MEAE brochures • 6/2019

# Act on the Protection of Privacy in Working Life

Ministry of Economic Affairs
and Employment of Finland

**Ministry of Economic Affairs and Employment**
Employment and Well-Functioning Markets
Johanna Ylitepsa, tel. +358 29 506 4207
PO Box 32, 00023 Government
Tel. +358 29 516 001 (switchboard)
www.tem.fi

MEAE brochures 6/2019

Layout: MEAE, December 2019

# Contents

# 1 Scope of application of the Act

The Act on the Protection of Privacy in Working Life lays down provisions on the following: the processing of an employee's personal data; the times when an employer can monitor an employee's personal credit data or drug use; aptitude and personality assessments carried out on employees; technical surveillance, especially by cameras, in the workplace; and the employer's right to retrieve and open messages in the employee's personal work email. In addition, the Act restricts the processing of data on the employee's health in the workplace.

The Act on the Protection of Privacy in Working Life applies to the protection of privacy in the relationship between an employee and an employer.

**The scope of application of the Act on the Protection of Privacy in Working Life includes:**

- employees under an employment contract;
- civil servants and any persons in a civil service relationship or comparable service relationship subject to public law;
- as appropriate, jobseekers and applicants for a post.

# 2 Other legislation associated with the privacy of employees

Employees' personal data must be processed in keeping with the EU General Data Protection Regulation (GDPR) and, in parallel with this, the Data Protection Act. The Act on the Protection of Privacy in Working Life serves as a special law.

Among other things, the General Data Protection Regulation sets out the grounds on which personal data may be processed (legal grounds for processing) and determines the general principles of data protection, the controller's obligations and the data subject's rights. Information on the content of the General Data Protection Regulation is available, for example, on the website of the Data Protection Ombudsman (tietosuoja.fi).

Unless otherwise prescribed by the Act on the Protection of Privacy in Working Life, the processing of an employee's personal data is governed by the Data Protection Act supplementing the General Data Protection Regulation. The Data Protection Act provides, among other things, for the processing of data belonging to special categories of personal data, such as trade union membership, as well as the processing of data relating to criminal convictions and offences. The Data Protection Act also contains provisions on certain restrictions to the data subject's rights.

**Provisions concerning employees' privacy have also been laid down in other legislation, such as**

- special legislation for civil servants;
- the Security Clearance Act;
- the Act on Checking the Criminal Background of Persons Working with Children;
- the Criminal Records Act;
- the Act on Electronic Communications Services; and
- the Occupational Health Care Act.

This brochure focuses on the provisions of the Act on the Protection of Privacy in Working Life.

**Personal data** means any information relating to an identified or identifiable natural person (data subject).

**An identifiable** natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as

- a name,
- an identification number,
- location data,
- an online identifier, or
- to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The concept of personal data is wide. It is enough that the person can be identified even indirectly, for example by combining data. A photo or a video recording may also contain personal data.

**Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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.

**Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The controller may also be appointed by law. The employer is the controller even when the management of employment relationship affairs has been outsourced. However, the provider of occupational health care services has the position of a controller independent of the employer.

# 3 General preconditions for processing personal data

## 3.1 Necessity requirement

**The employer is only allowed to process personal data that are *directly necessary* for the employee's employment relationship when these**

- relate to the management of the rights and obligations of the parties to the employment relationship;
- relate to the benefits provided by the employer to the employees; or
- arise from the special nature of the work concerned.

Not even the employee's consent authorises the processing of data that do not meet these requirements.

The necessity requirement applies to all processing of an employee's personal data. Already when planning the collection of data, the employer must determine the necessity and purpose of the processing of personal data by defining the tasks for which the employee's personal data are processed. Such an assessment must always be made on a case-by-case basis.

It is impossible to list all the personal data that the employer has the right to process. Processing situations and needs vary in working life, depending on the sector or the job. The need to collect data may stem, among others, from the authorities, customers, the working environment, personnel administration or organisational development. The public sector has specific provisions on, among other things, the application procedure for a post and the criteria for appointment, which give rise to data processing needs.

**Data that are directly necessary for the employment relationship may include data relating, for example, to**

- the selection of an employee;
- the performance of tasks;
- working conditions; or
- compliance with the provisions of collective agreements.

Data related to the benefits provided by the employer may include, for example, swimming tickets and discounts and their use. Data based on the special nature of the work may include, among other things, the family circumstances of an employee seconded abroad when the employer provides for the children's education. In recruitment situations, the employer must assess the necessity of the data in relation to the job applied for. This is mainly data on the job-seeker's qualifications and suitability.

The necessity requirement specifies the requirements under the General Data Protection Regulation. The General Data Protection Regulation includes the requirement to minimise the data processed: the personal data processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Personal data must be collected for a specified, explicit and legitimate purpose. Personal data may not be further processed in a manner that is incompatible with those purposes.

## 3.2 Erasure of unnecessary data

The employer may not keep outdated or unnecessary data about employees. Personal data which are inaccurate or incorrect with regard to the purposes of the processing must be erased or rectified without delay. Personal data may be kept only for as long as is necessary for the purposes for which the data processing is carried out.

There are specific provisions regarding the storing of personal data, which the employer must comply with. These include, for example, statutes of limitations under the Employment Contracts Act, the Working Hours Act and the Accounting Act. In addition, public administration has specific provisions on storing the personal data of employees and civil servants.

The employer must inform the employee of the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (see Informing the employee on page 12).

## 3.3 Prohibition of discrimination

Collecting unnecessary personal data may lead to discrimination. Therefore, the prohibition of discrimination laid down in legislation is important for the processing of personal data, for example, when assessing the necessity of personal data.

**Provisions on the prohibition of discrimination are found, for example in**

- the Constitution
- the Employment Contracts Act
- the Non-discrimination Act
- the State Civil Servants Act
- the Act on Municipal Officeholders
- the Church Act
- the Act on Equality between Women and Men (the Equality Act)
- the Criminal Code.

## 3.4 Prohibition to process data belonging to special categories of personal data

**The processing of (sensitive) data belonging to special categories of personal data is in principle prohibited. These data include:**

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership ;
- the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person;
- health records;
- data concerning a natural person's sex life or sexual orientation.

The prohibition of processing helps to prevent discrimination.

The processing of data concerning the employee's state of health is governed by the Act on the Protection of Privacy in Working Life and specific legislation, such as the Occupational Health Care Act.

The Data Protection Act also contains provisions on the processing of special categories of personal data. It prescribes, for example, the processing of data on trade union membership, which is necessary to comply with the controller's special rights and obligations in the field of labour law.

## 3.5 Collection of employees' personal data

The employer must collect personal data primarily from the employees themselves. This is the best way for employees to find out what information is collected about them. For collecting data from elsewhere, the employer must obtain the employee's consent.

**However, the employee's consent need not be obtained,**

- when an authority discloses information to the employer to enable the latter to fulfil a statutory duty (e.g. information provided by the execution authority to the employer for the purpose of wage attachment); or
- if it is expressly provided by legislation on collecting or obtaining data.

As a rule, the employer does not have the right to collect criminal record data on the employee. The employer does not have the right to require that employees obtain their criminal record extract under the data subject's inspection right (right of access to data) and present it to the employer.

The criminal background of persons appointed to work with minors can be checked under the conditions laid down separately by law (Act on Checking the Criminal Background of Persons Working with Children).

The Security Clearance Act lays down the conditions for drawing up a security clearance and the tasks covered by the security clearance. The security clearance is done by the Finnish Security Intelligence Service. They will consider, on a case-by-case basis, whether any data found in their register should be disclosed to the applicant for information. If anything significant is revealed, it will be communicated to the applicant in writing. Otherwise, the applicant is informed that no information relevant to the security clearance was discovered about the person.

Acquisition of data from the criminal records in accordance with the Criminal Records Act in order to ascertain the reliability of an employee is possible only in rare cases related to the authorities' activities.

**The employer, on his own initiative, must inform the employee**

- of the intention to obtain data in order to determine the employee's reliability before obtaining the data (personal credit data, other data collected with the employee's consent);
- from which register the personal credit data are obtained; and
- of the data collected from sources other than the employee, and the contents of such data, before the data are used in decision-making about the employee.

In addition, the employer (as the controller) must also ensure that the obligations to inform the data subject, as laid down in the General Data Protection Regulation, are met. The General Data Protection Regulation lists the data that must be provided for the data subject. The information obligations must be borne in mind, both when using electronic job application forms and when collecting data in other ways.

# 4 Processing data concerning health

The data concerning an employee's health are sensitive personal data belonging to special categories of personal data, and their processing is in principle prohibited. Therefore, the law restricts the employer's right to process information concerning the employee's health.

Even the employee's explicit consent does not justify the processing of data on the employee's health beyond what is stipulated by law.

**The employer is allowed to process data concerning the employee's health only**

- if the employee himself or herself gives the data to the employer; or
- if the employee has given written consent, for example to the occupational health service, to disclose such data to the employer.

**However, the employer (even with the employee's consent) may not process just any data on the employee's health. The employer has the right to process such data only if**

- the processing is necessary for paying sick pay;
- the processing is necessary to provide other health-related benefits comparable to sick pay;
- the processing is needed to determine if there is a valid reason for absence from work;
- the employee expressly wishes his or her working capacity to be assessed on the basis of health data; and
- the data are processed in the situations and to the extent provided separately elsewhere in legislation, such as legislation on occupational safety and health and on occupational health care.

A health-related benefit may be, for example, a doctor's appointment for examination or treatment on full pay.

The Employment Contracts Act and collective agreements include provisions for the payment of sick pay. The contractual terms cover periods of sick pay that are longer than those prescribed by law and apply extensively not only to organised employer companies but also to companies outside employers' organisations on the basis of the general applicability of collective agreements.

In collective agreements, the payment of sick pay is generally subject to the condition that the employee presents a doctor's certificate to the employer at least for illnesses lasting more than three days. In addition, agreements may contain a clause stating that the employer claims compensation under the Health Insurance Act for the period on which the employee is paid wages. That claim must be accompanied by a doctor's certificate. Agreements also contain provisions which entitle the employee to receive pay for the duration of a certain treatment or examination, even if the employee is not directly incapacitated for work. Agreements have been interpreted as meaning that the employer has the right to be informed of the medical diagnosis. On this basis, the employer determines whether the employee is entitled to sick pay.

The Act on the Protection of Privacy in Working Life does not require an employee to submit a detailed doctor's report to the employer. If the employee fails to deliver a doctor's certificate to the employer, he or she may forfeit sick pay and must then personally claim compensation under the Health Insurance Act.

The employer is entitled to process data concerning the state of health also to determine if there is a valid reason for absence from work; the doctor treating the employee does not always know the working conditions. The employer, in certain circumstances, may also reorganise the work in such a way that the health problem diagnosed does not de facto prevent working.

When determining the working capacity at the employee's request data relevant to the development of the employee's health and working conditions at the workplace can be processed.

The processing of data concerning employees' health is governed not only by the Act on the Protection of Privacy in Working Life but also by other legislation. For example, under the Occupational Health Care Act, the occupational physician, in the case of work involving a particular risk of illness, may provide the employer with a written statement of the conclusions of medical examinations and, based on these, the appropriate labour protection measures to the extent that they pertain to health and safety at work.

The employer may give the doctor's certificate received from the employee to the occupational health service provider for carrying out its tasks, unless the employee has forbidden this.

Information on the employee's health may not be made available at the workplace to persons other than those who need the information in the course of their work. Persons processing health data are under an obligation of confidentiality and must not disclose information to unauthorised persons. The obligation of confidentiality continues after the termination of employment.

**The processing of data concerning health involves specific requirements because of their sensitive nature**

- Data concerning employees' health may only be processed by persons who prepare, make or implement decisions on the basis of such data.
- The employer must nominate the persons who process data concerning health, or specify the tasks that involve the processing of such data.
- The circle of persons processing health-related data at workplaces must be defined so that it is as small as possible.
- Data concerning health must be kept separate from other personal data collected by the employer.
- Data concerning health must be erased from the register immediately after the grounds for processing have ceased to exist.
- The need for storing the data must be evaluated regularly, at least every five years.

In his register, the employer may compile information on the employee's periods of sick leave, for example, for the payroll system. However, the employer may not enter the diagnoses written on the doctor's sick-leave certificates into the register.

# 5 Processing of personal credit data

The Act on the Protection of Privacy in Working Life defines the grounds on which the employer has the right to obtain and use a jobseeker's or employee's personal credit data to assess their reliability. The employer has the right to obtain and use only the personal credit data of a candidate already selected for the job or of an employee changing tasks in the service of the same employer.

**The employer's right to obtain and use an employee's personal credit data is limited to tasks that require particular reliability and**

- 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;
- in which the employee's specific duty is to grant and control financially significant credits;
- in the administration of which the employee is given access to specially protected trade secrets of key significance for the employer or his customer;
- that require access rights to information systems that will allow the transfer of the employer's or his customer's funds, or modify the related information, or in which the employee is granted system administrator rights to such an information system;
- that essentially involve the processing, without any immediate supervision, of large amounts of money, or securities or valuable items;
- that involve the guarding of the employer's or its customer's property; or
- that, as a rule, involve working in a private home without supervision.

The employer is always responsible for the costs of obtaining the personal credit data, even if the employee submitted them to the employer. If the employer obtains the personal credit data, the employee must be informed of the register from which the data were obtained.

# 6 Processing data on drug use

The Act on the Protection of Privacy in Working Life provides for the employer's right to process the data marked on the drug test certificate, but not the actual drug testing. The starting point is that the jobseeker or employee himself or herself submits the certificate to the employer. The employer may process and store only the drug use data given in the certificate and only with the employee's consent. The certificate may merely report that the employee has been tested for drug use and conclude whether the employee has used drugs for non-medicinal purposes in a manner that has impaired his or her working capacity or functional capacity. Drugs are defined in the Narcotics Act.

Because the data on drug testing are sensitive health data, their processing is otherwise subject to the same procedural requirements as other data concerning health (see p. 15 above).

A certificate may only be requested if the conditions laid down by law are met. Data based on general screening tests may not be processed.

## 6.1 Submission of a drug test certificate during recruitment

**The employer has the right to request a drug test certificate from a person selected for the job only if both of the following conditions are met:**

1. The jobseeker is to do the type of work that requires
   - precision;
   - reliability;
   - independent judgment; or
   - good ability to react

These job-related requirements are more stringent than those generally required in contractual and public-service employment relationships.

2. Performing the work while under the influence of drugs or while addicted to drugs can
    - endanger the life, health or occupational safety of the employee or other persons;
    - endanger national defence or state security;
    - endanger traffic safety;
    - increase the risk of significant environmental damage;
    - endanger the information security 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
    - endanger a trade secret, or cause more than a minor level of financial loss to the employer or the employer's customer. This also requires that endangering a trade secret or causing a financial risk could not be prevented by other means.

**In addition, the employer has the right to request a certificate when the jobseeker intends 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;
- 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
- 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 jobseeker is not obliged to provide a certificate. However, when considering recruitment, the employer may disregard a jobseeker who does not provide a certificate. In most cases, the selection is in practice conditional until the person selected for the task has submitted a certificate. For civil servants and officeholders, the submission of a certificate may be a condition for appointment to a civil service post.

The provisions concerning jobseekers also apply if the employee's duties change during the employment relationship in such a way that they meet the preconditions referred to above.

## 6.2 Submission of a drug test certificate during the employment relationship

**The employer may require the employee to present a drug test certificate during the employment relationship if the following conditions are met:**

1. 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;

2. testing is necessary to establish the employee's working or functional capacity;

3. the employee does the type of work that requires
   - special precision;
   - reliability;
   - independent judgment; or
   - good ability to react

4. performing the work tasks while under the influence of drugs or while addicted to drugs
   - seriously endangers the life, health or occupational safety of the employee or other persons;
   - seriously endangers national defence or state security;
   - seriously endangers traffic safety;
   - can considerably increase the risk of significant environmental damage;
   - seriously endangers the information security of information received while working and thus can cause harm or damage to public interests protected by confidentiality provisions, or can endanger the protection of privacy or the rights of data subjects;

- endangers a financially significant trade secret or can cause a significant financial loss to the employer or the employer's customer, provided that endangering the trade secret or causing a financial risk cannot be prevented by other means; or
- can significantly increase the risk of illegal trading in or spread of substances that are in the employer's possession and referred to in section 3, subsection 1, paragraph 5 of the Narcotics Act.

In addition, the employer may require the employee to present a certificate when the employee is committed to having treatment after receiving a positive test result.

The preconditions for requesting a certificate during an employment relationship are clearly stricter than during recruitment.

The employer may impose a reasonable time limit within which the certificate must be presented. The submission of the certificate is an obligation associated with the employment relationship. If the employee does not submit the certificate to the employer, the potential consequences for the employee will be determined on the grounds of labour law and civil service law, based on overall consideration.

## 6.3 Other provisions on drug testing

The employer is required to notify the jobseeker 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 the contract, that, due to the nature of the work, the employer will request the applicant selected to submit a drug test certificate, or will require the employee to submit a drug test certificate during the employment relationship.

For this purpose, the employer may choose the appropriate procedure, such as submitting the certificate in conjunction with the pre-employment health examination. However, the person selected for the job must know what is expected of him or her and by which time the certificate must be submitted to the employer.

The employer is responsible for the costs of both the jobseeker's and the employee's certificate.

The employer commissioning the testing must have a written action programme on substance abuse prevention, as referred to in the Occupational Health Care Act. According to

the Occupational Health Care Act, the substance abuse programme must include the general objectives of the workplace and the practices observed to prevent substance abuse and for referral of persons with substance abuse problems to treatment. The action programme may be a part of the occupational health care action plan.

Before the programme is approved, the tasks that require testing must be discussed under the cooperation procedure. In companies and public-law corporations not governed by the legislation on cooperation, before decision-making, the employer must reserve an opportunity for the employees or their representatives to be consulted on tasks requiring testing.

The provisions on drug testing contained in the Act on the Protection of Privacy in Working Life do not apply to professional athletes under an employment contract. They are subject to their own regulations on doping tests.

Under the Occupational Health Care Act, a drug test can be done on an employee or a jobseeker in occupational health services. In such cases, the performance of tests is subject to health care legislation and the need for the test is assessed by a health care professional, not the employer. Nor can the test result be given to the employer. The employer can only obtain a general health report on the employee's working capacity. Under the specific legislation on civil servants, drug testing can also be part of the medical examination of civil servants.

# 7 Personality and aptitude assessments

Various personality and aptitude assessments are used to assess jobseekers' and employees' personal qualities and knowledge and skills. A jobseeker or an employee may only be tested by means of personality and aptitude assessments if he or she consents thereto.

**Tests may be conducted if they are designed to determine:**

- the capacity to perform the work in question; or
- the need for training or other vocational development.

The results of the assessments must be directly relevant to each employee's employment relationship. This requirement effectively limits both the content and the scope of the assessments, as there are differences in requirements between occupations and duties.

Because the employer uses information from the assessments to make decisions about an individual employee, the results must be free from error. To secure this, the employer is responsible for ensuring that the assessment methods used are reliable, the persons conducting the assessment are experts, and the findings of the assessment are free from error. However, as the assessment in most cases is grounded in behavioural sciences, it cannot be required that the information be absolutely free from error. Therefore, when determining the employer's responsibility, the assessment method and its nature must be taken into account.

Among the alternatives offered, there are many ways in which the employer can weigh the assessment appropriate for each purpose and the expertise of the person performing the assessment. The employer can seek expert help, make the selection by determining the assessor's training, base the selection on the generally known expertise of the assessment company, or find out in advance how, where and by whom the assessment has been developed and what it actually can reveal and what the probability is in each case.

Upon request, the employer or the assessor must give the jobseeker or employee a written statement on the personality and aptitude assessment free of charge. If the employer has received the statement orally, it can be given to the employee orally as well. The employer is ultimately responsible for ensuring that the employee receives the statement.

# 8 Obligation to use healthcare services

In order to guarantee employees' legal protection, when carrying out employees' health examinations or taking samples, the employer may only use healthcare professionals, persons who have received appropriate laboratory training, and healthcare services, whose operating conditions, training requirements and confidentiality obligations are defined in legislation concerning healthcare. The obligation to use healthcare services also applies to alcohol and drug tests. Healthcare professionals define the actions and examinations needed to determine the state of health.

Healthcare solutions emphasise the patient's free will, which also applies to work-related healthcare. In certain situations, the employee is required to undergo a medical examination. Provisions for medical examinations are given, for example, in the Occupational Health Care Act and the Communicable Diseases Act. Special work-related demands, for example in transport, police, fire and rescue tasks, may also require medical examinations. There are also special provisions for establishing the state of health of civil servants.

# 9 Prohibition of genetic testing

The employer may not require that a jobseeker or an employee participate in genetic testing. Nor does the employer have the right to know whether the employee has participated in genetic testing at some point of his or her life. Genetic testing refers to all genetic studies, including predictive genetic tests that investigate the relatives of individuals with hereditary diseases.

# 10 Camera surveillance in the workplace

## 10.1 Preconditions for camera surveillance

**The employer may carry out camera surveillance in the workplace only if the purpose is:**

- to ensure the personal safety of employees and others in the premises;
- to protect property;
- to supervise the proper operation of production processes; or
- to prevent or resolve situations that endanger safety, property, or the production process.

**Camera surveillance is prohibited**

- in the employees' toilet facilities;
- in the employees' changing rooms;
- in staff facilities;
- in work rooms designated for the personal use of employees.

**As a rule, camera surveillance may not be used for the surveillance of a particular employee or particular employees in the workplace. The employer may, however, direct the camera surveillance at a particular work station if the surveillance is essential for:**

- preventing an apparent threat of violence related to the employee's work or an apparent harm or danger to the employee's safety or health;
- 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
- safeguarding the employee's interests and rights, when the camera surveillance is based on the request of the employee who is to be the subject of the surveillance.

## 10.2 Requirements concerning camera surveillance

Camera surveillance must be as transparent as possible and necessary to achieve its purpose. Surveillance recordings can be used only for the purpose for which the surveillance was carried out. Before introducing camera surveillance, the possibilities of using other means that interfere less with the privacy of employees must be explored.

After cooperative or consultative procedures, employees must be informed of when the camera surveillance will begin, how it will be implemented, how and in what situations recordings would be used, and the locations of the cameras if they are directed at workstations where employees work. There must also be prominent signs about the use of camera surveillance indicating whether the camera surveillance is of the recording type.

**There are also certain exceptions to the restricted use of recordings obtained through camera surveillance. The recordings may be used for purposes other than those for which the surveillance was carried out:**

- to substantiate the grounds for termination of an employment relationship;
- to identify and prove harassment, abuse or inappropriate behaviour, as referred to in the Act on Equality between Women and Men, the Non-discrimination Act, and the Occupational Safety and Health Act, if the employer has reasonable grounds to suspect that an employee has been guilty of such behaviour; and
- to investigate occupational accidents or some other situations causing a danger or threat, as referred to in the Occupational Safety and Health Act.

In general, recordings obtained by means of camera surveillance must be destroyed as soon as they are no longer necessary for achieving the purpose of the surveillance, and no later than within one year. However, for special reasons, recordings may be stored beyond this period.

The processing of recordings containing personal data must comply with the General Data Protection Regulation and the obligations imposed on the controller therein.

# 11 Retrieval and opening of electronic mail messages belonging to the employer

In most cases, the email addresses given to employees have the form firstname.lastname@company.fi, and messages are sent and read using the username and password provided to the employee. However, workplace email is also commonly used for personal communications not related to the employer's activities, for example, instead of telephone. Like a call, a private email message is included in the sphere of confidential communication. However, as a form of communication, email is different from the telephone, because both the messages belonging to the employer and the employee's personal messages are recorded there at the same time.

The employer has the right to retrieve messages sent to or from the employee's personal work email only when the conditions provided by law are fulfilled.

Another person may open and read the employee's email messages with the employee's consent, following the procedures agreed. Thus, it is possible to give, for example, a secretary or a substitute explicit permission to read messages.

## 11.1 The employer's obligations regarding necessary arrangements

**In order for the employer to use his authority to retrieve and open the employee's emails, the employer must ensure that the employee can prepare for his or her absence by one of the following alternative means:**

- the employee can use an auto-reply, which informs the sender of the duration of the absence and the substitute;
- the employee can relay the emails to another recipient or to himself or herself at another email address; or
- with the employee's consent, another person may receive the email messages during the employee's absence and assess whether it is necessary for the employer to be informed of the message.

To make use of these possibilities, it is up to the employee to take action. The employer does not have the right to make such redirections to the employee's email.

The employee is not obligated to use the options offered. If the employee does not use these options, the mere offering of the possibilities entitles the employer to sort out the employee's email messages as described in the following section.

The intention is for the employer and the employees to create the most appropriate procedures for each workplace according to its activities and the employees' work tasks.

## 11.2 Retrieval of electronic mail messages belonging to the employer

Once the employer has ensured that the employee has access to one of the options described in the previous section, the employer is entitled to retrieve the employee's messages. The employer can then resolve whether the employee, during his or her absence, has been sent, or has sent or received immediately before the absence, messages belonging to the employer about which the employer must obtain information in order to complete negotiations associated with the employer's operations, serve customers, or otherwise safeguard his operations. Situations of this type arise, for example, with orders, invoicing, and claims, and with the related business negotiations.

**The employer may retrieve a message from the employee's personal work email only if all of the following conditions are met:**

- the employee manages tasks independently on behalf of the employer;
- the employer has no access to a system for recording or otherwise ascertaining the matters managed by the employee and their processing stages;
- it is evident, on account of the employee's tasks and matters pending, that messages belonging to the employer have been sent or received;
- the employee is temporarily prevented from performing his or her duties and the messages belonging to the employer cannot be accessed for use by the employer (although the employer has offered the employee the above possibilities, for example, to direct the messages to another person); and
- 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 is permanently prevented from performing his or her duties and the employee's consent cannot be obtained, the employer has the right to retrieve messages belonging to the employer if the following conditions are met:**

- the employee manages tasks independently on behalf of the employer;
- the employer has no access to a system for recording or otherwise ascertaining the matters managed by the employee and their processing stages;
- it is evident, on account of the employee's tasks and matters pending, that messages belonging to the employer have been sent or received; and
- determining the matters managed by the employee and safeguarding the employer's operations is not possible by other means.

The permanence of the impediment must be assessed on a case-by-case basis in the light of general life experience and the provisions of labour law. It is realised, for example, when the employment relationship is terminated. However, in doing so, it must be taken into account that the employer must also offer such a person the precautionary options described in the previous section. In this way, an employee who is subject to dismissal or termination of employment can, by his or her own actions, contribute to the protection of his or her confidential email, for example by deleting such messages.

The employer can use the data on the sender, recipient or message header to retrieve messages. In practice, the assessment of whether the message belongs to the employer can only be made on the basis of the sender's identification data or the subject field of the email message. This information is not part of the core content of a confidential message. While in most cases this information can be used to determine whether a message is private or not, this is not always possible.

The employer can exercise his right to retrieve messages only with the administrator's help. The employee must be given a written report on the retrieval of messages. The information on the message sender, recipient or header may not be processed more extensively than what is necessary for the purpose of retrieving the message. The persons processing the data may not disclose this information to a third party during or after the employment relationship.

## 11.3 Opening of electronic mail messages belonging to the employer

In the cases described in the previous section, the employer may open an email message only if it is apparent that the message is clearly one that belongs to the employer and it is essential for the employer to obtain information on its contents in order to complete negotiations associated with the employer's operations, to serve customers, or to safeguard the employer's operations. In addition, it is required that an attempt has been made, to no avail, to contact the sender or recipient of the message in order to determine the content of the message or send it to another email address designated by the employer.

The message may only be opened with the administrator's help in the presence of another person. The employee must be given a written report on the opening of the message. The content of the message may not be processed more widely than is necessary for the purpose of opening the message. Nor may the persons processing the message disclose the content of the message and its sender to a third party during or after the employment relationship.

# 12 Cooperation

The collection of personal data at the time of recruitment and during employment falls within the scope of the cooperation procedure. The employer must consult with the employees' representatives on the adoption and content of new personal data systems, as well as on other data to be collected. The cooperation procedure cannot be used to agree on the collection of data that do not meet the necessity requirement of the Act on the Protection of Privacy in Working Life. The objective of the Act on the Protection of Privacy in Working Life is to provide workplaces with procedures that apply to the purpose, adoption and methods of technical surveillance of employees, as well as the use of email and other information networks.

**The scope of the cooperation procedure also covers**

- the purpose and adoption of camera surveillance, access control and other technical monitoring of employees, and the methods used in such surveillance;
- use of email and other information networks;
- the processing of data pertaining to the employee's email and other electronic communication;
- substantial changes in surveillance methods.

**Technical monitoring means at least:**

- access control;
- camera surveillance;
- monitoring via the intranet or an electronic calendar;
- monitoring of email and the information network;
- monitoring of an employee's location.

The cooperation procedure must be carried out before decisions are made on the above matters. The cooperation procedure for email and other information networks primarily applies to their terms of use.

In companies and public-law corporations not governed by cooperation laws, the employer must ensure that employees or their representatives have the opportunity to be heard on similar issues before decision-making.

After the cooperation or consultative procedures, the employer must determine both the purpose of the monitoring and the surveillance methods used in it, as well as the principles for using email and the information network. Thereafter the employer must see to it that the employees are informed of the content of the decision.

# 13 Supervision

Compliance with this Act is supervised by the occupational health and safety authorities together with the Data Protection Ombudsman. When necessary, they can also give advice on the application of the Act.

The employer must keep the Act on the Protection of Privacy in Working Life available to employees at the places of work.

# 14 Penalties for breach of law

The employer or the employer's representative may be fined for violating several provisions of the Act on the Protection of Privacy in Working Life.

An administrative fine, referred to in the General Data Protection Regulation, may be imposed on the controller or the processor of personal data for violating the Regulation. The fine may result, for example, from a breach of the controller's obligations and the data subject's rights stipulated in the General Data Protection Regulation.

The Criminal Code of Finland lays down penalties for data protection offences, hacking, illicit viewing, eavesdropping, message interception, secrecy offences and offences in public office. Penalties for infringement of cooperation legislation are prescribed in cooperation legislation.

**Further information (finlex.fi):**

- Act on the Protection of Privacy in Working Life (759/2004)
- General Data Protection Regulation of European Union (EU 2016/678)
- Data Protection Act (1050/2018)
- Act on Checking the Criminal Background of Persons Working with Children (504/2002)
- Security Clearance Act (726/2014)
- Act on State Civil Servants (750/1994)
- Act on Municipal Officeholders (304/2003)
- Church Act (1054/1993)

Ministry of Economic Affairs
and Employment of Finland