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

Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security

(1054/2018; amendments up to 1226/2023 included)

By decision of Parliament, the following is enacted:

Chapter 1
General provisions

Section 1
Scope of application

This Act applies to the processing of personal data by competent authorities in the context of

1) preventing, detecting or investigating criminal offences or referring them for consideration of charges;

2) consideration of charges and other activities of a prosecutor in relation to a criminal offence;

3) hearing a criminal case in court;

4) enforcing a criminal sanction;

5) safeguarding against, and preventing threats to, public security in connection with activities referred to in paragraphs 1–4.

In addition to what is provided in subsection 1, this Act applies to

1) the processing of personal data by and on behalf of the Defence Forces, when the data are being processed for performing duties laid down in section 2, subsection 1, paragraph 1; paragraph 2, subparagraph a; and paragraphs 3 and 4 of the Act on the Defence Forces

(551/2007), and to the processing of personal data by the Defence Command for the purpose of performing duties laid down in section 9, subsection 3 of the Security Clearance Act (726/2014); (350/2020)

2) the processing of personal data by the police, when the data are being processed in performing such a duty referred to in chapter 1, section 1, subsection 1 of the Police Act (872/2011) that is related to the protection of national security, and in performing duties referred to in section 9, subsection 1 of the Security Clearance Act; (350/2020)

3) the processing of personal data by the Border Guard, when the data are being processed in performing such a duty referred to in section 3, subsections 2 and 3 of the Border Guard Act (578/2005) that is related to the protection of national security.

However, section 54 on mutual assistance with another EU Member State does not apply to the processing of personal data referred to in subsection 2. (903/2020)

This Act applies to the processing of personal data referred to in subsections 1 and 2, however, only if the processing is wholly or partly automated or if the data to be processed form, or are intended to form, a filing system or part of it.

This Act implements 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, hereafter *the Law Enforcement Directive*.

Section 2
Relationship to other legislation

If another Act contains provisions that derogate from those of this Act, the provisions of the other Act shall prevail over those of this Act.

The provisions on the openness of government activities apply to the right of access to data and to other disclosure of personal data from a filing system of a public authority.

Section 3
Definitions

In this Act,

1) *personal data* means any information relating directly or indirectly to an identified or identifiable natural person (*data subject*);

2) *processing* means collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction and any other operation or set of operations which is performed on personal data or on sets of personal data;

3) *restriction of processing* means the marking of stored personal data with the aim of limiting their processing in the future;

4) *filing system* means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

5) *competent authority* means any public authority competent for the prevention, detection, investigation, referral for consideration of charges, consideration of charges or other activities relating to the prosecution of criminal offences, conviction and sentencing or the execution of criminal penalties, including safeguarding against and preventing threats to public security, as well as the Defence Forces, the police and the Border Guard when performing duties referred to in section 1, subsection 2;

6) *controller* means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data or which is by law responsible for maintaining the filing system;

7) *processor* means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

8) *recipient* means a natural or legal person, public authority, agency or another body to which personal data are disclosed;

9) *personal data breach* means a breach of data security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transferred, stored or otherwise processed;

10) *appropriate safeguards* means technical or organisational measures to ensure the lawfulness of the processing of personal data taking into account the nature, scope, context and purposes of the processing and the risks to the rights of the data subjects;

11) *profiling* means any automated processing of personal data consisting of the use of personal data to evaluate personal aspects relating to a natural person;

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

13) *biometric data* means personal data resulting from technical processing relating to the physical, physiological or behavioural characteristics of a natural person, and allowing or confirming the unique identification of that natural person;

14) *data concerning health* means personal data related to the physical or mental health of a natural person which reveal information about their health status;

15) *third country* means any state which is not a Member State of the European Union (EU) or of the European Economic Area or Switzerland;

16) *international organisation* means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more states.

The provisions of this Act on a competent authority also apply to a private entity performing a duty referred to in subsection 1, paragraph 5.

The provisions of this Act on an EU Member State also apply to the Member States of the European Economic Area and to Switzerland.

Chapter 2
Principles relating to processing of personal data

Section 4
Requirement of lawfulness

Personal data may be processed only if it is necessary for performing a duty that is provided by law for a competent authority and that falls within the scope of section 1, subsection 1 or 2.

Personal data shall be processed fairly and carefully.

Section 5
Purpose limitation

The controller may collect personal data only for specified, explicit and legitimate purposes and shall not process them in a manner that is incompatible with those purposes.

Personal data collected for a purpose provided in section 1, subsection 1 or 2 may be processed for another purpose only if such processing is provided by law.

Personal data may be processed for a purpose provided in section 1, subsection 1 or 2 also for archiving purposes in the public interest or for scientific, statistical or historical purposes if appropriate safeguards exist for the rights of the data subject.

Section 6
Requirement of necessity

Personal data to be processed shall be adequate and necessary in relation to the purposes of the processing, and they shall not be too comprehensive for the purposes of the processing. Any unnecessary personal data shall be erased without undue delay.

Personal data may not be kept in a form that permits identification of the data subject any longer than is necessary for the purposes of their processing.

The necessity of storing personal data shall be reviewed at least every five years, unless otherwise provided elsewhere by law on the time limit for storing personal data.

Section 7
Requirement of accuracy

Personal data to be processed shall be accurate and, having regard to the purposes for which they are processed, up to date. The controller shall make sure that all reasonable measures have been taken to ensure the erasure or rectification without delay of any data that is inaccurate for the purposes of the processing.

Section 8
Distinction between certain personal data

The controller shall, where applicable and as far as possible, make a clear distinction between personal data concerning data subjects with different status in relation to the matter to be considered.

All reasonable measures shall be taken to distinguish personal data based on facts from personal data based on personal assessments.

Section 9
Verification of quality of personal data to be transferred or made available

The competent authority shall take all reasonable measures to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transferred or made available.

As far as possible, all personal data to be transferred shall be accompanied with the necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of the personal data, and the extent to which they are up to date.

If it emerges that incorrect personal data have been transferred or that personal data have been

unlawfully transferred, the recipient shall be notified without delay. After being notified of the matter, the recipient shall rectify or erase the personal data or restrict their processing.

Section 10
Obligation to provide information on specific processing conditions

If the processing of personal data is subject to specific conditions provided by law, the competent authority shall, in connection with the disclosure or transfer of personal data, inform the recipient of the specific conditions and the obligation to comply with them.

When the competent authority transfers personal data to a recipient located within the EU, it shall not impose stricter conditions for the processing of the data than those applied nationally to similar transfers of data.

Section 11
Processing of special categories of personal data

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

The processing of personal data referred to in subsection 1 is allowed only where it is strictly necessary, subject to appropriate safeguards for the rights of the data subject, and only where the processing

1) is provided by law;

2) relates to the consideration of a criminal case in the prosecution service or in court;

3) is necessary for protecting a vital interest of the data subject or of another natural person; or

4) relates to data which the data subject has manifestly made public.

Profiling that results in discrimination against natural persons on the basis of special categories of personal data is prohibited.

Section 12 (1226/2023)
Processing of personal identity codes

A personal identity code may be processed if it is important to uniquely distinguish a data subject and the data subject's personal data from other data subjects and their personal data (*unique identification*):

1) to perform a statutory duty of the competent authority;

2) to implement the rights or obligations of the data subject or the controller; or

3) for historical or scientific research purposes or statistical purposes referred to in section 5, subsection 3.

A personal identity code shall not be unnecessarily entered into documents printed out from or drawn up based on a filing system.

The personal identity code alone or a combination of the personal identity code and the name of a data subject shall not be used for the purpose of establishing the identity of the data subject based on information given or submitted by the data subject or documents presented by the data subject (*establishment of identity*).

Section 13
Automated individual decision-making

Unless otherwise provided by law, a decision shall not be based solely on automated processing of personal data, including profiling, if the decision produces adverse legal effects concerning the data subject or otherwise significantly affects the data subject. (1226/2023)

By derogation from subsection 1, a competent authority may decide an administrative matter based solely on automated processing of personal data, if the matter is decided automatically in the manner referred to in chapter 8b of the Administrative Procedure Act (434/2003). (490/2023)

Chapter 3
Controller and processor

Section 14
Responsibility of the controller

The controller is responsible for the lawful processing of personal data. The controller shall also be able to demonstrate that the personal data have been processed in accordance with chapter 2.

The controller shall implement the appropriate technical and organisational measures required by the responsibility provided in subsection 1. In implementing the measures, account shall be taken of the nature, scope, context and purposes of processing as well as the risks for the rights of natural persons.

Section 15
Data protection by design and by default

The controller shall, both when determining the means for processing personal data and at the time of the processing itself, implement appropriate technical and organisational protection measures to ensure the lawfulness of the processing and the protection of the rights of the data subject. In implementing the measures, account shall be taken of the available technical solutions, the cost of implementing the measures, and the nature, scope, context and purposes of processing, as well as the risks resulting from the processing to the rights of the person.

The controller shall implement appropriate technical and organisational measures to ensure that, by default, only personal data that are necessary for each specific purpose of the processing are processed.

Section 16
Joint controllers

Where two or more controllers jointly determine the purposes and means of processing, they shall agree on their respective responsibilities for compliance with the obligations under this Act, unless the division of responsibilities is laid down by law.

The controllers referred to in subsection 1 shall, among themselves, designate a controller acting as a contact point for data subjects in matters concerning the exercise of the data subjects' rights. A data subject may, however, exercise their rights under this Act in relation to each controller.

Section 17
Processor

Anyone processing personal data on behalf of a controller shall give the controller appropriate accounts and commitments and otherwise sufficient guarantees concerning the organisational and technical measures by which the processor ensures that the personal data are processed in compliance with the requirements laid down in this Act.

The processor or anyone in its service shall process personal data only on instructions from the controller and shall not delegate the processing of personal data to another processor without written authorisation by the controller.

The processing of personal data by a processor shall be governed by a written contract or a written order indicating the personal data to be processed, the duration, nature and purpose of the processing, the categories of personal data to be processed and the categories of data subjects as well as the obligations and rights of the controller. The written document referred to above shall also stipulate that the processor shall

1) act only on instructions from the controller;

2) ensure that natural persons processing personal data have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

3) assist the controller by any appropriate means to ensure compliance with the provisions on the rights of the data subject;

4) at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of processing services, and delete existing copies unless otherwise provided by law;

5) make available to the controller all information necessary to demonstrate compliance with this section;

6) meet the preconditions for the use of another processor referred to in this section.

Section 18
Records of processing activities

The controller shall maintain a written record of the processing of personal data under its responsibility, containing the following information:

1) the name and contact details of the controller and, where necessary, the joint controller and the data protection officer referred to in section 38;

2) the purposes of and legal basis for the processing of personal data;

3) a description of the category or categories of data subjects and the categories of personal data to be processed;

4) the categories of recipients to whom personal data have been or will be disclosed;

5) the categories of transfers of personal data to third countries or international organisations;

6) where possible, the envisaged time limits for erasing the different categories of personal data;

7) any use of profiling;

8) where possible, a general description of the information systems and the principles for protecting them as well as a general description of the technical and organisational protection measures referred to in section 31.

The processor shall maintain a written record of all processing of personal data carried out on behalf of a controller, containing:

1) the name and contact details of the processor or processors and of the data protection officer;

2) the name and contact details of each controller on behalf of which the processor is acting;

3) the categories of processing carried out on behalf of each controller;

4) on the specific instruction of the controller, any information on the transfer of personal data to a third country or an international organisation;

5) where possible, a general description of the technical and organisational protection measures referred to in section 31.

Section 19
Logging

The controller and the processor shall provide for logs to be kept for the collection, alteration, consultation, disclosure, transfer, combination and erasure of personal data in their automated processing systems. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipient of such personal data.

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

Section 20
Data protection impact assessment

Prior to beginning the processing of personal data, the controller shall assess the impact of the envisaged processing operations on the protection of personal data.

The controller shall carry out an impact assessment in writing if the envisaged processing of personal data may result in a high risk to the implementation of the rights of a natural person. The impact assessment shall include a general description of the envisaged processing operations, an assessment of the risks to the rights of the data subject, the measures to address those risks and the measures to ensure the protection of the personal data.

Section 21
Prior consultation of the data protection authority

The controller or the processor shall consult the Data Protection Ombudsman prior to processing personal data where

1) the processing will, according to the written impact assessment referred to in section 20, subsection 2, result in a high risk to the rights of the data subject despite the envisaged safeguards; or

2) the processing will, especially because of the use of new technologies, mechanisms or procedures, result in a high risk to the rights of the data subject.

The controller shall provide to the Data Protection Ombudsman the impact assessment referred to in section 20, subsection 2 and, on request, any other information permitting the Ombudsman to assess the lawfulness of the processing of personal data.

If the Data Protection Ombudsman considers that the processing referred to in subsection 1 would infringe this Act, the Ombudsman shall, within six weeks after receiving the request for consultation, provide the controller and any processor with guidance on making the processing comply with law. The time limit may be extended by one month if so required by the complexity of the envisaged processing. The Data Protection Ombudsman shall inform the controller and any processor of the extension of the time limit and the reasons for the delay within one month after receiving the request for consultation.

Chapter 4
Rights of data subjects

Section 22
Privacy notice and obligation to provide information

The controller shall maintain a written notice of the processing of personal data under its responsibility, to be made publicly available and containing at least the following information:

1) the contact details of the controller and the data protection officer and, if the controller considers it necessary, the name of the data protection officer;

2) the name and contact details of the controller acting as the contact point for joint controllers, and a statement that the data subject may exercise their rights under this Act in relation to each controller;

3) the purposes of and legal basis for the processing of personal data;

4) the envisaged time limit for storing the personal data, or if such a time limit has not been determined, the criteria for determining it;

5) any regular recipients or categories of recipients of personal data;

6) the information that the data subject has the right to request from the controller access to the data subject's personal data and the right to request rectification or erasure of the personal data or restriction of processing of the data;

7) the information that the data subject has the right to make a request for measures referred to in section 56 to the Data Protection Ombudsman, and the contact details of the Ombudsman.

The controller shall provide the data subject with the notice referred to in subsection 1 and with any other information that is necessary for exercising the rights of the data subject laid down in this chapter, if the provision of this information is necessary in an individual case to ensure the exercise of the rights. The controller may omit all or part of the information if this is necessary on the grounds mentioned in section 28.

Section 23
Right of access of the data subject

Everyone has the right to obtain from the controller information as to whether their personal data are being processed. If such data are being processed, the data subject has the right to obtain from the controller the following information:

1) the personal data being processed and all available information on the origin of the data;

2) the purposes of and legal basis for the processing;

3) the categories of personal data being processed;

4) the recipients or categories of recipients to whom personal data of the data subject have been disclosed;

5) the envisaged time limit for storing the personal data, or if such a time limit has not been determined, the criteria for determining it;

6) the right of the data subject to request from the controller rectification or erasure of personal data concerning the data subject or restriction of processing of the data;

7) the right of the data subject to make a request for measures referred to in section 56 to the Data Protection Ombudsman, and the contact details of the Ombudsman.

Anyone who wants to check their personal data in the manner referred to in subsection 1 may make a request to that effect to the controller by means of a document signed in person or in another corresponding certified manner or in person before the controller.

Section 24
Limitations to the right of access

The right of access of the data subject may be postponed or restricted wholly or partly, or it may be refused to the extent that is necessary on the grounds mentioned in section 28. If the right of access of the data subject is postponed, restricted or refused, the controller shall, without undue delay, inform the data subject thereof by a written certificate. The grounds for the postponement, restriction and refusal shall also be stated, unless this would undermine the purpose of the refusal or restriction. The controller is also considered to have refused the right of access if the controller, within three months after the making of the request, has not replied to the data subject in writing.

The controller shall inform the data subject of the right to make a request for measures to the Data Protection Ombudsman on grounds of the postponement, restriction or refusal of the right of access, and shall inform the data subject of the right to exercise the right of access in accordance with section 29 through the Data Protection Ombudsman.

The controller shall document the information on the grounds for refusing or restricting the right of access.

Section 25
Rectification or erasure of personal data and restriction of processing

The controller shall, on its own initiative or at the request of the data subject, without undue delay, rectify or supplement any personal data concerning the data subject if they are incorrect or incomplete for the purpose of the processing.

The controller shall, spontaneously or at the request of the data subject, without undue delay, erase any personal data of the data subject if their processing conflicts with the provisions of section 4 or 5, section 6, subsection 1 or 2, or section 7 or 11. Instead of erasing the data, the controller shall, however, restrict the processing if

1) the data subject contests the accuracy of the data and their accuracy or inaccuracy cannot be ascertained; or

2) the data must be maintained for the purposes of evidence.

If the processing has been restricted by virtue of subsection 2, paragraph 1, the controller shall inform the data subject of this before lifting the restriction.

Section 26
Refusing the request of the data subject

If the controller refuses the request of the data subject to rectify, supplement or erase personal data or to restrict their processing, the controller shall inform the data subject of the refusal and its grounds by a written certificate. The information on the grounds for the refusal may be omitted wholly or partly to the extent that this is necessary on the grounds mentioned in section 28.

The controller shall inform the data subject of the right to make a request for measures to the Data Protection Ombudsman on account of the refusal referred to in subsection 1, and of the right

to exercise the rights referred to in section 25 in accordance with section 29 through the Data Protection Ombudsman.

Section 27
Obligation of the controller to communicate rectification, erasure or restriction of processing

The controller shall communicate any rectification of inaccurate personal data to the authority from which the inaccurate personal data originate.

If personal data have been rectified or erased or if their processing has been restricted by virtue of section 25, the controller shall communicate the matter to the recipients to whom the controller has disclosed such data. The recipient shall rectify or erase any such personal data possessed by it or restrict their processing.

Section 28
Restrictions of the rights of the data subject

The rights of the data subject may be restricted in the manner referred to in section 22, subsection 2; section 24, subsection 1; section 26, subsection 1 and section 35 if this, considering the rights of the data subject, is proportionate and necessary in order to

1) avoid detriment to the prevention, detection, investigation or prosecution of criminal offences or the enforcement of criminal sanctions;

2) safeguard any other investigation, examination or other procedure of an authority;

3) protect public security;

4) protect national security; or

5) protect the rights of other persons.

Section 29

Exercise of rights through the Data Protection Ombudsman

The data subject has the right to request the Data Protection Ombudsman to verify the lawfulness of the personal data and their processing if the right of access of the data subject has been postponed, restricted or refused by virtue of this Act or another Act or if the controller does not accept the request of the data subject to rectify, supplement or erase personal data or to restrict their processing.

If the data subject exercises the right referred to in subsection 1, the Data Protection Ombudsman shall, within a reasonable time, inform the data subject of the measures taken by the Ombudsman. The Data Protection Ombudsman shall also inform the data subject of the right to make a request for measures referred to in section 56 to the Ombudsman.

The Data Protection Ombudsman has the right to inspect data in the operative information system of the Finnish Security Intelligence Service on the basis of a request referred to in section 17a, subsection 1 of Parliament's Rules of Procedure (40/2000). The inspection shall be conducted without delay. (125/2019)

Section 30

Promoting the exercise of the rights of the data subject, and provision of measures free of charge

The controller shall promote the opportunities of data subjects to exercise the rights referred to in this chapter. All communications to the data subject and all information on the processing of personal data shall be given in a compact, comprehensible and easily available format and in a clear and plain language.

The communications and information given to the data subject in accordance with this Act and the consideration of the requests made by the data subject in accordance with this Act are free of charge to the data subject. However, if the requests of the data subject are manifestly unreasonable or unfounded because of their recurrence or for another reason, the controller may collect a charge for the measure. Provisions on the criteria for the charges are laid down in the Act on Criteria for Charges Payable to the State (150/1992).

If the controller collects a charge by virtue of subsection 2, it shall, where necessary, demonstrate that the request is manifestly unfounded or unreasonable.

Chapter 5
Data security

Section 31
Protection of personal data

The controller and the processor shall, by technical and organisational measures, ensure an adequate protection of the personal data, taking into account the risk resulting from the processing to the rights of the data subject. In particular, the personal data shall be protected against unlawful processing and accidental loss, destruction and damage. In planning and implementing the measures, account shall be taken of

1) the state of the art;

2) the costs of implementing the measures;

3) the nature, scope, context and purposes of processing;

4) the risk of varying likelihood and severity for the rights of natural persons.

Section 32
Protection of personal data in automated processing

In addition to what is provided in section 31, the controller or processor shall, in respect of automated processing, and following an evaluation of risks, implement measures designed to

1) deny unauthorised persons access to equipment used for processing;

2) prevent the unauthorised reading, copying, modification or removal of data media;

3) prevent the unauthorised input of personal data into the system and the unauthorised inspection, modification or removal of personal data stored in the system;

4) prevent the use of automated processing systems by unauthorised persons using data communication equipment;

5) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation;

6) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transferred or made available by using data communication equipment;

7) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems, and when and by whom the personal data were input;

8) prevent the unauthorised reading, copying, modification or removal of personal data during transfers of personal data or during transportation of data media;

9) ensure that installed systems may, in the case of interruption, be restored;

10) ensure that the functions of the system perform, that the appearance of faults in the functions is reported and that stored personal data cannot be corrupted by means of a malfunctioning of the system.

Section 33
Obligation of the processor to notify the controller of a personal data breach

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

Section 34
Obligation of the controller to notify the Data Protection Ombudsman of a personal data breach

The controller shall notify the Data Protection Ombudsman of a personal data breach, unless the breach is unlikely to result in a risk to the rights of the data subject.

The controller shall make the notification referred to in subsection 1 without undue delay and, where feasible, not later than 72 hours after having become aware of the personal data breach. Where the notification to the Data Protection Ombudsman is made later, it shall state reasons for the delay.

The controller shall document the information on personal data breaches and the facts relating to them, their effects and the remedial action taken.

Section 35
Obligation of the controller to communicate a personal data breach to the data subject

The controller shall, without undue delay, communicate a personal data breach to the data subject where the breach is likely to result in a high risk to the rights of the data subject. No obligation to communicate exists, however, where

1) the controller has taken appropriate technological and organisational protection measures to effectively prevent any abuse of the personal data affected by the personal data breach; or

2) the controller has, after the breach, taken subsequent measures to ensure that the breach is no longer likely to result in a risk to the rights of the data subject.

Where communicating a personal data breach to the data subject would involve a disproportionate effort, the controller may give a public communication on the breach instead of communicating it to the data subject.

The communication to the data subject may be postponed, restricted or omitted if the conditions laid down in section 28 are met.

Section 36
Obligation of the controller to communicate a personal data breach to another controller

The controller shall, without undue delay, communicate a personal data breach to another controller located in Finland or another EU Member State if the breach concerns data transferred by or to the latter controller.

Section 37
Content of the notification or communication of a personal data breach

The notification to the Data Protection Ombudsman referred to in section 34 and the communication to a controller located in Finland or another EU Member State referred to in section 36 shall describe the personal data breach. The description shall, to the extent possible, contain information on the categories of the data subjects concerned, the approximate number of data subjects, the categories of personal data records and the approximate number of personal data records.

The communication to the data subject referred to in section 35 shall describe the nature of the personal data breach.

The notifications and communications referred to in subsections 1 and 2 shall indicate

1) the name and contact details of the data protection officer or other contact point where further information can be obtained;

2) the likely consequences of the personal data breach;

3) the measures taken or proposed by the controller to address the personal data breach, and, where appropriate, the measures to mitigate its possible adverse effects.

The information to be provided to the Data Protection Ombudsman and a controller located in Finland or another EU Member State may be provided in phases in so far as it is not possible to provide them at the same time.

Chapter 6
Data Protection Officer

Section 38
Designation of a data protection officer

The controller shall designate a data protection officer. The data protection officer shall have sufficient expert knowledge of legislation concerning the processing of personal data and of the

practices in the field as well as ability to perform the tasks referred to in section 40. A single data protection officer may be designated for a number of competent authorities if this is appropriate considering the organisational structure and size of the authorities.

The controller shall communicate the contact details of the data protection officer to the Data Protection Ombudsman.

Section 39
Position of the data protection officer

The controller shall involve the data protection officer properly and in a timely manner in all issues which relate to the protection of personal data.

The controller shall ensure for the data protection officer the resources needed for performing the tasks prescribed for the officer in section 40 and provide the officer access to personal data and processing operations.

Section 40
Tasks of the data protection officer

The data protection officer has the following tasks:

1) to advise the controller and its employees who process personal data on issues of personal data protection;

2) to monitor compliance with the regulation of the processing of personal data and with the policies of the controller in relation to the processing of personal data;

3) to provide advice where requested as regards the data protection impact assessment and to monitor its performance pursuant to section 20;

4) to cooperate with the Data Protection Ombudsman and to act as the contact point for the Ombudsman on issues relating to the processing of personal data.

The tasks of the data protection officer do not cover the administration of justice by courts or the oversight of legality by the Chancellor of Justice of the Government and the Parliamentary Ombudsman.

Chapter 7
Transfers of personal data to third countries and international organisations

A competent authority may transfer personal data to a third country or an international organisation only if the other provisions applicable to the processing of personal data referred to in this Act are complied with and if

1) the transfer is necessary for a purpose mentioned in section 1, subsection 1 or 2;

2) the personal data are transferred to a controller in a third country or to an international organisation which is competent to process personal data for a purpose mentioned in section 1, subsection 1 or 2; and

3) a valid decision of the European Commission (*the Commission*) on the adequacy of the level of protection referred to in Article 36 of the Law Enforcement Directive exists, or unless such a decision exists, appropriate safeguards exist as provided in section 42 of this Act, or if the derogations for specific situations under section 43 are applicable.
(903/2020)

If the personal data originate from another EU Member State, an additional condition for the transfer is that this Member State has given its authorisation to the transfer. A transfer without such an authorisation is permitted only if it is necessary for the prevention of an immediate and serious threat to public security of a state or to essential interests of an EU Member State, and if the authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed of the transfer without delay.

In the case of an onward transfer of personal data to another third country or international organisation, the competent authority that carried out the original transfer may authorise the onward transfer in compliance with subsections 1 and 2 after taking into due account the seriousness of the criminal offence, the purpose for which the personal data were originally

transferred and the level of protection of personal data in the third country or the international organisation to which personal data are onward transferred, as well as other relevant factors.

Section 42
Transfer based on appropriate safeguards

If the Commission has not made a decision referred to in section 41, subsection 1, paragraph 3, personal data may be transferred to a third country or an international organisation if the other conditions laid down in section 41 are met and

1) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

2) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.

The controller shall inform the Data Protection Ombudsman about the categories of the transfers made under subsection 1, paragraph 2. The following information on the transfers shall be documented and, on request, made available to the Data Protection Ombudsman:

1) the date and time of the transfers;

2) the receiving competent authority;

3) the justification for the transfers; and

4) the personal data transferred.

Section 43
Derogations for specific situations

In the absence of a decision of the Commission referred to in section 41, subsection 1, paragraph 3, and if the conditions for a transfer of personal data laid down in section 42 are not met, transfers of personal data to a third country or an international organisation may take place only if the transfer is necessary

1) in order to protect the vital interests of the data subject or another person;

2) in order to safeguard legitimate and important interests of the data subject;

3) in order to prevent an immediate and serious threat to the public security of an EU Member State or a third country; or

4) in an individual case, for the purposes mentioned in section 1, subsection 1 or for the establishment, exercise or defence of legal claims relating to these purposes.

However, personal data shall not be transferred by virtue of subsection 1, paragraph 4, if the rights of the data subject override the public interest in the transfer.

The following information on transfers based on subsection 1 shall be documented and, on request, made available to the Data Protection Ombudsman:

1) the date and time of the transfer;

2) the receiving competent authority;

3) the justification for the transfer; and

4) the personal data transferred.

Section 44
Transfers of personal data to private entities and other recipients established in third countries

Notwithstanding the provisions of section 41, subsection 1, paragraph 2, a competent authority may, in individual cases, transfer personal data directly to private entities and other recipients established in third countries, if the other provisions of this Act are complied with and

1) the transfer is strictly necessary for performing the tasks of the transferring competent authority laid down in section 1, subsection 1;

2) the transferring competent authority determines that the rights of the data subject concerned do not override the public interest necessitating the transfer in the case at hand;

3) the transferring competent authority considers that the transfer to the competent authority of the third country would be ineffective or inappropriate because of the urgency of the matter or for another reason;

4) the authority that is competent for the purposes referred to in section 1, subsection 1 in the third country is informed of the transfer without undue delay, unless this is ineffective or inappropriate;

5) the transferring competent authority informs the recipient of the specified purpose or purposes for which the recipient may process the personal data and informs the recipient that the processing shall be necessary for these purposes and that the data shall not be processed for any other purposes; and

6) the transfer does not violate international treaty-based obligations binding on Finland.

The competent authority transferring the data shall document the details of the transfer made by virtue of subsection 1 and inform the Data Protection Ombudsman of the transfer.

Chapter 8
Supervisory authority

Section 45
Data Protection Ombudsman

The Data Protection Ombudsman referred to in section 8 of the Data Protection Act (1050/2018) shall supervise compliance with this Act.

The provisions of this Act on supervision do not apply to courts, the Chancellor of Justice of the Government and the Parliamentary Ombudsman.

The Data Protection Ombudsman shall be autonomous and independent in performing their tasks provided in this Act.

Section 46
Tasks

In addition to the supervision of compliance with this Act, the tasks of the Data Protection Ombudsman include the following:

1) to promote public awareness of the risks, legislation, safeguards and rights related to the processing of personal data;

2) to promote the awareness of controllers and processors of their obligations under this Act;

3) to provide data subjects, on request, with information about the exercise of their rights under this Act;

4) to advise on the prior consultation referred to in section 21;

5) to examine compliance with this Act;

6) to verify the lawfulness of the processing in accordance with section 29;

7) to consider requests for measures made by data subjects and organisations referred to in section 56;

8) to monitor technological and other developments affecting the protection of personal data.

Moreover, the Data Protection Ombudsman shall participate in the activities of the European Data Protection Board referred to in article 68 of 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). However, the Data Protection Ombudsman shall not refer to the European Data Protection Board a matter concerning the processing of personal data in the context of the activities referred to in section 1, subsection 2.

The measures taken by the Data Protection Ombudsman are free of charge for the data subject and the data protection officer. If, however, the requests of the data subject or the data protection

officer are manifestly unreasonable or unfounded because of their recurrence or for another reason, the Ombudsman may collect a charge for the measures or refuses to act on the matter referred to in the request. The criteria for determining the amount of the charges are laid down in the Act on Criteria for Charges Payable to the State.

If the Data Protection Ombudsman collects a charge or refuses to act on a matter in the manner referred to in subsection 3, the Ombudsman shall, where necessary, demonstrate that the request is manifestly unfounded or unreasonable.

Section 47
Right of access to information

Notwithstanding non-disclosure provisions, the Data Protection Ombudsman has the right to obtain, free of charge, the record of processing activities referred to in section 18, the logs referred to in section 19 and any other information necessary for the performance of the Ombudsman's tasks. (350/2020)

The Data Protection Ombudsman has the right to obtain from the controller and the processor evidence of the circumstances necessary to know for the performance of the Ombudsman's tasks.

Section 48
Right to conduct inspections

The Data Protection Ombudsman may conduct an inspection in the premises of a controller or a processor, if the inspection is necessary for supervising compliance with this Act.

An inspection may be conducted in premises used for permanent residence only if it is necessary for examining the circumstances being inspected and if a well-founded and specific reason exists in the case for suspecting that provisions on the processing of personal data have been or are being infringed in a manner that may be sanctioned with imprisonment provided for in the Criminal Code (39/1889).

The inspection shall take place in compliance with the provisions of section 39 of the Administrative Procedure Act (434/2003).

Section 49
Executive assistance

For the performance of their tasks, the Data Protection Ombudsman has the right, on request, to obtain executive assistance from the police.

Section 50
Use of experts

The Data Protection Ombudsman may consult external experts and request them to issue statements.

In the context of an inspection referred to in section 48, the Data Protection Ombudsman may rely on the assistance of an external expert. The Data Protection Ombudsman may assign as an expert a person who has consented to the task and who has expert knowledge relevant to performing the tasks of the Data Protection Ombudsman.

The provisions on criminal liability for acts in office apply to experts when they perform the tasks referred to in this Act. Provisions on liability for damages are laid down in the Tort Liability Act (412/1974).

Section 51
Measures

In a matter falling within the scope of application of this Act, the Data Protection Ombudsman may

1) issue guidance to a controller in the prior consultation procedure referred to in section 21;

2) notify a controller or a processor of an alleged infringement of this Act;

3) issue a warning to a controller or a processor that intended processing operations are likely to infringe the provisions of this Act;

4) issue a reprimand to a controller or a processor if they have processed personal data unlawfully;

5) order a controller or a processor to comply with the data subject's requests concerning the exercise of the rights of the data subject pursuant to this Act;

6) order a controller to communicate a personal data breach to the data subject;

7) impose a temporary or definitive ban or another limitation on processing;

8) order the suspension of data transfers to a recipient in a third country or to an international organisation;

9) order the rectification or erasure of personal data or restriction of processing and other related measures under section 25;

10) order a controller or a processor to bring processing operations into compliance with the provisions of this Act, where appropriate, in a specified manner and within a reasonable time.

Section 52
Conditional fine

The Data Protection Ombudsman may impose a conditional fine for the purpose of enforcing an order referred to in section 51, paragraphs 5–10 and an order to provide information under section 47. Provisions on the imposition of a conditional fine and the ordering of its payment are laid down in the Act on Conditional Fines (1113/1990).

No conditional fine shall be imposed on a natural person for the purpose of enforcing an order to provide information referred to in subsection 1, if grounds exist for suspecting the person of a criminal offence and the information concerns the matter underlying the suspicion of a criminal offence.

Section 53
Hearing the Data Protection Ombudsman

The Data Protection Ombudsman may, on their own initiative or on request, issue statements on issues related to the processing of personal data referred to in section 1.

The Data Protection Ombudsman shall be given an opportunity to be heard during the preparation of legislative or administrative reforms concerning the processing of personal data referred to in section 1.

Section 54
Mutual assistance

Notwithstanding non-disclosure provisions, the Data Protection Ombudsman shall, free of charge, provide the corresponding supervisory authority of another EU Member State with any personal data that are indispensably necessary for performing its supervisory task and any other necessary information and, where needed, also otherwise assist this authority in carrying out the supervision. The Data Protection Ombudsman shall also take other necessary measures to ensure effective mutual assistance.

The Data Protection Ombudsman shall reply to the request of the supervisory authority referred to in subsection 1 without undue delay, and in any case no later than one month after receiving the request.

In addition to what is provided in section 1, the Data Protection Ombudsman has the right to take measures that are necessary to ensure effective cooperation with the authorities supervising compliance with the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Notwithstanding non-disclosure provisions, the Data Protection Ombudsman has the right to disclose personal data or other data to these supervisory authorities for the purpose of performing a supervisory task, if the data are necessary for safeguarding the rights of a data subject or if a data subject has given their explicit consent to the disclosure of personal data. (903/2020)

Chapter 9
Legal protection

Section 55
Reporting procedure concerning infringements of the Act

The competent authority shall have in place procedures enabling confidential reporting to it of any suspected infringements of this Act. The reporting procedure shall include appropriate and

adequate measures to organise an appropriate consideration of the reports. The reporting procedure shall also include instructions that ensure the protection of the identity of the reporting person.

The competent authority shall document the necessary information concerning a report referred to in subsection 1. The information shall be erased after five years from the submission of the report, unless retaining it is necessary in order to ensure criminal investigation, pending judicial proceedings, or an investigation by authorities, or to safeguard the rights of the person subject to the report. The necessity of retaining the information shall be reviewed at the latest three years after the previous review. Records shall be kept of the review.

When a natural person has submitted a report referred to in subsection 1 to the competent authority, the identity of the reporting person shall not be disclosed, if it is estimated, based on the circumstances, that revealing the identity would cause detriment to the reporting person.

Section 56
Right to refer a matter to the Data Protection Ombudsman

If a data subject considers that this Act or another Act concerning the processing of personal data is being infringed in the processing of their personal data, the data subject has the right to refer the matter to the Data Protection Ombudsman (*request for measures*). With the consent of the data subject, also a non-profit organisation promoting the protection of personal data may refer a matter to the Data Protection Ombudsman.

Section 57 (1226/2023)
Consideration of a request for measures and appeal against inactivity

The Data Protection Ombudsman shall handle a matter initiated under section 56 within three months of the date on which it became pending or, if the matter cannot be handled within this time limit, inform the data subject within this time limit of an estimated date of decision. The Ombudsman shall also inform the party who filed the matter if the consideration of the matter is delayed because of a need for additional evidence or for another reason.

The Data Protection Ombudsman may suspend the consideration of a matter, if another matter related to it is pending before a court.

If the Data Protection Ombudsman fails to comply with the three-month time limit referred to in subsection 1, the data subject has the right to lodge an appeal with an administrative court. The appeal shall be lodged before the Data Protection Ombudsman has handled the matter or given an estimate of the date of decision. In this case, the appeal is considered to concern an inadmissibility decision.

Section 58
Decisions of the Commission

If the Data Protection Ombudsman, in a matter pending before them, considers it necessary to examine whether a decision of the Commission on the adequacy of the level of protection referred to in section 41, subsection 1, paragraph 3 complies with the Law Enforcement Directive, the Ombudsman may, by application, refer a case concerning a request for a preliminary ruling to the Helsinki Administrative Court.

Subsection 2 was repealed by Act 870/2020.

Section 59
Request for a review of a decision of the Data Protection Ombudsman (870/2020)

Provisions on requesting a judicial review by an administrative court are laid down in the Administrative Judicial Procedure Act (808/2019). (870/2020)

Subsection 2 was repealed by Act 870/2020.

The Data Protection Ombudsman may order in their decision that the decision shall be complied with regardless of appeal, unless the appellate authority orders otherwise.

Chapter 10
Miscellaneous provisions

Section 60
Compensation for damage

The controller is obliged to compensate for any economic and other damage that has been caused to a data subject or another person by processing personal data in violation of this Act.

Other provisions on the right to compensation for damage are laid down in the Tort Liability Act.

Section 61
Penal provisions

The punishment for a data protection offence is laid down in chapter 38, section 9 of the Criminal Code. The punishments for a violation of the secrecy of communications, an aggravated violation of the secrecy of communication, unlawful access to an information system and aggravated unlawful access to an information system are laid down in chapter 38, sections 3, 4, 8 and 8a of the Criminal Code, respectively. The punishments for an infringement of the non-disclosure obligation laid down in section 55, subsection 3 and for an infringement of the obligation to remain silent referred to in section 62 are imposed in accordance with chapter 38, section 1 or 2 of the Criminal Code, unless the act is punishable under chapter 40, section 5 of the Criminal Code or unless a more severe punishment for the act is provided elsewhere by law.

Section 62
Obligation to remain silent

Provisions on the obligation to remain silent and the prohibition of use of information are laid down in section 23 of the Act on the Openness of Government Activities (621/1999).

Chapter 11
Entry into force and transitional provisions

Section 63
Entry into force and transitional provisions

This Act enters into force on 1 January 2019.

Section 64
Transitional provisions

Automated processing systems set up before 6 May 2016 shall be brought into conformity with section 19 on 6 May 2023 at the latest.