

Translation from Finnish
Legally binding only in Finnish and Swedish
Ministry of Economic Affairs and Employment

Act on the Protection of Privacy in Working Life
(759/2004; amendments up to 347/2019 included)

By decision of Parliament, the following is enacted:

Chapter 1

General provisions

Section 1

Purpose of the Act

The purpose of this Act is to promote the protection of privacy and other fundamental rights safeguarding the protection of privacy in working life.

Section 2

Scope of application

This Act lays down provisions on the processing of personal data concerning employees, the performance of tests and examinations on employees and the related requirements, technical surveillance in the workplace, and retrieving and opening employees' electronic mail messages.

The provisions of this Act concerning employees also apply to civil servants and any persons in a civil service relationship or comparable service relationship subject to public law, and, as appropriate, to job applicants.

In addition to what is provided in this Act, 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), hereinafter *Data Protection Regulation*, contains provisions regarding the processing of employees' personal data.

Unless otherwise provided in this Act, the provisions of the Data Protection Act (1050/2018) shall also apply to the processing of personal data. Part VI of the Act on Electronic Communications Services (917/2014) contains provisions regarding the confidentiality of communications and the protection of privacy. (347/2019)

The employee's obligation to undergo a health examination is governed by separate provisions.

Chapter 2

General preconditions for processing personal data

Section 3

Necessity requirement

The employer is only allowed to process personal data directly necessary for the employee's employment relationship, which is connected with managing the rights and obligations of the parties to the employment relationship or with the benefits provided by the employer for the employee or which arises from the special nature of the work concerned.

No exceptions can be made to the necessity requirement, even with the employee's consent.

Section 4 (347/2019)

General preconditions for collecting personal data concerning employees and the employer's duty to provide information

The employer shall collect personal data concerning the employee primarily from the employee himself or herself. In order to collect personal data from elsewhere, the employer must obtain the consent of the employee. However, this consent is not required when an authority discloses information to the employer to enable the latter to fulfil a statutory duty, or if it is expressly separately provided by law on collecting or obtaining data. The Security Clearance Act (726/2014) contains provisions regarding requests for

security clearance. The Act on Checking the Criminal Background of Persons Working with Children (504/2002) contains provisions laying out the procedure to be followed when checking the criminal background of persons appointed to work with minors. Provisions on the right to obtain data from the criminal records are laid down in the Criminal Records Act (770/1993).

The employer shall notify the employee in advance that data concerning the employee will be collected in order to establish his or her reliability. If the employer acquires personal credit data on an employee, the employer must also notify the employee of the register from which the credit data are obtained. If data concerning the employee has been collected from a source other than the employee himself or herself, the employer must notify the employee of this data before it is used in making decisions concerning the employee. Chapter III of the Data Protection Regulation contains provisions regarding the obligation of the controller to provide information to the data subject and regarding the right of access by the data subject.

The collection of personal data during recruitment and during an employment relationship is governed by the co-operation procedure referred to in the Act on Co-operation within Undertakings (334/2007), the Act on Cooperation in Government Agencies and Public Bodies (1233/2013), and the Act on Cooperation between the Employer and Employees in Municipalities (449/2007).

Section 5

Processing data concerning health

The employer has the right to process data concerning the employee's health status if the data has been collected from the employee himself or herself, or elsewhere with the employee's written consent, and the data needs to be processed in order to pay sick pay or other comparable health-related benefits or to establish whether there is a justified reason for absence or if the employee expressly wishes his or her working capacity to be assessed on the basis of data concerning his or her health. In addition, the employer has the right to process such data in the specific circumstances, and to the stipulated extent, separately provided elsewhere in the law.

Data concerning the employee's health may only be processed by persons who prepare, make or implement decisions concerning employment relationships on the basis of such data. The employer shall nominate such persons or specify the tasks that involve processing of the data concerning health. Persons who process such data may not disclose any of it to a third party either during or after their employment relationship.

A doctor's certificate or statement concerning the employee's working capacity given to the employer by the employee may, however, be supplied to the occupational health service provider for the purpose of carrying out the occupational health care duties laid down in the Occupational Health Care Act (1383/2001), unless the employee has forbidden this.

The employer must store any data in its possession concerning the employee's health separately from any other personal data that it has collected. Data concerning health shall be erased immediately after the grounds for processing referred to in paragraph 1 have ceased to exist. The grounds and necessity of processing shall be evaluated at least every five years. (347/2019)

Section 5 a (511/2008)

Processing of personal credit data

The employer has the right to obtain and use personal credit data referred to in section 4 of the Credit Information Act (527/2007) concerning a job applicant selected for a position for the purpose of assessing the job applicant's reliability when the intention is that the applicant will work in duties that require particular reliability and

- 1) that involve the power to make significant financial commitments on behalf of the employer or to use de facto independent discretionary power in the preparation of such commitments;
- 2) in which the employee's specific duty is to grant and control financially significant credits;
- 3) in the administration of which the employee is given access to specially protected trade secrets of key significance for the employer or its customer; (610/2018)

- 4) that require access rights to information systems that will allow the transfer of the employer's or its customer's funds, or modify the related information, or in which the employee is granted system administrator rights to such an information system;
- 5) that essentially involve the processing, without any immediate supervision, of large amounts of money, or securities or valuable items;
- 6) that involve the guarding of the employer's or its customer's property;
- 7) that, as a rule, involve working in a private home without supervision.

The provisions of subsection 1 shall also apply if the employee's duties change during the employment relationship in such a way that they fulfil the preconditions laid down in the stated subsection concerning the employer's right to handle personal credit data.

The employer is responsible for the costs of obtaining the personal credit data.

Section 19, subsection 2, paragraph 9 of the Credit Information Act contains provisions regarding the right to use personal credit data when a person is selected into a position of responsibility in a company.

Chapter 3

Processing data on drug use

Section 6

Drug test certificate

The employer may only process data on the drug use testing of the employee which is contained in the drug test certificate supplied to the employer by the person concerned. The processing of the data is otherwise subject to the provisions of section 5(2-4).

A drug test certificate means a certificate issued by a health care professional and laboratory designated by the employer stating that the employee has been tested for the use of a drug referred to in section 3, subsection 1, paragraph 5 of the Narcotics Act (373/2008) and containing a report based on the test stating whether the employee has

used drugs for non-medicinal purposes in a manner that has impaired his or her working capacity or functional capacity. (375/2008)

Drug tests and the certificates of such tests are subject to the provisions of section 19 of the Occupational Health Care Act.

Section 7

Submission of a drug test certificate during recruitment

The employer may receive or otherwise process data entered in a drug test certificate, with the consent of the applicant selected for the job, only if the applicant is to do the type of work that requires precision, reliability, independent judgement or good ability to react and if performing the work while under the influence of drugs or while addicted to drugs could:

- 1) endanger the life, health or occupational safety of the employee or other persons;
- 2) endanger national defence or state security;
- 3) endanger traffic safety;
- 4) increase the risk of significant environmental damage;
- 5) endanger the protection, usability, integrity and quality of information received while working and thus cause harm or damage to public interests protected by confidentiality provisions or endanger the protection of privacy or the rights of data subjects; or
- 6) endanger a trade secret, or cause more than a minor level of financial loss to the employer or the employer's customer, provided that endangering a trade secret or causing a financial risk could not be prevented by other means. (610/2018)

The employer also has the right to process data with the job applicant's consent, as referred to in subsection 1, in the event that:

- 1) the applicant is to carry out tasks in which special trust is required, in which work will be performed elsewhere than in premises supervised by the employer and in which the performance of duties while under the influence of drugs or while addicted to drugs may cause significant financial loss to a customer of the employer or endanger the customer's personal safety;

- 2) the applicant is to carry out tasks which, on a permanent basis and to a material degree, include raising, teaching, caring for or otherwise looking after a minor, or other work involving personal interaction with a minor, and no other person is involved; or
- 3) the applicant is to carry out the type of tasks in which there is independent and uncontrolled access to drugs or a more than minor quantity of medicines that could be used for the purposes of intoxication.

The provisions of subsections 1 and 2 also apply if the employee's duties change during the employment relationship in such a way that they meet the preconditions referred to above concerning the employer's right to process data entered in a drug test certificate.

Provisions on the submission of a drug test certificate to the employer as a precondition for appointment to a civil service post are laid down in section 8b of the State Civil Servants Act (750/1994) and, in the case of recruitment to a public sector service relationship, in section 7 of the Act on Civil Servants in Local Government (304/2003). Provisions on the action programme on substance abuse prevention are laid down in section 11 of the Occupational Health Care Act.

Section 8

Submission of a drug test certificate during the employment relationship

The employer may require the employee to present a drug test certificate during his or her employment relationship if the employer has a justified reason to suspect that the employee is under the influence of drugs at work or that the employee has a drug addiction and if testing is necessary to establish the employee's working or functional capacity and the employee does the type of work that requires special precision, reliability, independent judgement or good ability to react and in which the performance of duties while under the influence of drugs or while addicted to drugs:

- 1) seriously endangers the life, health or occupational safety of the employee or other persons;
- 2) seriously endangers national defence or state security;
- 3) seriously endangers traffic safety;
- 4) could considerably increase the risk of significant environmental damage;

- 5) seriously endangers the protection, usability, integrity and quality of information received while working and could thus cause harm or damage to public interests protected by confidentiality provisions or endanger the protection of privacy or the rights of data subjects;
- 6) endangers a financially significant trade secret or could cause a significant financial loss to the employer or the employer's customer, provided that endangering the trade secret or causing a financial risk could not be prevented by other means; or (610/2018)
- 7) could significantly increase the risk of illegal trading in or spread of substances in the possession of the employer that are referred to in section 3, subsection 1, paragraph 5 of the Narcotics Act. (375/2008)

The employer may impose on the employee a reasonable time limit within which the certificate must be presented. Provisions on the action programme on substance abuse prevention are laid down in section 11 of the Occupational Health Care Act.

The employer also has the right to process data entered in a drug test certificate if, on the basis of a positive drug test result, the employee has pledged to undergo treatment for drug abuse and the processing of data in the certificate is related to monitoring implementation of the treatment.

Section 9

The employer's duty to provide information about a drug test certificate

The employer shall notify the job applicant in connection with the application procedure prior to the signing of an employment contract, or the employee prior to a change in the terms of his or her contract, that the work is such that the employer intends to process the data entered in a drug test certificate in accordance with section 7, or is such that the employer intends to require the employee to present a drug test certificate in accordance with section 8(2).

Section 10

Cost of acquiring a certificate

The employer shall meet the cost of acquiring certificates referred to in this Chapter which are submitted to it.

Section 11

Relation to the provisions on health examinations

The provisions of sections 7 and 8 will not prevent the taking of a drug test as a part of the job applicant's or employee's health examination performed by the occupational health care unit under the Occupational Health Care Act, the State Civil Servants Act or the Act on Civil Servants in Local Government. Provisions on information to be entered in the certificate issued following a health examination under the Occupational Health Care Act shall be laid down separately.

Section 12

Application of the provisions to professional athletes

The provisions of this Chapter do not apply to athletes in an employment relationship referred to in Chapter 1, section 1, of the Employment Contracts Act (55/2001).

Chapter 4

Preconditions concerning the undertaking of tests and examinations

Section 13

Personality and aptitude assessments

With the employee's consent, he or she can be tested by means of personality and aptitude assessments to establish his or her capacity to perform the work in question or his or her need for training and other occupational development. The employer shall ensure that the assessment methods used are reliable, the persons conducting the assessment are experts, and the findings of the assessment are free from error. When checking that the findings are free from error, the assessment method used and the nature of the assessment method must be taken into account.

Upon request, the employer or an assessor designated by the employer shall provide the employee concerned with a written statement on the assessment of the employee's personality or aptitude free of charge. If the employer has received the statement orally, the employee must be informed of its content.

Section 14

Use of health care services

When carrying out employees health examinations and tests and taking samples, health care professionals, properly trained laboratory personnel and health care services must be used as provided in the health care legislation.

The provisions of subsection 1 also apply to alcohol and drug tests.

Section 15

Genetic testing

The employer is not permitted to require the employee to take part in genetic testing during recruitment or during the employment relationship, and has no right to know whether or not the employee has ever taken part in such testing.

Chapter 5

Camera surveillance in the workplace

Section 16

Preconditions for camera surveillance

The employer may operate a system of continuous surveillance within its premises based on the use of technical equipment which transmits or records images (*camera surveillance*) for the purpose of ensuring the personal security of employees and other persons on the premises, protecting property or supervising the proper operation of production processes, and for preventing or investigating situations that endanger safety, property or the production process. Camera surveillance may not, however, be used for

the surveillance of a particular employee or particular employees in the workplace. Neither may camera surveillance be used in lavatories, changing rooms or other similar places, in other staff facilities or in work rooms designated for the personal use of employees.

Notwithstanding subsection 1, the employer may, however, direct the camera surveillance at a particular work station where employees are at work if the surveillance is essential for:

- 1) preventing an apparent threat of violence related to the work of the employee or an apparent harm or danger to the employee's safety or health;
- 2) preventing or investigating property crimes if an essential part of the employee's work is to handle property of high value or quality, such as money, securities or valuables; or
- 3) safeguarding the employee's interests and rights, where the camera surveillance is based on the request of the employee who is to be the subject of the surveillance.

(347/2019)

Section 17

Transparency when implementing camera surveillance

When planning and implementing camera surveillance, the employer shall ensure that:

- 1) the opportunity of using other means that interfere less with the privacy of employees is explored before the introduction of camera surveillance;
- 2) the privacy of employees is not interfered with more than is necessary for achieving the aim of the measures;
- 3) paragraph was repealed by Act 347/2019
- 4) recordings are used only for the purpose for which the surveillance was carried out;
- 5) after the cooperative and consultative procedures referred to in section 21, employees are informed of when the camera surveillance will begin, how it will be implemented, how and in what situations any recordings would be used and, in situations referred to in section 16 subsection 2, the locations of the cameras; and
- 6) prominent notification of the camera surveillance and its method of implementation is displayed in the areas in which the cameras are located.

Notwithstanding subsection 1, paragraph 4 and section 21, the employer has the right to use recordings for:

- 1) substantiating the grounds for termination of an employment relationship;
- 2) investigating and substantiating harassment or molestation as referred to in the Act on Equality Between Women and Men (609/1986), harassment referred to in section 14 of the Non-Discrimination Act (1325/2014) or harassment and inappropriate behaviour as referred to in the Occupational Safety and Health Act (738/2002), provided that the employer has a justified reason to suspect that the employee is guilty of harassment, molestation or inappropriate behaviour; or (1345/2014)
- 3) investigating an occupational accident or some other situation causing a danger or threat referred to in the Occupational Safety and Health Act.

Recordings shall be destroyed as soon as they are no longer necessary for achieving the purpose of the camera surveillance, and no later than one year after the end of the recording. A recording may, however, be stored after this period if it is needed for completing the processing of a matter referred to in subsection 2 that emerged for investigation before the end of the maximum storage period or if the employer needs the recording to substantiate the appropriateness of terminating an employment relationship, or if there is some other special reason for keeping the recording.

Chapter 6

Retrieval and opening of electronic mail messages belonging to the employer

Section 18

The employer's obligations regarding necessary arrangements

The employer has the right to retrieve and open electronic mail messages sent to an electronic mail address allocated by the employer for the use of the employee or electronic mail messages sent by the employee from such an address only if the employer has planned and arranged for the employee the necessary measures to protect electronic mail messages sent in the employee's name or by the employee and, to this end, has specifically ensured that:

- 1) the employee can, with the aid of the electronic mail system's automatic reply function, send notification to a message sender about his or her absence and the length of

absence, and information about the person who is to take care of the tasks of the absent employee; or

- 2) the employee can direct messages to another person approved by the employer for this task or to another employer-approved address of the employee; or
- 3) the employee can give his or her consent to an arrangement whereby in his or her absence another person of his or her choosing and approved by the employer for the task can receive messages sent to the employee, with the aim of establishing whether the employee has been sent a message that is clearly intended for the employer for the purpose of managing the work and on which it is essential for the employer to have information on account of its operations or the appropriate organisation of the work.

The provisions of sections 19 and 20 constitute further preconditions for the retrieval or opening of the electronic mail messages referred to in subsection 1 above.

Section 19

Retrieval of electronic messages belonging to the employer

The employer has the right, assisted by the person vested with the authority of information system administrator, to find out on the basis of information concerning the message sender, recipient or title, whether the employee has, in his or her absence, been sent, or has sent or received immediately before the absence, messages belonging to the employer that, in order to complete negotiations concerning its operations or to serve customers or safeguard its operations, it is otherwise essential for the employer to gain information on, if:

- 1) the employee manages tasks independently on behalf of the employer and the employer does not operate a system with which the matters attended to by the employee and the processing stages involved are recorded or are otherwise ascertained;
- 2) it is evident, on account of the employee's tasks and matters pending, that messages belonging to the employer have been sent or received;
- 3) the employee is temporarily prevented from performing his or her duties, and messages belonging to the employer cannot be obtained for the employer's use despite the fact that the employer has seen to the obligations referred to in section 18; and

4) the employee's consent cannot be obtained within a reasonable time and the investigation of the matter cannot be delayed.

If the employee has died or if he or she is prevented in a permanent way from performing his or her duties and his or her consent cannot be obtained, the employer has the right, under the conditions laid down in subsection 1(1-2) and on the basis of information on the message sender, recipient or title, to find out if there are messages belonging to it, unless finding out about the matters attended to by the employee and safeguarding of the employer's operations is possible by other means.

If message retrieval does not lead to opening of the message, a report signed by the persons involved stating why the message was retrieved, the time it was retrieved and who performed the retrieval must be drawn up. The report shall be submitted to the employee without undue delay, unless otherwise provided by subsection 2. The information on the message sender, recipient or title may not be processed more extensively than necessary for the purpose of retrieving the message, and the persons processing the information may not disclose it to a third party during the employment relationship or after it has ended .

Section 20

Opening of electronic messages belonging to the employer

If, on the basis of the information on the sender or recipient of an electronic message or the message title, it is apparent that a message sent to the employee or by the employee is clearly one that belongs to the employer and about whose content it is essential that the employer obtains information in order to complete negotiations concerning its operations or to serve customers or safeguard its operations, and the message sender and recipient cannot be contacted for the purpose of establishing the content of the message or for the purpose of sending it to an address indicated by the employer, the employer may, in cases referred to in section 19, open the message with the assistance of the person vested with the authority of information system administrator and in the presence of another person.

A report about the opening shall be drawn up, signed by the persons involved, stating which message was opened, why it was opened, the time of opening, the persons performing the opening and to whom the information on the content of the opened message was given. The report shall be submitted to the employee without undue delay, unless otherwise provided by section 19 subsection 2. The opened message shall be stored, and its content and the information on the sender may not be processed more extensively than is necessary for the purpose of opening the message, nor may the persons processing the information disclose the content of the message to a third party during the employment relationship or after it has ended.

The person employed by the employer or a person acting on the instruction of the former, to whom the employee has directed his or her electronic mail in the manner referred to in section 18 subsection 1 paragraph 2 or who can, in the manner referred to in section 18 subsection 1 paragraph 3, and with the employee's consent, receive messages sent in the employee's name, has the right to open a message, complying with the provisions of subsection 2, unless the employee has given his or her consent to another procedure.

Chapter 7

Miscellaneous provisions

Section 21

Co-operation in organising technical monitoring and data network use

The purpose and introduction of and methods used in camera surveillance, access control and other technical monitoring of employees, and the use of electronic mail and other data networks and the processing of information pertaining to the employee's electronic mail and other electronic communication are governed by the cooperation procedure referred to in the Act on Cooperation within Undertakings, Act on Cooperation in Government Agencies and Public Bodies and the Act on Cooperation between the Employer and Employees in Municipalities. In undertakings and in organisations subject to public law that are not governed by the legislation on cooperation, the employer must, before making decisions on these matters, reserve the employees or their representatives an opportunity to be consulted. (126/2009)

After the co-operation or consultative procedures, the employer shall determine the purpose of the technical monitoring of employees and the methods used, and inform employees about the purpose and introduction of and methods used in the monitoring system, and about the use of electronic mail and the data network.

Section 22 (347/2019)

Supervision

Compliance with this Act shall be supervised by the occupational health and safety authorities within their competence together with the Data Protection Ombudsman. Provisions on the tasks and the competence of the Data Protection Ombudsman are laid down in Articles 55–59 of the Data Protection Regulation and section 14 of the Data Protection Act. Chapters 2 and 3 of the Act on Occupational Safety and Health Enforcement and Cooperation on Safety and Health at Workplaces (44/2006) lay down provisions on the competence of the occupational safety and health authorities.

Section 23

Display

The employer shall make this Act freely available to employees at the place of work.

Section 24 (347/2019)

Penal provisions

An employer or its representative who deliberately or out of gross negligence

- 1) violates the provisions of section 9 on the duty to provide information,
- 2) processes data concerning employee's health contrary to the provisions of section 5 subsection 1,
- 3) acquires or uses personal credit data of an applicant or employee contrary to the provisions of section 5a,
- 4) receives or otherwise processes data entered in a job applicant's drug test certificate, contrary to the provisions of section 7,

- 5) requires the employee to present a drug test certificate or otherwise processes data entered in such a certificate, contrary to the provisions of section 8,
 - 6) subjects the employee to personality or aptitude assessments without his or her consent or fails to confirm the reliability of the assessment methods, the expertise of the assessors or the freedom from error of the data from the assessments, contrary to the provisions of section 13 subsection 1,
 - 7) violates the provisions of section 13 subsection 2 on provision of a written statement or provision of information on the content of an oral statement,
 - 8) uses other than health care professionals, properly trained laboratory personnel or health care services, contrary to the provisions of section 14,
 - 9) requires the employee to take part in genetic testing or acquires information about such testing taken by the employee, contrary to the provisions of section 15,
 - 10) introduces camera surveillance, contrary to the provisions of section 16,
 - 11) violates the provisions of section 17 on the transparency of camera surveillance,
 - 12) retrieves, contrary to the provisions of section 19, or opens, contrary to the provisions of section 20, a message sent to or by the employee,
 - 13) violates the provisions of section 21 subsection 2 on the duty to determine and inform,
or
 - 14) violates the provisions of section 23 on the displaying of this Act,
- shall be sentenced to a fine for *violating the Act on the Protection of Privacy in Working Life*, unless a more severe penalty is provided elsewhere in the law.

The Criminal Code of Finland (39/1889) lays down punishments for a data protection offence, hacking, illicit viewing, eavesdropping, message interception, a secrecy offence and an offence in office.

Chapter 8

Entry into force

Section 25

Transitional provisions and entry into force

This Act enters into force on 1 October 2004.

If the employer's obligations laid down in sections 4 subsection 3 and section 21 of this Act are met in the manner laid down in section 4 subsection 3 and section 9 of the Act on the Protection of Privacy in Working Life in force at the time of the entry into force of this Act, the obligations will be considered to have been met in accordance with this Act. The employer's obligations laid down in section 17 of this Act shall be met no later than six months after the Act's entry into force.

Section 26

Repealed provisions

This Act repeals the Act of 8 June 2001 on the Protection of Privacy in Working Life (477/2001).

If another act or decree refers to the Act on the Protection of Privacy in Working Life valid at the time when this act comes into force, this Act must be applied instead.