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

Data Protection Act
(1050/2018)

By decision of Parliament, the following is enacted:

Chapter 1
General provisions

Section 1
Purpose of the Act

This Act specifies and supplements 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*, and its national application.

Section 2
Scope of application

This Act applies within the scope of application of Article 2 of the Data Protection Regulation. This Act and the Data Protection Regulation also apply, with the exception of Article 56 and Chapter VII of the Regulation, to the processing of personal data in the course of activities referred to in points (a) and (b) of Article 2(2), unless otherwise provided elsewhere by law.

This Act does not apply to parliamentary activities.

This Act does not apply to such processing of personal data that is governed by the Act on the Processing of Personal Data in Criminal Matters and in Maintaining National Security (1054/2018).

Section 3
Applicable law

Finnish law applies to the processing of personal data in the context of activities of an establishment of a controller or a processor located in the territory of the European Union, if the controller is established in Finland.

If the law of a foreign state applies to the processing of personal data and derogations are made by virtue of it in accordance with Article 89(2) of the Data Protection Regulation from the rights provided for the protection of the data subject, the safeguards laid down for the protection of the data subject in section 31 below shall, however, be complied with irrespective of the choice of applicable law.

Chapter 2
Legal basis for processing in certain cases

Section 4
Lawfulness of processing

Personal data may be processed in accordance with point (e) of Article 6(1) of the Data Protection Regulation if:
1) the data describe the position of a person, his or her duties or the performance of these duties in a public sector entity, business and industry, activities of civil society organisations, or other corresponding activities, in so far as the objective of the processing is of public interest and the processing is proportionate to the legitimate aim pursued;
2) the processing is proportionate and necessary for the performance of a task carried out in the public interest by an authority;
3) the processing is necessary for scientific or historical research purposes or statistical purposes and it is proportionate to the aim of public interest pursued; or
4) the processing of research material and cultural heritage material containing personal data and the processing of personal data included in their metadata for archiving purposes is necessary and proportionate to the aim of public interest pursued and to the rights of the data subject.

Section 5
Age limit for offering information society services to a child

Where personal data are processed based on consent referred to in point (a) of Article 6(1) of the Data Protection Regulation and in connection with offering of information society services referred to in Article 4(25) directly to a child, the processing of the personal data of the child is lawful where the child is at least 13 years old.

Section 6
Processing of special categories of personal data

Article 9(1) of the Data Protection Regulation does not apply:
1) when an insurance institution processes data it has received in the course of insurance activities on an insured person's or claimant's state of health, illness or disability, or such data on the treatment or other comparable measures directed at the insured or the claimant that are necessary for determining the liability of the insurance institution;
2) to any processing of data that is provided by law or that derives directly from a statutory duty set out for the controller by law;
3) to the processing of data concerning trade union membership, where this is necessary for carrying out the obligations and exercising the specific rights of the controller in the area of employment law;
4) when a healthcare service provider in the course of arranging or producing services processes data it has received in the context of these activities on the state of health or disability of a person or on the healthcare and rehabilitation services received by a person, or other data necessary for the treatment of the data subject;
5) when a social welfare service provider in the course of arranging or producing services or granting benefits processes data it has received or produced in the context of these activities on the state of health or disability of a person or on the healthcare and rehabilitation services received by a person, or other data necessary for granting a benefit or providing service to the data subject;
6) to the processing of data concerning health and of genetic data in the context of anti-doping work and sports for persons with disabilities, in so far as the processing of these data is necessary to enable anti-doping work or sports for persons with disabilities or long-term illness;
7) to the processing of data for scientific or historical research purposes or for statistical purposes;

8) to the processing of research and cultural heritage materials for archiving purposes in the public interest, with the exception of genetic data.

Where personal data are processed in a context referred to in subsection 1, the controller and the processor shall take suitable and specific measures to safeguard the rights of the data subject. Such measures include:

1) measures that enable subsequent checking and verification of the identity of the person who has recorded, altered or transferred personal data;

2) measures to improve the competence of the personnel processing personal data;

3) designation of a data protection officer;

4) internal measures by the controller and the processor for preventing access to personal data;

5) pseudonymisation of personal data;

6) encryption of personal data;

7) measures that ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;

8) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

9) specific rules of procedure for ensuring compliance with the Data Protection Regulation and this Act when personal data are transferred or processed for another purpose;

10) a data protection impact assessment in accordance with Article 35 of the Data Protection Regulation;

11) other technical, procedural and organisational measures.

Section 7

Processing of personal data relating to criminal convictions and offences

Personal data relating to criminal convictions and offences or related security measures referred to in Article 10 of the Data Protection Regulation may be processed if:

1) the processing is necessary for the investigation, establishment, exercise, defence or resolution of a legal claim; or

2) the data are processed for a purpose referred to in section 6, subsection 1, paragraph 1, 2 or 7.

The provisions of section 6, subsection 2 on the measures for safeguarding the rights of the data subject also apply to the processing of personal data referred to in subsection 1 of this section.

Chapter 3
Supervisory authority

Section 8
Data Protection Ombudsman

In Finland, the national supervisory authority referred to in the Data Protection Regulation is the Data Protection Ombudsman, who works under the auspices of the Ministry of Justice.

The Data Protection Ombudsman is autonomous and independent in his or her activities.

Section 9
Office of the Data Protection Ombudsman

The Data Protection Ombudsman has an Office with at least two Deputy Data Protection Ombudsmen and a necessary number of referendaries familiar with the Data Protection Ombudsman's field of action and other personnel.

The Data Protection Ombudsman appoints the public officials and hires the other personnel of the Office.

The Data Protection Ombudsman adopts the rules of procedure of the Office.

Section 10
Required qualifications and criteria for appointment

The qualifications required of the Data Protection Ombudsman and the Deputy Data Protection Ombudsman are a Master's degree in Law, other than a Master's degree in International and Comparative Law, good familiarity with matters related to the protection of personal data, and proven leadership skills. Furthermore, an ability to perform international duties is required.

Section 11
Appointment and term of office

The government appoints the Data Protection Ombudsman and the Deputy Data Protection Ombudsman for a term of five years.

The person appointed as Data Protection Ombudsman or Deputy Data Protection Ombudsman is exempt from attending to another office while acting as the Data Protection Ombudsman or the Deputy Data Protection Ombudsman.

Section 12
Expert board

The Office of the Data Protection Ombudsman has an expert board that consists of a chairperson, deputy chairperson and three other members. Each of them has a personal deputy.

The government appoints the board for a term of three years.

The chairperson and the deputy chairperson of the board shall hold a Master's degree in Law, other than a Master's degree in International and Comparative Law, and have good familiarity with matters related to the protection of personal data and other competence necessary for the performance of the task. The other members of the board are required to have familiarity with matters related to the protection of personal data and other competence necessary for the performance of the task.

Provisions on criminal liability for acts in office apply to the board members 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). The members and deputy members of the board are paid a fee for the performance of their tasks. The Ministry of Justice determines the amounts of the fees.

Section 13
Declaration of private interests

The Data Protection Ombudsman and the Deputy Data Protection Ombudsman shall submit a declaration of their private interests referred to in section 8a of the State Civil Servants Act (750/1994).

Section 14
Tasks and powers of the Data Protection Ombudsman

Provisions on the tasks and powers of the Data Protection Ombudsman are laid down in Articles 55–59 of the Data Protection Regulation. The Data Protection Ombudsman also has other tasks and powers provided in this Act or in other Acts.

The Data Protection Ombudsman does not supervise the activities of the Chancellor of Justice of the Government or the Parliamentary Ombudsman.

The Data Protection Ombudsman represents Finland in the European Data Protection Board.

The Data Protection Ombudsman conducts the accreditation of the certification body referred to in Article 43 of the Data Protection Regulation.

The Data Protection Ombudsman draws up an annual activity report referred to in Article 59 of the Data Protection Regulation and transmits it to the Government and Parliament. The activity report shall be kept available to the public.

Section 15
Decision-making by the Data Protection Ombudsman

The Data Protection Ombudsman decides matters upon presentation, unless he or she decides otherwise in an individual case.

Section 16
Tasks and powers of the Deputy Data Protection Ombudsman

The division of tasks between the Data Protection Ombudsman and the Deputy Data Protection Ombudsman is determined in the rules of procedure of the Office of the Data Protection Ombudsman.

In the performance of his or her tasks, the Deputy Data Protection Ombudsman has the same powers as the Data Protection Ombudsman.

Section 17
Tasks of the expert board and consideration of matters at the board

The task of the expert board is to issue, upon request of the Data Protection Ombudsman, opinions on significant questions related to the application of the legislation governing the processing of personal data.

The board may consult external experts.

A referendary of the Office of the Data Protection Ombudsman serves as the secretary of the board.

Section 18
Data Protection Ombudsman's investigative powers and right of access to information

In addition to what is provided in Article 58(1) of the Data Protection Regulation on the supervisory authority's investigative powers and right to obtain access to information, the Data Protection Ombudsman has the right, notwithstanding secrecy provisions, to obtain, free of charge, access to information that is necessary for the performance of his or her tasks.

An inspection may be carried out in premises used for permanent residence only if this 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 an administrative fine or a punishment provided in the Criminal Code (39/1889).

Section 19
Use of experts

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

The Data Protection Ombudsman may rely on the assistance of external experts in carrying out an inspection that falls within his or her powers. The provisions on criminal liability for acts in office apply to an expert when he or she performs such tasks. Provisions on liability for damages are laid down in the Tort Liability Act.

Section 20
Executive assistance

The Data Protection Ombudsman has the right to obtain, on request, executive assistance from the police for performing his or her tasks.

Chapter 4
Legal protection and sanctions

Section 21
Right to refer a matter to the Data Protection Ombudsman

A data subject has the right to refer a matter to the Data Protection Ombudsman for consideration, if he or she considers that the relevant legislation is being infringed in the processing of personal data concerning him or her.

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

Section 22
Conditional fine

The Data Protection Ombudsman may impose a conditional fine for the purpose of enforcing an order referred to in points (c)–(g) and (j) of Article 58(2) of the Data Protection Regulation and to enforce an order to provide information that has been issued under section 18, subsection 1 of this Act. 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 there are grounds to suspect the person of a criminal offence and the information concerns the matter underlying the suspicion of a criminal offence.

Section 23
Decisions of the Commission

If the Data Protection Ombudsman, in a matter pending before him or her, considers it necessary to examine whether a decision of the European Commission concerning the adequacy of the level of protection referred to in Article 45 of the Data Protection Regulation is in compliance with the Data Protection Regulation, the Data Protection Ombudsman may, by application, refer a matter concerning a request for preliminary ruling to the Helsinki Administrative Court.

The decision of the Administrative Court may be appealed against only if the Supreme Administrative Court grants leave to appeal.

Section 24
Administrative fine

The administrative penalty payment laid down in Article 83 of the Data Protection Regulation (*administrative fine*) is imposed by a collegial body for sanctions, which is composed of the Data Protection Ombudsman and the Deputy Data Protection Ombudsmen. The collegial body is chaired by the Data Protection Ombudsman. When a Deputy Data Protection Ombudsman is prevented from acting, a referendary determined in the rules of procedure of the Office of the Data

Protection Ombudsman may substitute for him or her in the collegial body. The collegial body has a quorum with three members present.

Decisions of the collegial body are made upon presentation. Decisions shall be based on the opinion seconded by the majority. In case of a tie, the decision shall be based on the opinion that is more favourable for the party subject to the sanction.

An administrative fine may also be imposed for an infringement of Article 10 of the Data Protection Regulation in compliance with the provisions of this Act and Article 83(5) of the Regulation.

An administrative fine cannot be imposed on central government authorities, state enterprises, municipal authorities, autonomous institutions governed by public law, agencies operating under Parliament or the Office of the President of the Republic, or the Evangelical Lutheran Church of Finland and the Orthodox Church of Finland or their parishes, parish unions and other bodies.

An administrative fine shall not be imposed if more than ten years have elapsed since the infringement or negligence. If the infringement or negligence has continued for a longer time, the ten-year time limit is calculated from the end of the infringement or negligence.

Provisions on the enforcement of an administrative fine are laid down in the Act on the Enforcement of Fines (672/2002). An administrative fine becomes time-barred in five years from the date on which it was imposed.

Section 25
Request for review

A decision of the Data Protection Ombudsman and the Deputy Data Protection Ombudsman and a decision referred to in section 24, subsection 1 may be appealed against to an administrative court as provided in the Administrative Procedure Act (586/1996).

A decision of an administrative court may only be appealed against if the Supreme Administrative Court grants leave to appeal. The Data Protection Ombudsman may also appeal against a decision of an administrative court.

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

Section 26
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 message interception and an aggravated message interception are laid down in chapter 38, sections 3 and 4 of the Criminal Code, and the punishments for a computer break-in and an aggravated computer break-in are laid down in chapter 38, sections 8 and 8a of the Criminal Code. The punishments for an infringement of the non-disclosure obligation referred to in section 35 and for an infringement of the secrecy obligation referred to in section 36 of this Act 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 has been provided for it elsewhere in law.

Provisions on the prosecutor's obligation to hear the Data Protection Ombudsman before bringing charges for offences specified in subsection 1 and provisions on the court's obligation to give the Data Protection Ombudsman an opportunity to be heard when such a case is being heard in court are laid down in chapter 38, section 10, subsection 3 of the Criminal Code.

Chapter 5
Specific data processing situations

Section 27
Processing of personal data for journalistic purposes or the purposes of academic, artistic or literary expression

To guarantee the freedom of expression and information, the following provisions of the Data Protection Regulation do not apply to the processing of personal data performed solely for journalistic purposes or for the purposes of academic, artistic or literary expression: points (c)–(e) of Article 5(1), Articles 6 and 7, Articles 9 and 10, Article 11(2), Articles 12–22, Article 30, Article 34(1)–(3), Articles 35 and 36, Article 56, point (f) of Article 58(2), Articles 60–63, and Articles 65–67.

Article 27 of the Data Protection Regulation does not apply to the processing of personal data in the course of activities referred to in the Act on the Exercise of Freedom of Expression in Mass Media (460/2003). Articles 44–50 of the Data Protection Regulation do not apply if the application would infringe on the right to freedom of expression or information.

To guarantee the freedom of expression and information, the following provisions of the Data Protection Regulation apply only where appropriate to the processing of personal data performed solely for journalistic purposes or for the purposes of academic, artistic or literary expression: points (a) and (b) of Article 5(1), Article 5(2), Articles 24–26, Article 31, Articles 39 and 40, Article 42, Articles 57 and 58, Article 64, and Article 70.

Section 28
Principle of openness of government activities

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 29
Processing of personal identity codes

A personal identity code may be processed if the data subject has given consent to it or if so provided by law. A personal identity code may also be processed if it is necessary to uniquely identify the data subject:
1) in order to perform a statutory duty;
2) in order to implement the rights and duties of the data subject or the controller; or
3) for scientific or historical research purposes or statistical purposes.

A personal identity code may be processed in credit granting and debt collection; in insurance, credit institution, payment service, renting and lending activities; in credit data processing; in healthcare and social welfare services and other activities to ensure social security; and in matters concerning public service employment relationships, employment relationships and other service relationships and benefits relating to these.

In addition to what is provided in subsections 1 and 2 on the processing of personal identity codes, a personal identity code may be disclosed for the purposes of data processing performed to

update address information or to prevent redundant postal traffic, if the personal identity code is already available to the recipient.

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

Section 30
Processing of personal data in employment context

Provisions on the processing of personal data concerning employees, performance of tests and examinations on employees and the related requirements, technical surveillance in the workplace, and retrieving and opening employees' email messages are laid down in the Act on the Protection of Privacy in Working Life (759/2004).

Section 31
Derogations and safeguards relating to processing of personal data for scientific and historical research purposes and statistical purposes

Where personal data are processed for scientific or historical research purposes, the rights of the data subject laid down in Articles 15, 16, 18 and 21 of the Data Protection Regulation may be derogated from, where necessary, provided that:
1) the processing is based on an appropriate research plan;
2) a person or group responsible for the research has been designated; and
3) the personal data are used and disclosed only for scientific or historical research purposes or for other compatible purposes, and the procedure followed is also otherwise such that data concerning a given individual are not revealed to outsiders.

Where personal data are processed for statistical purposes, the rights of the data subject laid down in Articles 15, 16, 18 and 21 of the Data Protection Regulation may be derogated from, where necessary, provided that:
1) the statistics cannot be compiled or the underlying data requirements fulfilled without processing personal data;
2) the compilation of the statistics in question has a factual connection with the activities of the controller; and

3) the data are not disclosed or made available in a way allowing for the identification of a given individual, except where the data are disclosed for the purposes of public statistics.

Where personal data referred to in Article 9(1) and Article 10 of the Data Protection Regulation are processed for the purposes referred to in subsection 1 or 2, a derogation from the rights of the data subject provided in Articles 15, 16, 18 and 21 of the Data Protection Regulation requires, in addition to what is provided in subsections 1 and 2, that a data protection impact assessment referred to in Article 35 of the Data Protection Regulation be carried out or that codes of conduct in accordance with Article 40 of the Data Protection Regulation, in which the derogation from the rights of the data subject referred to above is appropriately taken into account, be complied with. The written data protection impact assessment shall be submitted to the Data Protection Ombudsman for information before the processing is started.

Section 32
Derogations and safeguards relating to processing of personal data for archiving purposes in the public interest

Where personal data are processed for archiving purposes in the public interest pursuant to section 4, paragraph 4 of this Act or point (c) of Article 6(1) of the Data Protection Regulation, the rights of the data subject referred to in Articles 15, 16 and 18–21 of the Data Protection Regulation may be derogated from under the conditions laid down in Article 89(3) of the Data Protection Regulation.

Section 33
Restrictions concerning the controller's obligation to provide information to data subjects

The obligation to provide information to data subjects referred to in Articles 13 and 14 of the Data Protection Regulation may be derogated from, if this is necessary for national security, defence or public order and security, for preventing or investigating offences, or for a supervisory task relating to taxation or public finances.

The provisions of paragraphs 1–4 of Article 14 of the Data Protection Regulation may also be derogated from if the provision of information causes substantial damage or detriment to the data subject and the data to be recorded are not used for decision-making concerning the data subject.

If a data subject is not provided with information under subsection 1 or 2, the controller shall take appropriate measures to protect the rights of the data subject. These measures include keeping the information referred to in Article 14(1) and (2) of the Data Protection Regulation available to the public, unless this undermines the purpose of the restriction concerning the provision of information.

Section 34
Restrictions concerning the right of access by data subject

The data subject does not have the right of access to data which have been collected concerning him or her, referred to in Article 15 of the Data Protection Regulation, if:
1) providing access to the data could compromise national security, defence, or public order and security, or hamper the prevention or investigation of offences;
2) providing access to the data could seriously endanger the health or treatment of the data subject or the rights of some other person; or
3) the personal data are used in the performance of supervisory and inspection tasks and the refusal to provide access to the data is necessary to safeguard an important economic or financial interest of Finland or the European Union.

If only a part of the data concerning a data subject is such that it under subsection 1 falls outside the scope of the right of access referred to in Article 15 of the Data Protection Regulation, the data subject has the right of access to the remainder of the data concerning him or her.

The data subject shall be informed of the reasons for the restriction, unless this undermines the purpose of the restriction.

Where the data subject does not have the right of access to data which have been collected concerning him or her, the information referred to in Article 15(1) of the Data Protection Regulation shall be provided to the Data Protection Ombudsman on the request of the data subject.

Chapter 6
Miscellaneous provisions

Section 35
Non-disclosure obligation

Anyone who has gained knowledge of the characteristics, personal circumstances, economic situation or a trade secret of another person while carrying out measures relating to the processing of personal data shall not unlawfully disclose the information to a third person nor make use of it to his or her own benefit or to the benefit or detriment of someone else.

Section 36
Protection of identity of reporting persons

Where a natural person has reported a suspected infringement of the provisions subject to the supervision of the Data Protection Ombudsman to the Ombudsman, the identity of the reporting person shall be kept secret, if it is estimated, based on the circumstances, that revealing the identity would cause detriment to the reporting person.

Section 37
Entry into force

This Act enters into force on 1 January 2019.

This Act repeals the Personal Data Act (523/1999) and the Act on the Data Protection Board and the Data Protection Ombudsman (389/1994).

Section 38
Transitional provisions

The validity of permissions granted by the Data Protection Board expires when this Act enters into force. Matters pending before the Data Protection Board upon the entry into force of this Act lapse when this Act enters into force.

The provisions of sections 36 and 37 of the Personal Data Act on the duty of notification and submission of a notification apply to matters that concern notifications made to the Data Protection Ombudsman and are pending when this Act enters into force.

Where the provisions of Articles 12 and 15–18 of the Data Protection Regulation that impose broader obligations on the controller than the provisions in force upon the entry into force of this Act, those provisions do not apply to such cases of exercise of the right of access and rectification of personal data that are pending when this Act enters into force, if the application of the said provisions of the Data Protection Regulation would be unreasonable for the controller.

The provisions in force upon the entry into force of this Act apply to requesting a review of a decision of the Data Protection Board or the Data Protection Ombudsman issued before the entry into force of this Act. However, the provisions in force upon the entry into force of this Act apply to a request for extraordinary review only if the request has been filed before the entry into force of this Act.

If an act causing damage has been committed before the entry into force of this Act, the provisions in force upon the entry into force of this Act apply to liability for damages.