network and for the purpose of informing the general public and receiving leads from the public, disclose personal data where this is especially necessary for the purpose of providing information as a result of the urgency of the matter, a dangerous situation, crime prevention, returning property to its owner, maintaining border security or for investigative reasons. Personal data may be disclosed only if this is materially important to perform a statutory duty of the Border Guard and the disclosure of the data does not conflict with a legitimate interest of the data subject. Personal data received from another authority may only be disclosed with the consent of the authority that disclosed the data.

Section 35

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

Notwithstanding secrecy provisions, the Border Guard may disclose personal data referred to in sections 7–15 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 Border Guard may process the said personal data.

Notwithstanding secrecy provisions, the Border Guard may also disclose personal data referred to in sections 7–15 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.

In addition to the provisions of this Act and 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 36

Disclosure of personal data in European Union border control cooperation

Notwithstanding secrecy provisions, the Border Guard may disclose the personal data referred to in sections 7–11 and 15 to:

1) an authority responsible for the border control of another Member State of the European Union and of another country applying the Schengen Borders Code for carrying out border control;

2) the European Border and Coast Guard Agency, liaison officers of the Agency and an official of a Member State participating in an operation or in a pilot project in Finland coordinated by the Agency in compliance with the provisions of Regulation (EU) 2016/1624 of the European Parliament and of the Council on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC;

3) an official of a Member State of the European Union providing border security assistance referred to in section 15d, subsection 1 of the Border Guard Act for performing the actions required by the request for assistance presented by Finland.

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

Section 37
Certain international information systems

Notwithstanding secrecy provisions, the Border Guard may disclose personal data to be recorded in the Schengen Information System (SIS) that are necessary for the purposes laid down in the legislative basis for the SIS. The supplementary information referred to in the legislative basis for the SIS shall be supplied via the National Bureau of Investigation. The information may also be disclosed as a set of data.

Notwithstanding secrecy provisions, the Border Guard 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 38
Other disclosure of data abroad

Notwithstanding secrecy provisions, the Border Guard may disclose personal data in compliance with chapter 7 of the Criminal Matters Personal Data Act.

Notwithstanding secrecy provisions, the Border Guard may disclose the personal data referred to in sections 7–11 and 15 to:

1) the authorities referred to in the agreement concerning the régime of the Finnish-Soviet State Frontier and the procedure for the settlement of frontier incidents (Finnish Treaty Series 32/1960) for carrying out the duties referred to in the agreement;

2) an authority responsible for the border control of another state if the data are essential to perform border control;

3) the competent authorities referred to in international obligations or arrangements on the readmission of persons entering the country and residing there without authorisation for carrying out the duties referred to in the said international obligations or arrangements.

Notwithstanding secrecy provisions, the Border Guard may disclose personal data relating to the acquisition, possession, transfer, import and export of firearms, firearm components, cartridges and specially dangerous projectiles to an arms control authority of another state provided that the disclosure of the data is essential for arms control.

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

Section 39
Disclosure procedure

The controller or some other administrative unit assigned by the controller to carry out this duty decides on the disclosure of the personal data referred to in this Act if the disclosure takes place with the aid of a technical interface or as a set of data or if it involves disclosure of other than individual data abroad.

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. Prior to the disclosure of personal data with the aid of a technical interface or as a set of data, the recipient shall provide the controller with a reliable report on the appropriate protection of the data.

The quality of the data to be disclosed shall be verified and, where possible, the data shall be supplemented with 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.

Chapter 5
Erasure and archiving of personal data

Section 40
Erasure of personal data processed in border control and for the purpose of the maintenance of border security and order along the border

The personal data processed in border control and for the purpose of the maintenance of border security and order along the border are erased at the latest five years after the latest entry of data.

By derogation from subsection 1:

1) permit or licence data are erased ten years after the expiry of the permit or licence;

2) notification data are erased ten years after the entry of the data in the filing system;

3) the recordings of technical monitoring referred to in section 29 of the Border Guard Act are erased at the latest six months after the recording was made;

4) data on the imposition of a financial penalty on a carrier are erased ten years after their entry in the filing system;

5) data on an entry ban are erased three years after the withdrawal or termination of the ban;

6) data referred to in section 7, subsection 2, paragraph 8 are erased 25 years after the last entry of data;

7) data referred to in section 7, subsection 2, paragraph 10 are erased at the latest one year after the death of the data subject.

However, personal data referred to in subsections 1 and 2 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 Border Guard. The necessity of retaining personal data shall be reviewed at least every five years.

Section 41
Erasure of air passenger data

The air passenger data referred to in section 25 are erased at the latest 24 hours after they were submitted to the border check authorities after the passengers have entered or left the country unless the data are needed in another statutory duty of the Border Guard, the police or Customs. The provisions of the Act on the Use of Air Carriers' Passenger Name Record Data in the Prevention of Terrorist Offences and Serious Crime also apply to the processing of air passenger data after 24 hours.

Unless otherwise provided, the party disclosing the air passenger data referred to in section 25 shall destroy the personal data it has acquired and submitted to the border check authorities at the latest 24 hours after the means of transport used has arrived at its destination.

Section 42
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 a maximum 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 severe punishment for the most serious 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 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 Border Guard. The necessity of retaining personal data shall be reviewed at least every five years.

Section 43

Erasure of other personal data processed for the purpose of investigating offences and erasure of personal data processed for the purpose of maintaining public order and security

Personal data processed for the purpose of investigating offences other than those referred to in section 42 and personal data processed for the purpose of maintaining public order and security

are erased five years after the recording of a notification or matter unless they are connected to a criminal matter under investigation.

By derogation from subsection 1:

1) data processed for finding, monitoring, surveillance or protection of individuals concerning a warrant of apprehension or a travel ban are erased three years after the cancellation or expiry of the warrant or ban;

2) the data referred to in section 9, subsection 3 are erased no later than one year after the death of the data subject.

However, the personal data referred to in subsections 1 and 2 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 Border Guard. The necessity of retaining personal data shall be reviewed at least every five years.

Section 44
Erasure of personal data processed for the purpose of preventing and detecting offences

Personal data processed for the purpose of preventing and detecting offences are erased no later than ten years after the last entry of data concerning an offence, criminal activity or action. The data referred to in section 10, subsection 5 are, however, erased no later than six months after making the entry and the data referred to in section 11, subsection 1, paragraph 4 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 Border Guard. The necessity of retaining personal data shall be reviewed at least every five years.

Section 45
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 46
Erasure of personal data processed in military administration of justice

Of personal data processed in military administration of justice, the following are erased:

1) data concerning an admonition, extra duty and confinement to barracks not exceeding ten days, three years after the disciplinary punishment was sentenced or imposed unless the said party has during this period been sentenced by a decision of a court or in disciplinary proceedings;

2) data concerning a warning, confinement to barracks exceeding ten days, disciplinary fine and detention, five years after the disciplinary punishment was sentenced or imposed unless the said party has during this period been sentenced by a decision of a court or in disciplinary proceedings.

Data on a sentence imposed by a court in military court procedure are erased in compliance with the provisions of section 10 of the Criminal Records Act (770/1993) and section 52 of the Act on the Enforcement of Fines.

If a person has been punished by a decision of a court or in disciplinary proceedings more than once, the data are erased five years after the last disciplinary punishment.

Personal data relating to criminal investigation processed in military administration of justice are erased no later than:

1) one year after the expiration of the limitation period for bringing charges for the offence if the said expiry period is more than ten years;

2) one year after the controller has received information on a decision of the prosecutor not to take measures to bring charges against the person who has committed an offence or on a decision of the prosecutor that no offence has been committed or that there is no evidence of an offence;

3) one year after the controller has received information on a decision of the prosecutor that the offence has become time-barred;

4) one year after the controller has received information that the charge has been finally dismissed or the charge brought has been dismissed due to time-barring;

5) one year after the death of the suspect of an offence;

6) ten years after the last entry.

The data referred to in section 14, subsection 3 processed in military administration of justice are erased no later than one year after the death of the data subject.

Section 47
Erasure of other personal data

The personal data referred to in section 15 are erased five years after their entry in the filing system unless there are special reasons for their retaining for investigative, surveillance or other justified reasons or to ensure the rights of the data subject, other parties or employees of the Border Guard. The necessity of retaining personal data shall be reviewed at least every five years.

By derogation from subsection 1:

1) data on aliens detained are erased five years after the last entry of data related to the person in question;

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

3) the data referred to in section 15, subsection 2, paragraph 4 are erased no later than one year after the death of the data subject.

Section 48
Data found to be incorrect

Notwithstanding the provisions of the Data Protection Regulation and the Criminal Matters Personal Data Act on the rectification of incorrect data in filing systems, any data that are found to

be incorrect may be retained with the rectified data if this is necessary to ensure the rights of the data subject, other parties or employees of the Border Guard. Such data may only be used for the stated purpose.

Any data found to be incorrect and retained under subsection 1 shall be erased once the retaining of the data is no longer necessary to ensure the rights.

Section 49
Archiving information

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

Chapter 6
Rights of data subjects

Section 50
Implementing the right of access of the data subject

In order to implement the right of access by the data subject referred to in Article 15 of the Data Protection Regulation and the right of access of the data subject referred to in section 23 of the Criminal Matters Personal Data Act, the controller or another authority ordered by it provides access to the data.

The data subject shall, when exercising his or her right of access, make a request to this effect in person to the controller or to another authority 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 51
Limitations to the right of access

By derogation from section 23 of the Criminal Matters Personal Data Act and in addition to the provisions of section 28 of the said Act, the data subject does not have the right of access to:

1) the personal data referred to in section 12;

2) information concerning the tactical and technical methods of the Border Guard, 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 8–11.

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, the controller or to another authority referred to in section 50, subsection 1 of this Act as provided in subsection 2 of the said section. A request made to the controller or the other authority shall be referred to the Data Protection Ombudsman without delay.

Section 52
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
Miscellaneous provisions

Section 53
An electronic identifier based on the physical characteristics of a person

To identify a person and to verify the authenticity of a document, the Border Guard has the right, unless otherwise provided, to accept an electronic identifier which is based on the physical characteristics of a person and which is attached to a travel document.

The Border Guard has the right to compare the identifier in the document with the person. An electronic identifier may not be recorded unless otherwise provided.

Section 54
Penal provision

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

Section 55
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 Border Guard (579/2005).

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 this Act. During the said period, the provisions of section 61, subsection 3 of the Act on the Processing of Personal Data by the Police on the erasure of personal data referred to in sections 5 and 6 of the said Act apply, however, to erasure of personal data referred to in sections 8 and 9 of this Act.